EDITOR'S NOTE

It is my distinct privilege to welcome you to the first Issue of Volume 72 of the Federal Communications Law Journal, the nation's premier communications law journal and the official journal of the Federal Communications Bar Association.

This Issue explores a breadth of diverse topics in the communications sector, including perennial constitutional questions, privacy and data protection, machine learning and artificial intelligence, competition law, and public safety. The Issue opens with an Article on privacy as a parameter of competition in merger reviews by Mark MacCarthy, a Senior Fellow at the Institute for Technology Law and Policy at Georgetown Law, Senior Policy Fellow at the Center for Business and Public Policy at Georgetown's McDonough School of Business, senior fellow at the Future of Privacy Forum, and an adjunct faculty member in the Communication, Culture & Technology Program in the Graduate School at Georgetown University. After eschewing the neo-Brandeisian antitrust reform perspective, Professor MacCarthy concludes that traditional antitrust jurisprudence may consider privacy as an element of competition, though he cautions that such an approach would raise a number of considerations that would likely preclude competition law from being an effective vehicle to increase privacy protections.

In addition to this piece, this Issue contains four student Notes. In the first Note, Brian DeMocker examines the autonomous vehicle industry, arguing for federal legislation to regulate the handling of personal information and analyzing the financial industry's Gramm-Leach-Bailey Act as a model.

In the second Note, Conor Kelly takes a hard look at the *Carpenter v. United States* decision, proposing a reconsideration of consent and privacy by applying the Carpenter blueprint to personal information collected by ride-hailing services.

In the third Note, Christine Kumar considers how the rise in public attention of videos capturing the implicit bias of whites mobilizing police force against Blacks overshadows the more pervasive use of machine learning technologies that likewise perpetuate systemic bias and proposes the scrutiny of such tools under a strict product liability framework and argues for data protection legislation to ensure transparency.

In the final note, John Bick advocates for narrowly tailored state legislation in light of the 2018 Restoring Internet Freedom Order aimed at protecting public health and safety.

The Journal is committed to providing its readership with substantive coverage of relevant topics in communications law, and we appreciate the continued support of contributors and readers alike. We welcome your feedback and submissions—any questions or comments about this Issue or future Issues may be directed to fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. This Issue and our archive are available at http://www.fclj.org.

Tawanna Lee
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

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 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 Federal Communications Bar Association, the *Journal* is distributed to over 2,500 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 http://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 Federal Communications Bar Association (FCBA) 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 communications industry. That is 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, D.C., area, the FCBA has ten active regional chapters: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the United States, its territories, and several other countries.

The George Washington University Law School

Established in 1865, The George Washington University Law School is the oldest law school in Washington, DC. The school is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. The Law School is located on the GW campus in the downtown neighborhood familiarly known as Foggy Bottom.

GW Law has one of the largest curricula of any law school in the nation with more than 250 elective courses covering every aspect of legal study. GW Law's home institution, The George Washington University, is a private, nonsectarian institution founded in 1821 by charter of Congress.

The *Federal Communications Law Journal* is published by The George Washington University Law School and the Federal Communications Bar Association 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 the Federal Communications Bar Association, 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 fcljsubscribe@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 fcljsubscribe@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* (20th ed., 2015), copyright by the *Columbia*, *Harvard*, and *University of Pennsylvania Law Reviews* and the *Yale Law Journal*. 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 72 FED. COMM. L.J. 1 (2020).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 72 ISSUE 1

MAY 2020

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLES

This Article describes how merger reviews under current competition law are able to treat privacy as a dimension of competition. It illustrates this possibility through an examination of the European Commission's reviews of the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger. This Article examines the legal, factual and practical considerations that collectively amount to large and potentially insurmountable obstacles to this effort to improve privacy protection through merger review. These obstacles include the inability to apply or extend privacy law directly, the unresolved conceptual knots in clarifying the notion of privacy competition, the empirical difficulties in determining the existence and extent of privacy competition, and the requirement to show that any post-merger failure to satisfy privacy preferences results from a substantial lessening of competition, rather than from independent business judgements or the proper operation of competitive forces. This Article concludes that merger reviews are not likely to improve privacy very much. It would be better to turn to other aspects of antitrust law or to privacy law itself to vindicate privacy rights.

NOTES

This Note argues that, just as the banking and financial industry is a "vital" industry due to its central and important role in society, the autonomous vehicle industry will be considered a "vital" industry in the coming years for the same reason. Because the banking and financial industry is subject to regulatory restrictions on the handling of users' nonpublic personal information, which incentivizes increased use of the industry's products and services, the autonomous vehicle industry should be subjected to similar data privacy regulations to incentivize usage of autonomous and connected vehicles, which are safer than conventional vehicles. This Note proposes federal legislation, which could be called the Privacy in Autonomous Vehicles and Enforcement Regulation (or "P.A.V.E.R."), that closely mirrors (but

racial biases within the police context need to be suppressed not perpetuated, and thus any new technology used by the police should be properly scrutinized for racial biases.

Public Safety, Preemption, and the Dormant Commerce Clause: A Narrow Solution for States Concerned with the 2018 Restoring Internet Freedom Order's Preemption Clause

This Note examines the important role Internet service providers have come to play in public health and safety, and considers regulatory steps state lawmakers can take to ensure consistent and un-degraded internet content delivery to state public health and safety entities in light of the 2018 Restoring Internet Freedom Order (the *2018 Order*). It focuses on crafting a state law that is able to avoid being preempted by the *2018 Order*, and that also survives dormant commerce clause challenges. Ultimately it concludes that states can enact narrowly tailored laws aimed at protecting state public health and safety entities because (1) the *2018 Order* did not consider the effect its regulatory roll-back would have on public health and safety, (2) limited state laws would not interfere with the FCC's deregulatory agenda, and (3) states have a traditional and important interest in protecting their citizens.

Privacy as a Parameter of Competition in Merger Reviews

Mark MacCarthy[*]

TABLE OF CONTENTS

[*] Adjunct Professor, Communication, Culture, and Technology Program, Georgetown University; Senior Fellow, Institute for Technology Law and Policy at Georgetown Law. Thanks to Mark Whitener, John Mayo, Peter Swire, the participants at presentations of previous versions of this paper at the September 2019 TPRC Conference and at the November 2019 Brussels Privacy Conference, including Orly Lynskey, Joris von Hoboken, and Nicolo Zingales. They are not responsible for the views expressed in the paper or for any remaining errors. Thanks also to the Federal Communications Law Journal staff for their assistance with this publication.

I. INTRODUCTION

Over a decade ago, legal scholars and advocates started a discussion on the intersection of privacy and competition law and policy. This discussion arose from the merger of Google and DoubleClick, and the possibility that the privacy practices of the merged entity could be cognizable under the antitrust merger review at the FTC. Advocates such as the Electronic Privacy Information Center (EPIC)[1] and FTC Commissioner Pamela Harbour[2] argued that privacy as such was a relevant aspect of competition falling within the scope of merger review. The FTC majority at the time, however, thought otherwise, and approved the merger after finding that advertising competitors would have access to the data they needed to compete.[3]

At the time, privacy scholar Peter Swire offered the now-standard explanation of how competition law could accommodate privacy concerns. Without taking a position on the merits of the Google-DoubleClick merger, he argued that: "[P]rivacy harms can lead to a reduction in the *quality of a good or service*, which is a standard category of harm that results from market power. Where these sorts of harms exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them."[4]

What is the realistic potential for merger reviews to address privacy concerns, especially among digital platforms where privacy concerns are most pronounced? In order to answer this question, this Article focuses on how merger reviews under current competition law treat privacy as a dimension of competition.[5] After making some general remarks on the topic, this Article

---

1. *See* Complaint and Request for Injunction for the Electronic Privacy Information Center, Google, Inc., F.T.C. File No. 071-0170 (Apr. 20, 2007) https://epic.org/privacy/ftc/google/epic_complaint.pdf [https://perma.cc/U9EB-BQRR].

2. *See* Pamela Jones Harbour, Dissenting Statement, Google, Inc., F.T.C. File No. 071-0170 (Dec. 20, 2007) https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf [https://perma.cc/6E8A-GBTY].

3. "[T]he evidence indicates that neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product. A number of Google's competitors have at their disposal valuable stores of data not available to Google." Statement of FTC, Google, Inc., F.T.C. File No. 071-017, 12 (Dec. 20, 2007) [hereinafter FTC Statement, Google/Doubleclick], https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [https://perma.cc/8BCF-7G6G]. The European Commission reached a similar conclusion that "the combination of [Google's] data about searches with [DoubleClick's] data about users' web surfing behaviour is already available to a number of Google's competitors today." Commission Decision 139/2004 of Nov. 3, 2018, Case M.4731 Google/DoubleClick, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf [https://perma.cc/WW7V-NBGC].

4. Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR FOR AM. PROGRESS (Oct. 19, 2007) https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/ [https://perma.cc/WW7V-NBGC].

5. *See, e.g.*, MAURICE STUCKE & ALLEN GRUNES, BIG DATA AND COMPETITION POLICY 259-260 (Oxford Univ. Press) (2016) (discussing "how privacy can be viewed as a parameter of quality competition.").

illustrates how merger reviews can assess privacy through an examination of two recent merger reviews involving digital platforms: the European Commission's decisions in their reviews of the Facebook/WhatsApp merger[6] and the Microsoft/LinkedIn merger.[7]

This Article avoids embracing the neo-Brandeisian antitrust reform perspective, which has given a huge impetus to the growing discussion of privacy and antitrust. The neo-Brandeisian movement urges antitrust enforcers to look beyond the consumer welfare standard that has guided antitrust law and policy for several generations.[8] According to this perspective, if antitrust should consider issues such as wage inequality, political corruption, and the power of companies to influence elections, then surely the protection of privacy in the age of big data is also within scope.[9]

The problem, however, is that this broader neo-Brandeisian perspective requires reform of antitrust law. In particular, it would need adjustment of merger review standards, which would be a long and uncertain process. Legislative reforms to improve privacy might ultimately be needed. After all, the conclusion of this Article is that it might be wiser to look elsewhere than current merger reviews if we want to address the privacy concerns that are a focus of such widespread public concern. But before going that route, it might be helpful to see how far we can get without a legislative adjustment to antitrust law.

Instead, this Article adopts the traditional antitrust perspective that merger reviews can examine privacy as an element of competition and take steps to preserve this privacy competition by blocking or conditioning proposed transactions that substantially lessen this form of competition. It also seeks to assess, however, the realistic prospects for making progress on privacy in this way.

The implications of this assessment should not give us cause for optimism. Any exercise of antitrust merger review mechanisms to address privacy concerns necessarily confronts a range of legal, factual, and practical considerations that collectively amount to large and potentially insurmountable obstacles. These include the inability to apply or extend privacy law directly, the unresolved conceptual knots in clarifying the notion of privacy competition, the empirical difficulties in determining the existence and extent of privacy competition, and the requirement to show that any post-merger failure to satisfy privacy preferences results from a substantial lessening of competition, rather than from independent business judgements

---

6. Commission Decision of Oct. 3, 2014, Case M.7217 Facebook/WhatsApp [hereinafter EU Commission Decision, Facebook/WhatsApp], http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf [https://perma.cc/8BWF-G53W].

7. Commission Decision of Dec. 6, 2016, Case M. 8124 Microsoft/LinkedIn [hereinafter EU Commission Decision, Microsoft/LinkedIn], http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf [https://perma.cc/WZ4N-RFBQ].

8. *See* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009 (2013).

9. *See* Khan, *supra* note 8.

or the proper operation of competitive forces.[10] Finally, merger reviews face a fundamental legal limitation in the form of an inability to introduce new competition into the marketplace.[11] This makes it highly unlikely, though not impossible, for merger reviews to increase privacy protections beyond what would already be provided for in the marketplace.

The topic of antitrust and privacy is broad, and this Article deals only with a fraction of the possible overlap—the role of privacy competition in merger reviews. Another area of overlap concerns whether data sets themselves are such crucial competitive assets that antitrust authorities should block or condition mergers that create very large concentrations of data, or take other steps to limit anticompetitive unilateral conduct based on monopoly control of data.[12] In principle, antitrust action to reduce the size or exclusive access to data sets to preserve competition could limit privacy risks. It is important to be aware, however, that competition remedies to data control issues do not necessarily work in favor of privacy protection. Some merger conditions or other measures to remedy dominant positions in the control of competitively essential data, such as mandated data sharing, might create additional privacy risks, for example, by requiring the transfer of information a customer shared with one company to a company with less privacy protective data practices.[13]

A further intensively discussed overlap is whether antitrust action against abuse by dominant companies can impose data protection requirements—such as additional consent requirements—that are effectively more stringent than the data protection rules that have to be followed by non-

10. *See* Section II B-H infra.

11. *See* Section II A infra.

12. Considering data as an asset will be increasingly important in merger reviews, but it is not the same as assessing privacy competition in merger reviews. The key question in thinking of data as a key asset is whether there will be enough of it left over after the merger for rivals to compete fairly. That is different from the question of whether companies compete over privacy. Data as a competitive asset was a focal point of the FTC's merger review of the Google/DoubleClick merger. *See* FTC Statement, Google/Doubleclick, *supra* note 3. It was an issue in the European Commission reviews of Facebook and WhatsApp as well as Microsoft and LinkedIn. *See* EU Commission Decision, Facebook/WhatsApp, *supra* note 6; EU Commission Decision, Microsoft/LinkedIn, *supra* note 7. In each case, discussed below in Sections III and IV, the reviewing authority approved the merger after finding that post-merger there would be adequate data left over for advertising rivals.

13. Viktor Mayer-Schönberger & Thomas Ramge, *A Big Choice for Big Tech: Share Data or Suffer the Consequences*, FOREIGN AFFAIRS (Aug. 13 2018), https://www.foreignaffairs.com/articles/world/2018-08-13/big-choice-big-tech [https://perma.cc/3Y6E-B2CB].

dominant companies.[14] This might not improve matters for all companies, but like merger conditions that effectively imposed net neutrality obligations on merging communications companies, they remedy special problems created by mergers or strong market positions.[15]

An assessment of these other areas might yield other ways in which antitrust enforcers could improve privacy protection. But they are outside the scope of this Article and hopefully will be dealt with in future work.

It is certainly legitimate for antitrust authorities to take privacy into account in merger reviews in certain circumstances. It is not bad policy to do this, but such efforts are not likely to improve privacy very much. If we want more privacy than current law requires, and more than companies would normally provide on their own, we will need to establish it through other resources available to competition law or directly through new national privacy legislation.

In Section II, this Article makes general remarks about the relationship of traditional merger review and privacy. In Sections III and IV, this Article discusses the European Commission's review of the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger to reveal how they treated privacy as an element of competition. Section V reviews some lessons learned from these cases, and Section VI concludes that merger reviews should not be

---

14. In an abuse of dominance case, the German Federal Cartel Office required Facebook to get affirmative consent for collecting and merging third-party and affiliate data from users. Facebook FAQ, Bundeskartellamt (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6 [http://perma.cc/2CHY-NVP7]; B6-22/16 - *Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing* (Feb. 15, 2019) [hereinafter *Case Summary: Facebook*], https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3 [http://perma.cc/B6VW-MZXG]; Press Release, *Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources* (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html[http://perma.cc/2H8E-8E77]. *See also* Dr. Jörg Hladjk et al., *The German Facebook Case – Towards an Increasing Symbiosis Between Competition and Data Protection Laws?*, CPI ANTITRUST CHRONICLE (Feb. 2019), https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/CPI-Hladjk-Werner-Stoican.pdf [https://perma.cc/W42Q-MQ9Y]. On August 26, 2019, the Düsseldorf Higher Regional Court suspended the competition authority's ruling. *See* The Decision of the Higher Regional Court of Düsseldorf, Case VI-Kart 1/19 (V) (Aug. 26, 2019) [hereinafter Düsseldorf Decision], https://www.d-kart.de/wp-content/uploads/2019/08/OLG-Düsseldorf-Facebook-2019-English.pdf [https://perma.cc/Z2BU-XE2P] (English translation). A different example comes from the FCC's now-repealed broadband privacy rules imposing opt-out consent for dominant broadband companies. *See* News Release, FCC Adopts Broadband Consumer Privacy Rules, FCC (Oct. 27, 2016), https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules [https://perma.cc/8FKL-DK9L].

15. Because the merged entity controlled both cable systems and a leading ISP (AOL) that relied on open access to cable to reach its subscribers, the FTC's consent order required it to provide non-discriminatory access to its cable systems for ISPs competing with AOL and prohibited it from interfering with the content provided by competing ISPs. *See* America Online, Inc. & Time Warner Inc., F.T.C. Dkt. No. C-3989 (Apr. 17, 2001), https://www.ftc.gov/sites/default/files/documents/cases/2001/04/aoltwdo.pdf [http://perma.cc/S5NX-6FRL].

relied upon as a significant legal mechanism securing the maintenance of privacy protections. The results of this Article strongly suggest that it would be better to turn to other aspects of antitrust law or to privacy law itself to vindicate privacy rights.

II. GENERAL REMARKS

A. Traditional Antitrust Merger Review Preserves, But Does Not Enhance, Competition.

Merger reviews under traditional antitrust principles seek to block the loss of competition. Section 7 of the Clayton Act bars any acquisition with an effect that "may be substantially to lessen competition, or to tend to create a monopoly."[16] The "unifying theme" of the Justice Department's 2010 Horizontal Merger Guidelines is that "mergers should not be permitted to create, enhance, or entrench market power or to facilitate its exercise."[17]

European competition law is similar. Under the European Council's Merger Regulation:

> [A] concentration which would not significantly impede effective competition . . . shall be declared compatible with the common market . . . [and] . . . a concentration which would significantly impede effective competition, in particular as a result of the creation or strengthening of a dominant position, shall be declared incompatible with the common market.[18]

Thus, the touchstone of antitrust merger review is the preservation, not the enhancement of existing competition. Reviewing agencies do not have the capacity to block a transaction on the grounds that it does not introduce new

---

16. 15 U.S.C. § 18 (2018).

17. U.S. DEP'T JUST. & FTC, HORIZONTAL MERGER GUIDELINES 2 (2010) [hereinafter "DOJ 2010 Merger Guidelines"], https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf [http://perma.cc/Q7MR-9T8W]. The FTC's retrospective 2007 study of the success or failure of merger remedies defined success as "maintaining or restoring competition[,]" that is, "competition in the relevant market remained at its pre-merger level or returned to that level within a short time (two to three years)." FTC, THE FTC'S MERGER REMEDIES 2006-2012 15 (January 2017), https://www.ftc.gov/system/files/documents/reports/ftcs-merger-remedies-2006-2012-report-bureaus-competition-economics/p143100_ftc_merger_remedies_2006-2012.pdf [https://perma.cc/WK2Z-BXD5]. Even proposed reforms of merger enforcement do not change this focus on avoiding the lessening of competition, rather than enhancing it. *See, e.g.*, S. 1812, Consolidation Prevention and Competition Promotion Act of 2017, introduced by Senator Amy Klobuchar (D-MN), September 14, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1812 [https://perma.cc/M4XN-7QFB] (changing the standard from "substantially lessens competition" to "materially lessens competition in more than a de minimis amount.").

18. Council Regulation (EC) No 139/2004 of Jan. 20, 2004, *The control of concentrations between undertakings (the EC Merger Regulation)*, OJ L 24, 29.1.2004, Article 2(2) and Article 2(3), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0139&from=EN [https://perma.cc/6TXC-3F29].

competition that was not previously there.[19] A merger review is forward-looking only to the extent that is does not want to allow the competitive future to be worse than the past.

This is in contrast to the standard of review that applies to mergers under the jurisdiction of some sector-specific regulatory agencies. For instance, the FCC reviews mergers when they involve the assignment and transfer of control of certain spectrum licenses and approves them only when it determines that they serve the "public interest, convenience and necessity."[20] The FCC can and does apply traditional analysis relating to the loss of competition in its merger reviews, but it also must make a broader public interest determination. In particular, the FCC considers "whether a transaction will enhance, rather than merely preserve, existing competition, and often takes a more expansive view of potential and future competition in analyzing that issue."[21]

As a result of this fundamental difference, the best that might be expected from traditional antitrust merger reviews is that they will block or condition mergers that would substantially weaken the privacy competition that existed in the market prior to the merger. It is hard to see how a traditional antitrust merger review could condition a merger so as to require companies to provide customers with improved privacy protections that they previously did not enjoy.

Despite this obstacle, it is possible to imagine circumstances in which a merger condition imposed purely to remedy a competition problem could have the effect of improving privacy protection. For instance, as described in the German antitrust case against Facebook, the social media company requires its users to accept tracking on third-party websites as a condition of using its service.[22] An antitrust authority could, of course, simply block the merger as anticompetitive, and this would leave privacy protections exactly the way they were before the proposed merger. But it could also seek to offset that anticompetitive effect by prohibiting the merged entity from combining third-party tracking data with data from activity on the social media site or requiring it to get separate consent to do so. That is, it could try to require the social media company to be more protective of its existing users' privacy as a condition of approving the merger. This would have the effect of improving

---

19. *Id.*; 15 U.S.C. § 18, *supra* note 16; DOJ 2010 Merger Guidelines, *supra* note 17, at 2.

20. FCC, *Applications of Comcast Corp., Gen. Elec. Co., and NBC Universal, Inc. for Consent to Assign Licenses and Transfer Control of Licenses*, Memorandum Opinion and Order, 26 FCC Rcd. 4238, ¶23-24 (2011) [hereinafter FCC, *Comcast, Gen. Elec. & NBC*, Memo], https://www.fcc.gov/document/applications-comcast-corporation-general-electric-company-and-nbc-1 [http://perma.cc/99NY-3NPA]. *See also* Jon Sallet, FCC, *FCC Transaction Review: Competition and the Public Interest* (2014), https://www.fcc.gov/news-events/blog/2014/08/12/fcc-transaction-review-competition-and-public-interest [http://perma.cc/4G97-RPAU].

21. FCC, *Comcast, Gen. Elec. & NBC*, Memo, *supra* note 20, at 11.

22. *See Case Summary: Facebook*, *supra* note 14. *See also* Terms of Service, FACEBOOK (last accessed Apr. 28, 2020) https://www.facebook.com/terms.php [https://perma.cc/SJ6B-EM8G].

privacy protection for its existing users, as well as protecting competitors in the advertising market.[23]

This example suggests that it is possible for traditional antitrust authorities to seek in the context of a merger review to improve the state of privacy protection beyond what is already being provided in the market. This possibility seems to arise where the antitrust authority could establish that a merger would lessen competition due to a combination of data that foreclosed competition. With the growth of data as a competitive asset in today's digital economy, this might not be rare. Still, the antitrust authority would need to explain why prohibiting the combination of data wouldn't be sufficient to resolve the issue, rather than improving privacy protections for existing users. This might be an uphill climb both legally and factually. My sense is that while an activist antitrust authority might try to improve privacy protections in this way, it would be unlikely to succeed.

B. Advancing Privacy Protections is Not a Legitimate Objective of Traditional Antitrust Merger Reviews

As discussed further in this section, traditional antitrust merger review has no authority to consider extraneous factors, such as privacy, independently of the transaction's effect on competition.[24] Not only is it unlikely to advance privacy values beyond what would occur in the marketplace, it may not independently consider such matters at all.

This contrasts with transaction reviews conducted by some specialized agencies. When the FCC reviews mergers, it is required to take into account values other than competition including ensuring a "diversity of sources of information" and "whether the transaction will affect the quality of communications services or will result in the provision of new or additional services to consumers."[25]

In its Google/DoubleClick decision, the FTC articulated this notion that merger reviews can aim only at preserving competition, not preserving or enhancing other values:

---

23. This is the fact pattern in the German FCO's case against Facebook altered to suppose that the merging companies sought to achieve a dominant position through merger rather than attaining it through organic growth. *Case Summary: Facebook*, *supra* note 14. I am imagining in this hypothetical that the merger review authority focuses only on protecting competition in the advertising market, not on improving privacy protection as such.

24. *See infra* notes 26 and 27.

25. *See* Sallet, *supra* note 20.

> The Commission has been asked before to intervene in transactions for reasons unrelated to antitrust concerns, such as concerns about environmental quality or impact on employees. Although such issues may present important policy questions for the Nation, the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition.[26]

This view has the backing of Supreme Court precedent. In *United States v. Philadelphia National Bank*, the Court ruled that the effect upon competition is the sole criterion to determine whether a merger violates Section 7 of the Clayton Act.[27] The fact that the merger would increase employment in a particular city was deemed irrelevant.[28]

European competition law enforcers take the same general view. For instance, the European Commission adopted it in its review of the Facebook/WhatsApp merger:

> Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.[29]

The European Court of Justice upheld this view of the relationship between competition law and data protection law: "[S]ince . . . any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."[30] This is the antitrust consensus even today. Antitrust scholar Carl Shapiro recently said: "Antitrust is not designed or equipped to deal with many of the major social and political problems

---

26. FTC Statement, Google/Doubleclick, *supra* note 3, at 2.

27. 374 U.S. 321 (1963).

28. This decision is famous for establishing the since-modified quick-look standard that used increased concentration as a test for lessening competition: "a merger which produces a firm controlling an undue percentage share of the relevant market, and results in a significant increase in the concentration of firms in that market, is so inherently likely to lessen competition substantially that it must be enjoined in the absence of evidence clearly showing that the merger is not likely to have such anticompetitive effects." *Id.* at 363. But it also rejected the idea that merger reviews could go beyond the standard of lessening competition to take into account other "social or economic" effects of a proposed merger: "a merger the effect of which 'may be substantially to lessen competition' is not saved because, on some ultimate reckoning of social or economic debits and credits, it may be deemed beneficial." *Id.* at 371.

29. *See* EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 164.

30. Case C-238/05 – , Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios (Ausbanc), [2006] E.C.R. I-1116425, par. 63, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62005CJ0238&from=EN [https://perma.cc/KYU2-SN6K].

associated with the tech titans, including threats to consumer privacy and data security, or the spread of hateful speech and fake news."[31]

Moreover, the recent Common Understanding among the G7 competition authorities also repeats the point that: "[G]overnments should avoid using competition law enforcement to address non-competition objectives . . . ."[32]

Of course, an agency review that blocks a merger on the grounds that it would substantially lessen competition in the advertising market might also preserve data practices that people value as privacy protective. In a similar way, conditions on a merger designed to preserve competitive conditions in the advertising market after the merger might also preserve valued data practices, as in the social media example sketched above. Antitrust practitioners likely would not look askance upon merger controls that accidentally preserved privacy in this way.

On the other hand, these possibilities should not give much comfort to the proponents of using merger reviews to protect privacy, since it would be only a coincidence that merger controls aiming to preserve competition also improve privacy. Privacy advocates would want more from privacy-aware merger reviews than this sort of accidental privacy protection.

C. Relationship of Privacy Law to Merger Review

This general point that merger reviews are focused on preserving competition, not enhancing or maintaining privacy, has several implications that are worth emphasizing. One is that merger control reviews do not apply or enforce existing privacy law. A second is that data collection practices of the merging companies must be viewed as satisfying current legal requirements. Third, any merger requirements for data practices that exceed current legal privacy requirements must be justified as necessary to sustain competition. They cannot be based solely on the idea that they constitute better privacy protection.

Traditional antitrust merger reviews apply the standards of competition law, not the requirements of privacy or data protection law.[33] In the cases we consider below the European Commission reviewed potential mergers between companies that, prior to the merger, were in full compliance with European data protection law. There was no question of using merger review as a way to bring non-compliant companies into compliance with data protection law.

---

31. Carl Shapiro, *Protecting Competition in the American Economy: Merger Control, Tech Titans, Labor Markets*, 33 J. ECON. PERSPS. 69, 79 (2019).

32. FTC, G7 France, Common Understanding of G7 Competition Authorities on 'Competition and the Digital Economy' (June 5, 2019) https://www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports-common-understanding-g7-competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf?utm_source=govdelivery [https://perma.cc/NAT3-9JDE].

33. *Supra* Section IIA.

Both the US and Europe have extensive legal structures aimed at promoting privacy. In its complaint to the FTC in connection with the Google/DoubleClick merger, EPIC properly noted that: "The right of privacy is a personal and fundamental right in the United States."[34] Privacy is also regulated by specialized agencies, the FTC, and a variety of state laws, including the recently passed California Consumer Privacy Act of 2018.[35] In Europe, the General Data Protection Regulation (GDPR), adopted in 2018, provides a comprehensive framework to vindicate what European law regards as the fundamental rights to privacy and data protection.[36]

But in assessing mergers through the lens of privacy, compliance with privacy law is not at issue. The question before the reviewing agency is not whether companies comply with privacy law. The question is whether the merger substantially lessens competition, and in doing so whether it harms consumers, including whether the loss of competition deprives them of privacy choices they previously had and valued.[37]

This is not to say that competition law in general in Europe is powerless to apply data protection law. The European Commission's practice of avoiding data protection enforcement in merger reviews is in sharp contrast to the approach taken by Germany's Federal Cartel Office (FCO) in its action against Facebook. In that case, the FCO claimed authority to act as an enforcer of the European GDPR.[38] It determined that Facebook needed consent from its users to combine third-party data with its data from user interactions on Facebook's own service.[39] Because of its dominance in social media, the take-it-or-leave it form of choice it provided did not amount to genuine consent. And it imposed a data protection remedy in the form of a separate consent requirement.[40]

But this was a case of abuse of dominance, not a merger review, and it was brought under German law, not European competition law. It is not clear that the same legal opportunity arises for merger reviews in light of *Asnef-Equifax,* a decision by the European Union Court of Justice, which held that: "[I]ssues relating to the sensitivity of personal data are not, as such, a matter for competition law."[41] As a result, at this point merger reviews are not an occasion for enforcement of privacy laws in Europe.

This means that the data practices assessed in the context of a merger review are all legal practices. These practices might involve greater or lesser collection and use of data, and a corresponding increase or decrease in product or service personalization. But they are all within the parameters allowed by

---

34. EPIC Complaint, *supra* note 1, at 2.

35. Cal. Civ. Code § 1798.100-198.

36. *See* Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en [https://perma.cc/3L9R-L3FU].

37. *See* infra Section IIH.

38. *See Case Summary: Facebook*, *supra* note 14.

39. *Id.*

40. *Id.*

41. *Supra* note 30.

existing privacy and data protection law. In so far as merger reviews under competition law are concerned, no data practice that is legal under data protection law has a preferred status.

Merger reviews can take privacy into account, but not directly, by ascertaining whether the rivalry among companies in the markets affected by a proposed transaction takes place significantly along the dimension of these differing but legal data practices. And if a merger review finds the existence of significant privacy competition, it then needs to assess whether measures are needed to preserve that competition in a post-merger world.

This point affects some of the language used to describe the way in which merger authorities can take privacy into account. Peter Swire, for example, describes the consumer loss connected to loss of privacy competition as "privacy harms."[42] This phrase suggests to me that the company has used data in a way that violates consumer privacy rights and that it is a legitimate role of merger analysis to take these privacy law violations into account in assessing a merger.

But the consumer harm involved, if any, is not that the companies are violating consumer privacy rights, but that they are not satisfying consumer privacy preferences. This failure to satisfy consumer privacy preferences, even when there is no legal obligation to do so, is likely what Swire intends by the phrase "privacy harm." But it has, to my ear anyway, suggestions of illegality under privacy law.[43]

Finally, some advocates think that merger reviews should consider possible improvements in privacy law that might more adequately vindicate the fundamental right to privacy.[44] An opt-in form of consent might be more protective of privacy than opt-out, for instance, and so a merger review might contemplate imposing that requirement as a merger condition, even if it is not required by current privacy law. The merging of separate data sets might create new privacy risks in the form of new and more detailed consumer profiles. These collections of data might be entirely legal under existing privacy law, but a merger review might block a transaction that would merge these data sets or might condition the merger on maintaining them in a separate non-linkable form. The reviewing agency might think it would be better for the merging companies to face privacy rules that go beyond their current legal obligations under privacy law.

But these measures would be unavailable to merger reviewing agencies if aimed at improving privacy protections instead of maintaining competitive conditions. The FTC recognized this restriction on advancing privacy interests in the context of merger reviews, saying in its decision on

---

42. *See* Swire, *supra* note 4.

43. *Id.*

44. EPIC seems to take this view in its Congressional testimony that merger reviews can legitimately impose merger conditions that exceed current privacy law. *See An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy?*, *Hearing Before the Subcomm. on Antitrust, Competition Policy and Consumer Rights, of the S. Comm. on the Judiciary*, 110th Cong. (2007) (statement of Marc Rotenberg, President, EPIC).

Google/DoubleClick: "[T]he Commission lack[s] legal authority to require conditions to this merger that do not relate to antitrust . . . ."[45]

This is not to say that privacy law is perfect and cannot be improved. It is rather that needed improvements of privacy law are not within the scope of traditional merger reviews.

D. Privacy Can Be Legitimately Treated as an Aspect of Competition in Merger Reviews

Despite constraints on the ability of merger reviews to advance privacy interests, there is a way forward for merger reviews to account for privacy. Merger control might advance privacy interests by rejecting or conditioning a merger that would restrict consumer choice of stronger privacy practices. This would have the effect of maintaining privacy protections that the merger might eliminate because it would block or condition a merger that would absorb or marginalize a competitor with more privacy protective data practices.

This approach treats privacy as a non-price aspect of competition. Merger reviews are not limited to examining whether the merged entity could impose an anticompetitive price increase unrelated to an improvement in quality. A company might choose to exercise its post-merger market power by a cost-saving reduction in the quality of its product or service. It might also reduce its efforts to innovate, since it no longer faces the prospect that strong competitors will steal customers by introducing new features that make the product or service faster, more convenient, or easier to use. Merger reviews can investigate whether the resulting market conditions would allow any substantial reduction in competition along any dimension of product or service quality that is valued by consumers and that forms the basis for rivalry between competing firms.

The DOJ Merger Guidelines countenance steps that would enable reviewing agencies to consider privacy in the context of merger reviews.[46] They note that impermissible increases in market power following a merger can be manifested in "non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation."[47] Data practices that adversely affect consumer privacy preferences could be considered one of these "non-price terms and conditions."[48]

The Guidelines explicitly recognize that the loss of product variety is a cognizable antitrust harm: "If the merged firm would withdraw a product that a significant number of customers strongly prefer to those products that would remain available, this can constitute a harm to customers over and above any effects on the price or quality of any given product."[49] The loss of a service

45. FTC Statement, Google/Doubleclick, *supra* note 3, at 2.
46. DOJ 2010 Merger Guidelines, *supra* note 17.
47. *Id.* at 2.
48. *Id.*
49. *Id.* at 24.

providing strong privacy protections following a merger might be viewed as a reduction in product variety and taken into account in a merger review.

Companies could compete on privacy in any number of ways: providing clearer, easier to read descriptions of their data collection practices, allowing choice about data use in a wider range of circumstances, adjusting the choice architecture to provide for opt-in rather than opt-out choice, allowing secondary use only with affirmative opt-in consent, not sharing customer data for third-party marketing, minimizing the data collected and discarding it after its initial use. When differences in these privacy practices are valuable for consumers and a basis for choice among competing products or services, they are a dimension, aspect, or parameter of competition.

Traditional antitrust officials increasingly accept the idea that privacy can be an aspect or dimension of competition. Former FTC Commissioner Maureen Ohlhausen has written: "Privacy therefore increasingly represents a non-price dimension of competition." [50] European Commission competition officials Eleonora Ocello and Cristina Sjödin say that in digital markets, "the degree of privacy afforded by the platform (i.e. the type of data protection policy in place) may thus become a relevant parameter of competition."[51] The current head of the DOJ Antitrust Division, Makan Delrahim, has also supported this view: "[C]onsumers may choose . . . online search services based on more accurate results or greater privacy protections."[52] Proponents of incorporating privacy considerations into antitrust enforcement such as Maurice Stucke and Allen Grunes agree with this framework whereby privacy can be incorporated into merger control analysis, accepting as a touchstone "the requirement that privacy be an 'important' factor in the decision to purchase or a 'key' parameter of competition."[53]

As a result, notwithstanding the general principle that competition policy is concerned solely with protecting competition, when privacy is a "main" or "key" or "important" element in consumers' decisions to purchase a good or service, a merger that eliminated or reduced competition along this non-price dimension could be blocked or conditioned under antitrust law. This possibility means merger reviews could in principle maintain privacy-protective data practices that already exist in the marketplace.

---

50. Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 151 (2015).

51. Eleonora Ocello & Cristina Sjödin, *Digital Markets in EU Merger Control: Key Features and Implications*, CPI, ANTITRUST CHRONICLE, at 5 (Feb. 2018), https://www.competitionpolicyinternational.com/digital-markets-in-eu-merger-control-key-features-and-implications/ [https://perma.cc/8G8F-BC23].

52. Makan Delrahim, Assistant Attorney-General, Speech at the Silicon Flatirons Annual Technology Policy Conference at The University of Colorado Law School, *"I'm Free": Platforms and Antitrust Enforcement in the Zero-Price Economy* (Feb. 11, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-silicon-flatirons [https://perma.cc/HFY3-485D].

53. STUCKE & GRUNES, *supra* note 5, at 131.

E. Some Conceptual Points

Noting that privacy can be considered as a feature or parameter of competition invokes the question of how to do it. An important first step is to develop a concept of privacy that is suitable for merger control analysis.

European competition policy officials involved in the Commission's review of the Facebook/WhatsApp merger offer a common conceptualization of how to treat privacy as an element of competition in a merger review case:

> In two-sided markets, where products are offered to users for free and monetised through targeted advertising, personal data can be viewed as the currency paid by the user in return for receiving the 'free' product, or as a dimension of product quality. Hence, a website that, post-merger, would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product could be seen as either increasing its price or as degrading the quality of its product. In certain circumstances, this behaviour could arguably amount to an infringement of competition law (irrespective of whether or not it also constitutes an infringement of data protection rules). However, while technically viable, this theory of harm could only be relevant in those cases where privacy is an important factor in the decision to purchase a product or service, i.e. a key parameter of competition.[54]

As this quotation illustrates, these Commission officials conceptualize data collection and use as a reduction in the quality of a service. In doing this, they are accepting a widespread notion that data collection and use is a uniformly negative phenomenon or, equivalently, that a decrease in data collection and use is intrinsically a good thing. Privacy becomes like product safety or the power of a car engine, something that all consumers would likely want more of rather than less. This conception of privacy as a loss of product quality feeds into merger reviews because degradation of quality is a consumer loss that can be considered in merger reviews.[55]

But is it really useful for merger reviews to think of a decreased flow of information as uniformly a good thing? Is a company that collects more information really, objectively, and for that reason alone, providing a worse product or service?

For merger review purposes it is much more realistic to think of privacy as subjective in that it "may be valuable only to some consumers, or more

---

54. Eleonora Ocello et al., *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case*, Competition Merger Brief 1, 6 (2015) http://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf [https://perma.cc/7SRY-69QU].

55. *See* Swire, *supra* note 4.

valuable to some than others."[56] Whether a company collects a lot of data or a small amount of it is as objective a fact as the engine power or color of a car. The data practices of data collection, choice architecture, data minimization and retention, and so on are all objective conditions that in principle are observable. What is subjective is the value that people place on these practices.

Alan Westin's surveys over a thirty-year period show substantial variation in the value people place on privacy. Some people value privacy highly in almost all circumstances (the privacy fundamentalists, roughly 25%), some are largely indifferent (the privacy unconcerned, roughly 25%), and the rest (the privacy pragmatists, about 50%) say it depends on the context.[57]

Moreover, people's responses to survey questions likely do not match their marketplace behavior. A solid line of research has shown the existence of a "privacy paradox: users claim to be very concerned about their privacy but do very little to protect their personal data."[58] This well-established phenomenon makes it difficult to assume universal agreement that more privacy and less data collection is inherently good.

The variation in consumer preferences in surveys and the lack of fit between those surveys and actual consumer behavior might very well be attributable to market defects in the provision of adequate information to allow a timely and informed privacy choice. Consumers might never be able to develop an adequate and timely understanding of information uses simply because of the complexities of modern data collection and analysis techniques. Moreover, companies might be using overly complicated legalistic notices to discourage proper understanding and might design websites and apps deceptively through the use of "dark patterns" to encourage information sharing that might not be in the best interests of consumers or reflect their true preferences.[59]

---

56. Organization for Economic Cooperation & Development, *The Role and Measurement of Quality in Competition Analysis,* Quality Report (2013) [hereinafter OECD Quality Report], http://www.oecd.org/competition/Quality-in-competition-analysis-2013.pdf [https://perma.cc/M7HK-ZQYW].

57. Ponnurangam Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies*, SCH. OF COMPUT. SCIENCE, CARNEGIE MELLON UNIV. (Dec. 2005), http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf [https://perma.cc/W6MM-LJ6G]. Recent survey research confirms this variation in privacy preferences, especially when combined with increased personalization services. *See* Phyllis Rothschild et al., *Why Personalization Matters for Consumer Privacy*, MIT SLOAN MGMT REV. (June 6, 2019), https://sloanreview.mit.edu/article/why-personalization-matters-for-consumer-privacy/.

58. *See* Susanne Barth & Menno D.T. de Jong, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*, 34 TELEMATICS & INFORMATICS 1038 (2017), https://www.sciencedirect.com/science/article/pii/S0736585317302022 [https://perma.cc/U7WY-E92W].

59. Norwegian Consumer Councils, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, FORBRUKERRADET (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/ZL2X-FFTW].

But it is not clear how to bring these insights to bear in a merger review. These marketplace defects would be more appropriately remedied through additional consumer protection measures designed to provide consumers with adequate and timely information. Indeed, that is the purpose of many privacy laws. A new law might also be needed to prevent deceptive dark pattern.[60] But these reforms cannot be implemented as part of a merger review. For merger control purposes, preferences expressed in measures of marketplace demand have to be assumed to reflect real preferences.

Competition law has to conceive of privacy as a feature of a service that is offered to consumers on the market. People have different preferences for different economic goods, including differing preferences in connection with privacy. Those differences must be acknowledged when engaged in competition analysis.

As a result, in an assessment of competition in privacy for merger review purposes, people have to be viewed as having privacy tastes in the same way that they have color tastes or food tastes. It is no more legitimate from the point of view of assessing marketplace privacy competition to say that privacy protective practices are higher quality than it is to say, without any evidence from surveys or other assessments of effective actual consumer preferences, that blue cars are of higher quality than yellow cars or that corn is better than green beans.

James Cooper provides an additional perspective on why increasing data collection and use might not always amount to a reduction in product quality. He suggests that data collection and use is an intermediate good, an input that companies use to improve the overall quality of their product and services:

> Taking additional consumer data is not the same as skimping on quality, because collecting, storing, and analyzing data is an additional cost. For the publisher, improved data is an investment. The publisher hopes to enhance its revenue by using the additional data to improve the quality of its content and through selling more finely targeted ads.[61]

The result is that consumers are offered additional benefits associated with the additional data collection. It is that bundle that consumers are asked to evaluate, not the additional data collection all by itself. As Cooper notes, consumers do not reach a uniform judgment about the value of these bundles:

---

60. *See, e.g.*, S. 1084, 116th Cong. (2019).

61. James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1135-1136 (2013).

> Some consumers may care little about being tracked online or having Google read their e-mails, and they may derive great utility from easier searching and highly relevant ads. On the other hand, there are others who may detest targeted ads and the "creepy" feeling from knowing that their search and browsing histories are stored on multiple servers. For these people, data collection may well be a net reduction in quality.[62]

The key idea here is that data collection and use are inputs for production of goods and services. In the absence of a given level of data collection and use, the product or service would be different. In particular, it would differ in the level of personalization it would provide, that is, in the extent to which it was designed to satisfy the interests and preferences of the consumer.

Companies compile personal information about their customers or potential customers in order to tailor their services to their interests and needs and thereby make it more attractive to them and to increase their engagement with the service.[63] This is true of many digital companies such as search engines, social networks, and online marketplaces, whether they are general marketplaces selling a variety of products or providing specific services such as streaming music or videos. In a social network, for instance, the additional data collection and use make possible recommendations for content and contacts that better match the interests of the user. In networks supported by targeted advertising, the data collection and use also powers ads that are more likely to be of interest to the user.

This use of data to personalize services is broader than digital companies, and broader than two-sided markets for "free" goods. To name just two other sectors, healthcare providers use data to personalize medicine[64] and educators use data to personalize education.[65] The oddity of conceptualizing data collection and use as a quality degradation is perhaps more apparent in these cases where such a conception would have to treat the increases in the quality of medicine and education from personalization as a decline in service quality.

The same point arises from consideration of traditional ways personal information is used to provide services. Sharing personal, and sometimes sensitive, information with your doctor, lawyer, counselor, or bank in order to get services relevant to your situation is the only way to get the services, or at least to get them in a form that provides real value. It is hard to see such information sharing as intrinsically reducing the quality of the service provided.

---

62. *Id.* at 1137.

63. *See, e.g.*, Terms of Service, FACEBOOK, *supra* note 22.

64. *See, e.g.*, Irene Dankwa-Mullan, *Examining health disparities in precision medicine*, IBM (Oct. 14, 2019), https://www.ibm.com/blogs/watson-health/examining-health-disparities-in-precision-medicine/ [https://perma.cc/KZ6S-B7SX].

65. *See, e.g.*, U.S. Dep't of Education, Office of Educational Technology, Learning (last accessed Apr. 29, 2020) https://tech.ed.gov/netp/learning/ [https://perma.cc/2WNS-ES6L].

Privacy conceived of as limited data collection and use often operates at the expense of personalization. The two vary inversely. As privacy goes up, personalization goes down, and vice versa. Consumers typically purchase a bundle, not privacy as an isolated feature of a product or service. The range of possible bundles a company could offer would extend from one extreme of very high personalization and data collection to the other extreme of very low personalization and data collection.[66]

Economist Joseph Farrell has a different perspective on these conceptual issues.[67] He understands that privacy comes bundled with a service but conceives of this bundling as productively inoperative, a feature that can be arbitrarily added or removed from the service without making any difference to its other features that consumers might value.[68] In his view, book-selling companies might attach a privacy policy allowing them to collect and use information or not, with no other difference to the consumer in the service that the book-selling company offers.[69]

It is this assumption—that data collection and use has no role in the production of the service—that allows him to assert, as a key element in his economic model of privacy as "just another good" that: "A book, bundled with privacy policy B, is a less attractive good than the book bundled with privacy policy A," where B allows greater data collection and use and A allows less.[70] In fact, a book-selling service that collects substantial information about its purchasers is able to make recommendations that might match the consumers' interests and tastes far more effectively than a service that discards this information, and might therefore provide a service that is more valued, not one that is automatically inferior because of its greater data collection practices.

It is true that in some circumstances, data collection could be completely disconnected from the provision of the service. This seems to be the case with the example Farrell has in mind of a publisher who simply sells consumer information to the highest bidder, without changing the nature or character of the books it sells or recommends.[71] But that is not the central case of data collection and use. Companies typically collect information about their customers to improve the service they provide and, when they are advertiser-supported, to target ads more closely to their interests.[72]

For this reason, Farrell's model of data collection and use as arbitrarily added to a final good is not likely to be of much help in merger reviews. Much more relevant is the conception of data collection as an intermediate good

---

66. Cooper, *supra* note 61, at 1137.

67. Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. ON TELECOMM. & HIGH TECH. L. 251, 254 (2012).

68. *Id.* at 253. "[L]et's think about a firm selling a book to a consumer, and analyze choice of the firm's privacy policy governing later re-purposing of the consumer's information."

69. *Id.*

70. *Id.* at 254.

71. *Id.* at 253.

72. *See, e.g.*, Terms of Service, YOUTUBE, https://www.youtube.com/static?template=terms (last accessed Apr. 28, 2020) [https://perma.cc/T289-8CPZ].

which is used to produce a final service. It is this final service which consumers value, some more than others.[73]

Much conceptual work needs to be done on privacy as a form of competition. For example, data sharing could be viewed as the "price" that users pay for personalization of a service.[74] It could also be thought of as a form of labor or an asset that users provide to companies for which compensation is needed.[75] These conceptualizations need to be explored more fully and their place in merger reviews should be better understood.

In the meantime, a step toward conceptual clarity might come from rethinking the idea of privacy as an objective improvement in a product or service. It might be more useful to recognize that the value consumers place on privacy is subjective. Moreover, to understand the nature of privacy competition, it might be helpful in merger reviews to think of data collection and use as an input to the personalization of a service. Companies compete along this privacy-personalization frontier, offering consumers not simply more privacy or less privacy but a bundled choice of more privacy and less personalization or more personalization and less privacy. The preferences of consumers for these bundles then have to be assessed empirically as part of a merger review.

F. Empirical Requirements

This recognition that privacy preferences differ, in part because privacy comes bundled with personalization services, has important implications for the assessment of privacy competition in merger reviews. In particular, it implies that an observed difference in data practices cannot be assumed to reflect different levels of consumer value. Changes in consumer welfare resulting from changes in data practices have to be assessed empirically by assessing actual consumer preferences.

It is possible that changes in company data practices following a merger might constitute a significant consumer harm. However, this cannot be assumed as a matter of definition any more than—to use Cooper's example in a merger context—it could be assumed that a restaurant's post-merger

---

73. In his classic article, Richard Posner thinks of privacy and prying as intermediate goods, leading to other things that people value rather than valued for their own sake: "We could regard them purely as consumption goods, the way economic analysis normally regards turnips or beer; and we would then speak of a 'taste' for privacy or for prying. But this would bring the economic analysis to a grinding halt because tastes are unanalyzable from an economic standpoint." Richard A. Posner, *The Right of Privacy*, 12 GA L. REV. 393, 394 (1977). Farrell also thinks of the possibility of privacy as an intermediate good, when, for example, he mentions that withholding information can protect people from adverse decisions in credit and employment. But his model focuses on the marginal case of companies who collect data for no reason related to the customization of a service or its supporting adverting. *See* Farrell, *supra* note 67.

74. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 52, PublicAffairs (2018) (attributing to tech companies the view, which she criticizes, that privacy is "the price one must pay for the abundant rewards of information, connection, and other digital goods when, where, and how you want them.").

75. *See, e.g.*, Imanol Arrieta Ibarra et al., *Should We Treat Data as Labor? Moving Beyond 'Free'*, 1 AEA PAPERS & PROCEEDINGS, 1 (May 2018).

decision "to replace corn with green beans on its menu" would constitute a consumer harm that needs to be assessed in a merger review.[76]

Even if privacy is conceptualized as an increase in product quality, the size of the increase must be assessed empirically. As the European Commission competition officials said after outlining their view of data collection as intrinsically harmful: "However, while technically viable, this theory of harm could only be relevant in those cases where privacy is an important factor in the decision to purchase a product or service, i.e. a key parameter of competition."[77] That is, even if merger reviewing authorities assume that increased data collection degrades product quality, there still remains the empirical question of how large this effect might be.

Swire recognizes this point as well. About the Google/DoubleClick merger, he says:

> If the merger is approved, then individuals using the market leader in search may face a search product that has both "deep" and "broad" collection of information. For the many millions of individuals with high privacy preferences, this may be a significant reduction in the quality of the search product—search previously was conducted without the combined deep and broad tracking, and now the combination will exist. I am not in a position to quantify the harm to consumers from such a reduction in quality.[78]

Let me emphasize that in this quotation Swire says that a merger creating more data collection "may be a significant reduction in the quality" of the product. He is not arguing that the merger would create this harm, merely that it is possible. In order to be considered in a merger review, such possible harm has to be demonstrated as actual and its size estimated.

Even if privacy is thought of as an increase in quality, it still might be that these differences in quality are too small to affect consumer behavior. A market investigation must assess and confirm that "privacy is an important factor in the decision to purchase a product or service."[79]

The FTC did such an assessment in its Google/DoubleClick merger review.[80] Despite its view that the prevention of harm to competition is the sole aim of merger review, the FTC also "investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as

76. Cooper, *supra* note 61, at 1138.
77. Ocello et al., *supra* note 54, at 6.
78. Swire, *supra* note 4, at 6-7.
79. Ocello, *supra* note 54, at 6.
80. FTC Statement, Google/Doubleclick, *supra* note 3, at 2-3.

consumer privacy." It "concluded that the evidence does not support a conclusion that it would do so."[81]

To determine that privacy is an important parameter of competition, it is necessary to assess whether a significant number of people base market choices on their privacy preferences. Universality is not needed. As one commentator says: "[I]t seems unreasonable to conclude that protecting competition over privacy would require a finding that consumers are unanimous in their preference for additional privacy protections."[82] When large numbers of people make their decisions about the goods or services that they buy on the basis of the privacy practices of the companies involved, then privacy is a "key" or "important" parameter of competition in those markets.

The way to ascertain the value of privacy for merger review purposes is through consumer surveys or interrogation of the expert opinion of those involved in the marketplace and have experience in seeking to meet consumer demand as it manifests itself in consumer behavior.[83] Expert opinion might be preferable to asking people specific hypothetical questions about their preferences in connection with the merged company's data practices. Surveys in this area are especially unreliable, as the privacy paradox phenomenon shows.[84]

As described in the two case studies in Sections III and IV, obstacles to an accurate empirical assessment of the role of privacy in marketplace competition are formidable.[85] But if merger reviews are ever to be a reliable mechanism to address privacy concerns, they have to be faced and overcome.

G. Privacy Competition Can Be Reduced After a Merger in Several Different Ways

Consumer harm can take the form of a post-merger failure to satisfy consumer privacy preferences that were satisfied before the merger. And in

---

81. The extent to which this was a detailed, empirical investigation of whether privacy was an element of competition between Google and DoubleClick is unclear. It might have just been fall-out from the Commission's general conclusion that Google and DoubleClick did not compete at all: "Because Google and DoubleClick do not presently compete in the same relevant market these two companies do not act as significant competitive restraints on one another. In practical terms, this means that the parties do not significantly affect each other's prices, nor non-price product attributes, such as consumer privacy protections or service quality." *Id.* at 8, n.7.

82. Keith Waehrer, *Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions* 10 (Media Democracy Action Fund, Working Paper, August 21, 2018), http://waehrer.net/Merger%20effects%20in%20privacy%20protections.pdf [https://perma.cc/W4X5-P44V].

83. OECD Quality Report, *supra* note 56, at 6-7. The report also suggests the possible use of hedonic price techniques that are commonly used in econometric studies to adjust prices for quality changes in order to compare the value of products whose quality has improved such as color TVs or automobiles with automatic brakes. They note data difficulties in putting this approach into practice.

84. *See Id.*

85. *See* Sections III and IV, infra.

some circumstances, this can be a cognizable consumer harm that needs to be addressed in merger reviews.

A diminution of privacy competition post-merger could take place a variety of ways. One would be a merger in which a company with weak privacy protections takes over a company with strong privacy protections and reduces these protections after the merger. Some analysts seem to think that this cannot be a problem because a company that provides weak privacy protection does not compete with a company that provides strong privacy protection.[86] They are not in the same market of aiming to satisfy consumer privacy preferences and so a merger cannot result in any consumer harm.[87]

Stucke and Grunes rightly point out that consumers who are dissatisfied with the privacy features of one company rarely go looking for another company with poor privacy protection.[88] If consumer preferences for privacy are important in the market, "privacy is a dimension on which (companies) are competing, whether they offer a lot of protection for the data or a little."[89] Indeed, given the bundled nature of personalization and privacy described earlier, it is hard to see how companies could fail to compete.

As a result, the failure to satisfy consumer privacy preferences post-merger could be a real consumer harm that is properly subject to assessment in merger review, even when one of the companies has no interest in protecting privacy beyond what is legally required. As we will see, this was an important issue in the Facebook/WhatsApp merger.

A fact pattern similar to that in the abuse of dominance case brought by Germany's Federal Cartel Office (FCO) against Facebook might also arise in a merger context.[90] In its case, the FCO observed Facebook's practice of requiring users to accept, as a condition of using Facebook, the collection of information about their use of third-party and affiliated services and the combination of this information with the information about their use of the Facebook service itself.[91] The FCO said that this practice was both a violation of European privacy law and a violation of German competition law.[92]

The FCO said that this practice was a violation of the General Data Protection Directive—specifically, its requirement that Facebook must have a legal basis for the collection and use of personal information.[93] Because Facebook occupies a dominant position in the social media marketplace, the legal basis for data collection cannot be consent because consent has to be voluntary and the lack of genuine alternatives to Facebook means that

---

86. Darren S. Tucker, for instance, argues that a merger will adversely affect privacy choices only "where privacy is an important element of competition and the merger is between two firms that offer stronger privacy protections than most other rivals." Darren S. Tucker, *The Proper Role of Privacy in Merger Review*, 7 *CPI Antitrust Chronicle*, (2015), https://www.competitionpolicyinternational.com/assets/Uploads/TuckerMay-15.pdf.

87. *Id.*

88. *See* STUCKE & GRUNES, *supra* note 5, at 131.

89. *Id.*

90. *See Case Summary: Facebook*, *supra* note 14.

91. *Id.* at 1.

92. *Id.* at 7.

93. *Id.* at 10.

Facebook users cannot give genuine consent to data collection.[94] Moreover, the third-party and affiliate data collection cannot be based on contractual necessity, since the collection of this extra data is not necessary for the provision of Facebook service.[95] Finally, the data collection cannot be based on Facebook's legitimate interests because the extent of the data collection so far exceeded the reasonable expectations of Facebook's users that only marketplace dominance could explain why users accepted it.[96]

In addition, the FCO asserted that the collection and combination of third-party data was a competition problem because the resulting profiles, which can exist only because of Facebook's abuse of its dominant position, gave it an unfair and insuperable advantage in the advertising marketplace.[97] In effect, the FCO asserted that the combined data set does not leave enough data left over for advertising rivals to function effectively.[98]

The FCO proposed what is essentially a data protection remedy. Facebook must allow its users a separate choice in connection with third party and affiliate data collection and combination that would enable them to refuse this collection and combination of data and still be able to use the Facebook social media service.[99] Failing that, it may continue to collect third-party and affiliate data from its users, but it may not combine them together with organic Facebook data to create a single user profile.[100]

This fact pattern can be reimagined as a merger circumstance, in which a social media company seeks to merge to a position of dominance through the acquisition of another social media company with pro-privacy data practices. The merged entity might change the pro-privacy practices of its acquired company, thereby depriving its users of their previous pro-privacy choice. The merged entity's dominance in the social media market prevents these users from moving to a viable alternative, and so the loss of privacy choice is a direct result of the loss of competition.

A merger could harm privacy competition in a different way. If a firm aiming to provide strong privacy protections merges with the only other firm

---

94. *Id.*

95. *Id.* The competition authority conceded that the collection of data from the use of its own service is necessary for the provision of Facebook's service, despite the existence of theoretical alternatives such as user fees or non-targeted advertising support. For this reason, the FCO did not require Facebook to rely on voluntary consent as a legal basis for data collection, which might be vitiated by Facebook's dominant marketplace position. Presumably, it would accept contractual necessity as the legitimate basis for Facebook's collection and use of data on its own service. In any case, it interposed no objections to Facebook requiring, as a condition of using the Facebook service at all, that users accept virtually unlimited data collection about their activities on Facebook's own social media service.

96. *Id.* at 10-11; Düsseldorf Decision, *supra* note 14, at 26 (criticizing the aspect of the FCO decision saying that inattention or indifference might also lead users to accept this level of data collection).

97. *Case Summary: Facebook*, *supra* note 14, at 11.

98. *Id.* at 11. This raises the question why it did not prohibit combining third-party data with Facebook's own data, rather than independent consent to that linkage of data. The harm to competition in the advertising market would seem to arise from the existence of the profiles rather than from the fact of their construction through take-it-or-leave it consent.

99. *Id.* at 12.

100. *Id.*

also aiming to provide strong privacy protections, the merged company might, under certain conditions, be able to reduce privacy protections for its customers without fear of retaliation from other companies.[101] This would provide an interesting case for competition authority to review, but to my knowledge no such case has arisen yet in practice.

A third way privacy competition could be adversely affected by a merger might arise if the acquiring company has a dominant position in a separate market related to the market in which its target competes. The merged entity might then be able to use this dominant position in the related market to advantage its new acquisition against its rivals. When the new acquisition provides less privacy protection than its rivals in the related market, the result might be the foreclosure or marginalization of competitors who provide better privacy protection. This is the fact pattern that arose in the Microsoft/LinkedIn merger review.[102]

H. Consumer Harms Connected to Privacy Are Cognizable in Merger Analysis Only If They Result from a Lessening of Competition

Even if privacy preferences are an important element of competition in the marketplace and even if the merged company would not satisfy them, a review should not necessarily block or condition a proposed transaction. It is not enough to show that a merger leaves some consumer preferences for privacy unsatisfied compared to the market situation before the merger. The privacy loss has to result from the loss of competition.

This is a very general point. Consumer harm counts in merger reviews only if the harm results from a lessening of competition post-merger. Consumer preferences that are no longer satisfied after a merger count as a cognizable merger harm only if the post-merger failure to satisfy them is related to some defect of competition.

The DOJ Merger Guidelines are explicit on this point. They say that a merger "enhances market power if it is likely to encourage one or more firms to raise price, reduce output, diminish innovation, or otherwise harm customers *as a result of diminished competitive constraints or incentives*."[103]

The DOJ Guidelines note that a merged firm might withdraw a product that a significant number of people value.[104] But they add that if there is evidence that this has happened, "the Agencies may inquire whether the reduction in variety is largely due to a loss of competitive incentives attributable to the merger."[105] The reason for making this additional attribution inquiry is that:

---

101. Tucker, *supra* note 56, at 5.
102. *See* EU Commission Decision, Microsoft/LinkedIn, *supra* note 7.
103. DOJ 2010 Merger Guidelines, s*upra* note 17, at 2 (emphasis added).
104. *Id.* at 24.
105. *Id.*

> Reductions in variety following a merger may or may not be anticompetitive. Mergers can lead to the efficient consolidation of products when variety offers little in value to customers. In other cases, a merger may increase variety by encouraging the merged firm to reposition its products to be more differentiated from one another.[106]

The DOJ Merger Guidelines consider the circumstance in which two actual or potential competitors merge. When that happens, of course, they no longer compete with each other. Following such a merger, there might be consumer harm such as a price increase or unsatisfied consumer preferences. But the reviewing agency can consider those post-merger consumer harms only when they "result directly from the loss of that competition."[107]

Some examples illustrate the point. Color might be an important dimension of car competition and a merged car company's decision to stop making yellow cars might leave some consumers unsatisfied. But if the merged company's decision is based on a market assessment of demand, or even if it is just based on the whim of the new owners, there is nothing merger review should do to stop this. The merger review might reach a different conclusion if the merger would change competitive conditions so that the merged car company faces substantially lessened competition, which might be the case in a merger to monopoly. Then the company's decision to stop making yellow cars would be predicated on its understanding that in the post-merger world it will not face any competitive response.

To take another example, suppose credit card company American Express seeks acquiring rival Visa and vows that at the end of the transaction Visa will no longer accept transactions for porn merchants. American Express has long had a policy of not accepting the business of porn merchants, because it seeks to preserve what it views as an attractive brand and valuable business image. After the merger, it wants to extend this branding policy to its new acquisition. As a result, some customer preferences will be frustrated after the merger, both on the merchant side and on the cardholder side. Nevertheless, according to DOJ Guidelines, antitrust authorities should be indifferent to this consumer harm as long as there is sufficient competition in the market so that another payment company seeking to gain market share is free to pick up those disgruntled porn merchants as customers. If the loss in consumer satisfaction derives from a newly created dominant position, however, rather than from a branding preference of the acquiring company, then it is cognizable by the merger reviewer, but not otherwise.

The same reasoning applies to a reduction of privacy alternatives after a merger, even when consumers make marketplace choices in large measure on the basis of privacy. It is not enough to show that a merged company might end the pro-privacy practices of an acquired rival by merging. It is also not enough to show that a merged company might be able to defeat a rival that offers its customers more privacy protection. These results have to be the

106. *Id.*
107. *Id.* at 3.

consequence of some reduction of competition in the post-merger market. If there would continue to be plenty of rivals in the market, if entry and expansion in the market would remain inexpensive and easy, and if network effects would pose no extraordinary barriers to entry or expansion, then there would be no lessening of competitive conditions after the merger. In the presence of these competitive conditions, especially if privacy is truly an important dimension of competition in that market, a company that did not provide the privacy that many customers want would almost certainly face a strong competitive response. Actual or potential rivals would be able to provide it without facing anticompetitive barriers, and, especially if privacy preferences are strong, they would have every incentive to step forward to provide it.

Swire understands the need to connect any consumer harm in a merger analysis to some failure of competition: "Possible harm to product quality, due to monopoly power, has been clearly recognized in the courts."[108] As a result, even if the "broadening and deepening" of information collection following the Google/DoubleClick merger is accepted as a consumer harm, a reviewing agency has to ask, so what?[109] If the consumer harm—failure to satisfy some consumer preferences, who nevertheless continue to use the product—is not caused by a lack of competition, then the merger review cannot reach it.

In a similar way, Stucke and Grunes understand that a reviewing agency might want to object to a hypothetical Facebook/WhatsApp transaction where it has the effect of eliminating all viable texting choices where privacy is protected.[110] But, as they also point out, this objection can only have force in a merger review where the loss of these choices is "because of entry barriers and network effects" that result in a "lessening of competition."[111] The key is that the elimination of choice derives from failure of competitive conditions due to entry barriers and network effects, not simply from the decision of the merged entity to increase data collection. As we will see later, the European Commission approved the Facebook/WhatsApp merger, even if Facebook would have eliminated WhatsApp's privacy protective business model, because it found plenty of suppliers in the marketplace for communications apps, no substantial entry or switching barriers, and weak network effects.

It is sometimes easy to forget this added burden in merger reviews. Stucke and Grunes raise the possibility of a hypothetical Google/DuckDuckGo merger and say correctly that a key issue in a merger review "would be the degradation in privacy protection post-merger."[112] But they do not focus on the more critical question of whether the loss of DuckDuckGo's privacy protective business model derives solely from a business decision of the new owner or whether it is an exercise of newly-formed market power deriving from the merger itself.

---

108. Swire, *supra* note 4, at 6.
109. *Id.*
110. STUCKE & GRUNES, *supra* note 5, at 265.
111. *Id.*
112. *Id.* at 266.

This need to trace consumer harm to a loss of competition requires a substantial showing, as is revealed by considering what would have to be established to condition or block a Google/DuckDuckGo merger. DuckDuckGo has a one percent market share; its search technology differs from Google's, and it has generated profit every year for the last five years by selling contextual ad services that do not track its users.[113] Even if Google acquired the company and ended its pro-privacy practices, a merger review that follows the DOJ Guidelines would have to show that the resulting lack of competitive conditions would prevent other companies from replicating these elements of a successful business model to meet the frustrated demand of people for whom DuckDuckGo's privacy practices were attractive.[114] With that showing, the merger could possibly be blocked or conditioned, but not without it.

To see how privacy-aware merger reviews work in practice and to derive some lessons for the future, the rest of this Article looks carefully at the European Commission's reviews of the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger. The questions we will be examining in the assessments that follow include whether the merger review considered the differences in privacy practices and, if it did, whether it rejected or conditioned the merger on the basis of these differences. An additional and crucial question is whether the conditions imposed directly or indirectly served to maintain the pro-privacy practices that were at risk in the merger.

III. FACEBOOK/WHATSAPP

In 2014 the European Commission conducted a review of the proposed Facebook merger with the messaging service WhatsApp.[115] Facebook controlled its own competing communications app, Facebook Messenger.[116] The Commission reviewed the possible loss of competition in the social media market,[117] in the communications app market,[118] and in the online advertising market,[119] and approved the merger without conditions.[120]

A key issue in the merger review was one of the possibilities of privacy and antitrust overlap discussed earlier, namely, that the merger would create an excessive concentration of commercially valuable data.[121] Despite its general statement in the decision that privacy issues as such belonged with the data protection authorities, the Commission nonetheless reviewed these

---

113. Nathaniel Popper, *A Feisty Google Adversary Tests How Much People Care About Privacy*, N.Y. TIMES (July 15, 2019), https://www.nytimes.com/2019/07/15/technology/duckduckgo-private-search.html [https://perma.cc/PF6U-TXBB].

114. DOJ 2010 Merger Guidelines, *supra* note 17, at 3.

115. *See* EU Commission Decision, Facebook/WhatsApp, *supra* note 6.

116. *Id.* at par. 4.

117. *Id.* at pars. 143-63.

118. *Id.* at pars. 84-142

119. *Id.* at pars. 164-190.

120. *Id.* at par. 191.

121. *Id.* at par. 164.

data issues.[122] It considered whether the combination of Facebook and WhatsApp user data sets could create a data monopoly.[123] It found that there would be plenty of data left over after the merger for competitors: "[R]egardless of whether the merged entity will start using WhatsApp user data to improve targeted advertising on Facebook's social network, there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control."[124]

In addition, and as a separate matter, the Commission extensively considered the role of privacy as an element of competition. It started by recognizing that: "[C]ontrary to WhatsApp, Facebook Messenger enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities."[125] It noted that it was a deliberate choice for WhatsApp to build its business "around the goal of knowing as little about [users] as possible."[126] Also, the Commission said that while the importance of privacy and security "varies from user to user . . . [they] are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues . . . ."[127]

In particular, the Commission observed that besides WhatsApp, two other messaging services, Threema and Telegram, were more protective of privacy than Facebook Messenger.[128] It further noted that privacy concerns "seem to have prompted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp."[129] And it also noted that "after the announcement of WhatsApp's acquisition by Facebook and because of privacy concerns, thousands of users downloaded different messaging platforms, in particular Telegram, which offers increased privacy protection."[130] In sum, while not a "maverick" in the marketplace, WhatsApp provided "behavioural ads."[131]

So, the Commission, while not taking privacy as such into account, spent a significant part of its merger review on observing different privacy practices present in the market. Still, the Commission did not conclude that these differences in privacy practices were an important element in the

---

122. *Id.*

123. *Id.*

124. *Id.* at par. 189.

125. *Id.* at par. 102.

126. EU Commission Decision, Facebook/WhatsApp, *supra* note 6. *See also* par. 169: "WhatsApp does not allow ads because it believes that they would disrupt the experience that it wants to deliver to its users." This rejection of ads is not quite the same as a pro-privacy practice, since non-targeted ads do not rely extensively on user data.

127. *Id.* at par. 87.

128. *Id.* at par. 90, 128 (par. 90 for Threema "increased security of communications" and par. 128 for Telegram).

129. *Id.* at par. 174.

130. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, n. 79.

131. STUCKE & GRUNES, *supra* note 5, at 133. In this way, WhatsApp satisfied the DOJ's "disruptive role" condition of a company able to "disrupt market conditions with a new technology or business model" whose merger with a market incumbent "can involve the loss of actual or potential competition." DOJ 2010 Merger Guidelines, *supra* note 31, at Introduction.

competition between the merging messaging services.[132] It found instead that privacy was just like some of the other relatively minor differences between Facebook and WhatsApp.[133]

These minor differences included the contrasting identifiers used to access the services and the different sources of the contact information used to connect users.[134] Price was a differentiator as well. While most apps were provided for free, Threema charged a subscription fee, as did WhatsApp in some markets.[135]

These contrasting features, including the privacy differences, were real ways in which the services differed, but they were not key factors driving competition in that marketplace, not the main or the paramount basis for consumer choice of communications app.

The Commission concluded instead that, in general: "[T]he main drivers of the competitive interaction between consumer communications apps appear to be (i) the functionalities offered and (ii) the underlying network."[136] It found that the competition between Facebook and WhatsApp also turned on these same two factors: communications functionalities offered and network size.[137] In particular, the size of the network seemed of crucial importance to a typical user since it increases "the number of people he or she can reach."[138]

Moreover, the Commission observed that WhatsApp users did not seem to reject Facebook's privacy practices. The Commission noted: "[B]etween [70-80]% and [80-90]% of WhatsApp users were Facebook users and were therefore already within the reach of Facebook Messenger."[139] If WhatsApp users were genuinely put off by Facebook's privacy practices, so much so that they would prefer to use WhatsApp instead, why were up to 90% of them Facebook users?

Stucke and Grunes wonder why a Facebook user would avoid Facebook Messenger and use WhatsApp instead.[140] Why not just use Facebook Messenger? They speculate that these Facebook users wanted the greater WhatsApp privacy protections.[141] But an alternative possibility is that these users needed WhatsApp to reach the people they wanted to be in touch with who were not Facebook users, and they had no need of the additional people they could reach on Facebook Messenger. So, the Commission concluded

---

132. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 87.

133. *Id.*

134. *Id.*

135. *Id.* at par. 90.

136. *Id.* at par. 86.

137. *Id.* at par. 103.

138. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 129. Stucke and Grunes recognize this primacy of network: "In choosing a texting app, the primary consideration, given the network effects, is whether their friends, family, and acquaintances use the app." STUCKE & GRUNES, *supra* note 5, at 131.

139. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 140.

140. STUCKE & GRUNES, *supra* note 5, at 132.

141. *Id.*

privacy was not a "main" driver of competition in the consumer communications market.[142] It found, moreover, that the merger would not significantly impede effective competition in that communications market.[143]

The proposed transaction would increase the combined company's market share to as much as 40%, with the rest spread among smaller providers.[144] But the Commission also found that, due to substantial overlap of their user base, Facebook Messenger and WhatsApp were more like providers of complementary services than close competitors.[145] So, the merger did not really a diminish existing competition.

It also found that there would be many alternative providers after the merger for users to easily choose,[146] that there were no significant barriers to entry,[147] and that network effects would not seriously hinder competitor expansion or entry,[148] even if Facebook integrated its Messenger service with WhatsApp.[149]

The results of the merger have not been what privacy advocates might have hoped. At the time of the merger, WhatsApp founder Jan Koum said: "Here's what will change for you, our users: nothing."[150] However, in 2016 things began to change. WhatsApp began to share information with Facebook about WhatsApp users, including a user's phone number, last seen data, operating system, mobile country code, mobile carrier code, screen resolution, and device identifier.[151] Two years later, Facebook clarified that WhatsApp would join Facebook, Instagram, and Messenger as an app that advertisers could use to reach their intended audience. These actions triggered the resignation of the WhatsApp founders from Facebook.[152] In May 2019, Facebook announced that the first ads would begin to appear on WhatsApp in 2020.[153]

One result of the merger, then, is that WhatsApp's pro-privacy practices have largely been replaced with the less protective but still legal data collection and use practices typical of the rest of the Facebook product family.

---

142. *Id.* at par. 86.
143. *Id.* at par. 142.
144. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 96.
145. *Id.* at pars. 101-107.
146. *Id.* at par. 109.
147. *Id.* at par. 117.
148. *Id.* at par. 135.
149. *Id.* at par. 140.
150. WhatsApp Blog, WHATSAPP (Feb. 19, 2014), https://blog.whatsapp.com/499/Facebook? [https://perma.cc/5L48-399R].
151. Natasha Lomas, *WhatsApp to Share User Data With Facebook for Ad Targeting — Here's How to Opt Out*, TECHCRUNCH (Aug. 25, 2016), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/ [https://perma.cc/U9UA-R5AX].
152. Deepa Seetharaman, *Facebook's New Message to WhatsApp: Make Money*, WALL ST. J. (Aug. 1, 2018), https://www.wsj.com/articles/facebooks-new-message-to-whatsapp-make-money-1533139325?mod=rss_Technology [https://perma.cc/RY96-A5LD].
153. Anthony Cuthbertson, *Whatsapp: Adverts Coming to Messaging App Next Year, Facebook Reveals*, INDEPENDENT (May 28, 2019), https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-adverts-update-new-advertising-when-a8933131.html [https://perma.cc/WKN6-ZLV7].

This result might seem to be a step backwards in privacy protection, perhaps attributable to a mistake in the merger review process.

Is it the case, for instance, that the approval was dependent on misleading information that Facebook provided to the Commission during the review? It is true that Facebook faced disciplinary action from the Commission for providing misleading information during the merger review.[154] It was, in fact, able to automatically match users who had both the Facebook app and the WhatsApp app installed on their phones, using the phone's unique code as a common identifier.[155] Facebook, however, had not disclosed this possibility to the Commission during the merger review, even though it had developed such a matching system for Facebook and Instagram, and was working to implement it for WhatsApp after the merger.[156] Facebook admitted that it had negligently provided incorrect or misleading information to the Commission during the merger review.[157] The Commission fined it €110 million.[158]

But the Commission did not change its decision about the legitimacy of the merger even knowing about the ease with which Facebook could merge Facebook and WhatsApp data and it would not have made a different decision if it had been told the truth.[159] It had evaluated the merger based on the assumption that Facebook would be able to merge the data sets after the merger and it still found that the merger did not substantially lessen competition.[160] It said that if Facebook managed to integrate WhatsApp and Facebook data despite apparent technical difficulties, it would "pose a business risk" because "users could switch to competing consumer communications apps."[161] That is, there was still plenty of competition available so that users who wanted to switch to privacy-protective communications apps would be able to do so.[162]

The change in WhatsApp privacy practices after the merger could perhaps be reached by consumer protection law. At the time of the merger, the United States FTC sent a letter to Facebook, saying:

---

154. European Commission, Case No. COMP/M.8228, Facebook/ WhatsApp, 2017 O.J. (C 286). http://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf [https://perma.cc/N7M2-MJ7H].

155. *Id.* at pars. 49-51.

156. *Id.* at par. 86.

157. *Id.* at pars. 41-42.

158. *Id.* at par 108.

159. *Id.* at par 100.

160. *Id.* at pars 27-29.

161. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 139.

162. *Id.*

> WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties – promises that exceed the protections currently promised to Facebook users. We want to make clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to consumers. Further, if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the Federal Trade Commission (FTC) Act and, potentially, the FTC's order against Facebook.[163]

The FTC has not taken any such consumer protection enforcement actions, but there is clearly a remedy available for companies who mislead the public and their consumers about their data practices. That might be a more productive avenue to pursue to reverse changes in WhatsApp privacy practices post-merger, rather than reopening the merger decision to address privacy issues.

There might have been some mistakes in the European Commission's review of the proposed merger.[164] But the Commission's judgment at the time of the merger that privacy was not a crucial element of competition between Facebook and WhatsApp seems reasonable, even today. At the time of the review, there was no compelling evidence that WhatsApp's pro-privacy practices were a distinguishing feature of communications app competition.[165] Functionality and user base seemed to be the key elements of competition, not privacy.[166] The merger review reasonably avoided blocking or conditioning the merger on the basis of a likely threat to reduce privacy competition.

---

163. *See* Letter from Jessica L. Rich, Bureau of Consumer Protection Director, FTC, to Erin Egan, Chief Privacy Officer, Facebook, and Anne Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer [https://perma.cc/8Y7G-N4Z4]. The FTC has not taken any consumer protection enforcement actions against Facebook for changes in WhatsApp's data practices, including in the recent settlement for violations of the earlier FTC order. *See* Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/UY7L-U4LG].

164. There might be other competition reasons for revisiting the merger such as a dramatic increase in the market share of the combined company that perhaps could reasonably have been foreseen at the time, and the possibility that absent the merger WhatsApp would have emerged as a formidable competitor to Facebook in one or more of the relevant markets. *See also, e.g.*, Mark Glick & Catherine Ruetschlin, *Big Tech Acquisitions and the Potential Competition Doctrine: The Case of Facebook Institute for New Economic Thinking* (Inst. for New Econ. Thinking, Working Paper No. 104) https://www.ineteconomics.org/uploads/papers/WP-104-Glick-and-Reut-Oct-10.pdf [https://perma.cc/LX49-KYDL]. But that is independent of the role of privacy as an element of competition.

165. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par 86.

166. *Id.*

IV. MICROSOFT/LINKEDIN

In 2016, the European Commission reviewed the proposed Microsoft/LinkedIn merger.[167] After determining that the merger posed a risk of competitive harm in the market for professional social networks, it accepted Microsoft's commitments in the area of pre-installation and integration with Microsoft's other products and approved the merger with these conditions.[168]

The Commission assessed the possibility of a data monopoly emerging from the sharing of data between Microsoft and LinkedIn.[169] The Commission concluded that there would be no dearth of data for competitors after the merger: "[T]he combination of their respective datasets does not appear to result in raising the barriers to entry/expansion for other players in this space, as there will continue to be a large amount of internet user data that are valuable for advertising purposes . . . not within Microsoft's exclusive control."[170]

Separately and independently, the Commission also assessed the state of privacy competition in the market. Its conclusion on privacy competition in this case was different:

> Privacy related concerns as such do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction.[171]

The Commission determined that Xing, a professional social network competing with LinkedIn in Germany and Austria, "seems to offer a greater degree of privacy protection than LinkedIn."[172] Xing had a separate box to tick to accept its privacy policy, while LinkedIn users automatically accepted its privacy policy when they pressed the "join now" button.[173] Moreover, Xing sought active user consent for new policies and allowed users to continue to use the service regardless of their choice.[174] In contrast, LinkedIn notified users of its privacy policy changes and assumed consent if they continued to

---

167. *See* EU Commission Decision, Microsoft/LinkedIn, *supra* note 7.

168. *Id.* at par. 470.

169. *Id.* at pars. 176-180.

170. *Id.* at par. 180.

171. European Commission, press release of Dec. 6, 2016, Case M.8124, Microsoft/LinkedIn, (Microsoft Press release) https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284 [https://perma.cc/PUJ5-WP34].

172. EU Commission Decision, Microsoft/LinkedIn, *supra* note 7, at par. 350.

173. *Id.*

174. *Id.*

use the service.[175] The Commission found that these differences were important in determining consumer choice: "[P]rivacy is an important parameter of competition and driver of customer choice in the market for (professional social network) services . . . ."[176]

This conclusion on the strength of privacy competition was mentioned in the Commission's determination of a potential competition problem with the merger.[177] The Commission was concerned that Microsoft after the merger could use certain integration and pre-installment practices in connection with its newly acquired LinkedIn app to foreclose competition in the market for professional social networks.[178] This foreclosing of competition would reduce consumer choice for their preferred social network.[179] But it would also prevent consumers from choosing the professional social network that would best protect their privacy. As the Commission put it:

> [T]o the extent that these foreclosure effects would lead to the marginalisation of an existing competitor which offers a greater degree of privacy protection to users than LinkedIn (or make the entry of any such competitor more difficult), the Transaction would also restrict consumer choice in relation to this important parameter of competition when choosing a [professional social network].[180]

To remedy that potential foreclosure problem, the Commission solicited and accepted 5-year commitments from Microsoft restricting their conduct in connection with integrating and pre-installing the LinkedIn app.[181] With these commitments, the Commission cleared the merger.[182]

How did the Commission reach its conclusion on privacy competition? How did it use that conclusion in its final decision and remedy?

The Commission provided an analysis of the market for professional social network services, distinguishing that market from personal social networks such as Facebook, from more specialized professional social networks such as Academia, and from closed social networks such as those limited to a particular enterprise.[183] It identified the other marketplace participants, XING, Viadeo, and GoldenLine,[184] and listed their market shares.[185] The Commission noted the "essential" functionalities that all competing professional social networks must and do have, including: "the creation and update of a CV, searching for jobs, receiving alerts and ads about jobs, and asking to be introduced to new contacts through a common

175. *See id.*
176. *Id.* at n.330.
177. *Id.* at par. 350.
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.* at par. 470.
182. *See id.*
183. *See id.* at par. 115.
184. *Id.* at par. 108.
185. *Id.* at par. 285-286.

connection."[186] But it did not include disclosing its privacy protections as one of these essential functionalities.

It is unclear from the Commission's account what the evidence was for its conclusion that privacy was an "important parameter" in the competition between LinkedIn and Xing, as opposed to just a relatively minor difference between the social networks that did not determine consumer choice.[187] It cited only the "results of the marketplace investigation" and some questions in a survey distributed to social networks.[188]

This lack of detail is disappointing. Moreover, the finding is implausible on its face. Would a person seeking a quality professional social network really base the decision in whole or in substantial part on the basis of the opt-in or opt-out choice structure for data sharing and policy updates described by the Commission? In addition, if privacy was such a major element of competition, why didn't the Commission list a privacy policy as one of the essential functionalities that a professional social network must provide?

To this point, business press accounts of the rivalry between LinkedIn and Xing, its main competitor in German-speaking countries, make no mention of privacy differences, providing some evidence that consumers do not view privacy as a major element of competition.[189] These accounts suggest that a contrast between local and international focus seems to be the key to consumer choice, not privacy.[190] Xing is most compatible with local culture and styles in German-speaking countries, while LinkedIn is more connected with global networks. Privacy does not figure in the rivalry in these accounts at all. If privacy is such a driver of competition in this market, why don't the industry accounts of competition between LinkedIn and Xing in Germany mention it?

As a separate matter, it is hard to interpret the Commission's perplexing assertion that their conclusion on privacy competition in Microsoft/LinkedIn dovetails with their finding in the Facebook/WhatsApp case: "The finding of the importance of privacy as parameter of competition is consistent with the Commission's findings in Facebook/WhatsApp . . . in relation to consumer communication services."[191]

As we saw, the WhatsApp decision clearly says that: "The only factors on the basis of which WhatsApp and Facebook Messenger were considered close competitors . . . are the communications functionalities offered and the

---

186. *Id.* par. 102.

187. *Id.* at n.330.

188. *Id.*

189. *See* Shelley Pascual, *The career-oriented social networking site LinkedIn is growing faster than its main competitor, Xing. What has it been offering professionals to account for this growth?*, THE LOCAL (Feb. 1, 2018), https://www.thelocal.de/20180201/goodbye-xing-the-success-of-linkedin-in-germany [https://perma.cc/8HTB-RZWA];Top Dog Social Media, *LinkedIn vs. Xing: The Battle for DACH*, 2018, https://topdogsocialmedia.com/linkedin-vs-xing/ [https://perma.cc/Y3RP-CMX6].

190. *Id.*

191. EU Commission Decision, Microsoft/LinkedIn, *supra* note 7, at 77 n.330.

size of their respective networks."[192] And the Commission in that case determined that privacy was not a "main" driver of competition.[193]

Moreover, expert commentary two years after the Microsoft/LinkedIn decision from Commission officials who were close to both decisions presents a clear contrast between the conclusions in the two cases:

> For example, in *Facebook/WhatsApp*, in 2014, the Commission found that, while an increasing number of users valued privacy and security, at that time the majority of consumer communications apps (e.g. Facebook Messenger, Skype, WeChat, Line, etc.) did not (*mainly*) compete on privacy features. When reviewing *Microsoft/LinkedIn* in 2016, the Commission found that privacy was an *important* parameter of competition among professional social networks, in particular in certain EU Member States, such as Germany.[194]

So, according to these Commission experts, the Commission found in the Facebook/WhatsApp case that privacy was not a "main" driver of competition and found in the Microsoft/LinkedIn case that privacy was an "important" driver of competition.[195]

The Commission seemed to be going to extraordinary lengths to make their disparate conclusions seem consistent. It is hard to see the motivation for this. It is reasonable, even likely, that privacy will be a more important driver of competition in one market than in another. There is no need to impose an artificial consistency between the two cases.

In any case, the finding of privacy as an important driver of professional social network competition was not a determinant of the Commission's conclusion.[196] It might have added weight to the Commission's reasoning in favor of conditioning the merger before approving it.[197] But the crucial finding was that Microsoft had the incentive and ability to foreclose competition in the professional social network market, regardless of what the drivers of competition in that market actually were.[198] This competition problem derived from Microsoft's control over key business productivity software that allowed it to provide its affiliated LinkedIn app with ease of access and price advantages that competitors would not be able to match.[199] The resulting consumer harm was ultimately the loss of choice of alternative professional social networks, and with it the loss of a privacy alternative that consumers

192. EU Commission Decision, Facebook/WhatsApp, *supra* note 6, at par. 103.
193. *Id.* at par. 86.
194. Ocello & Sjödin, *supra* note 51, at 5-6 (emphasis added).
195. *Id.*
196. EU Commission Decision, Microsoft/LinkedIn, *supra* note 7, at pars 306-337, par 338.
197. *Id.* at par. 350.
198. *Id.* at par. 338.
199. *Id.*

valued.[200] The reasoning was from a foreclosing tie to a consumer harm, rather than from the loss of privacy competition to a competition problem.[201]

Moreover, the Commission's remedy did nothing to address LinkedIn's post-merger privacy practices.[202] It did not require the post-merger LinkedIn to make its data practices more pro-privacy or even to preserve the status quo in its data practices by not weakening privacy protections below what they were before the merger.[203] Indeed, the Commission's remedy to avoid certain pre-installation and integration practices would have been exactly the same if the Commission had concluded that privacy was not a parameter of competition at all.

V. LESSONS LEARNED

This review of Commission practice in two high-profile cases reveals the existence of substantial legal and factual obstacles to making progress on privacy through thinking of privacy as an element of competition and using antitrust merger review tools to preserve it. It confirms and illustrates many of the general points made earlier, including the inapplicability of data protection law and the need for factual case-by-case evaluation of privacy preferences. The cases also illustrate some of the formidable empirical difficulties in establishing the existence and strength of privacy preferences. Finally, the cases show that even when agencies examine privacy competition in merger reviews, these considerations do not necessarily play a strong role in the decision itself or in the formulation of the conditions designed to remedy competitive harm.

In both cases, the European Commission explicitly asserted that it did not apply data protection law in its merger reviews and that privacy as such belonged with data protection law, not with antirust merger reviews. Without explicitly stating so, it presumed that different privacy practices it observed in the marketplace all complied with data protection law. It did not seek out violations of data protection law and did not seek to remedy any perceived data protection violations through conditions on the mergers. It did not presume that robust privacy protective practices it observed from some companies in the marketplace were better, or more worthy or of higher quality than the less protective practices of others.

This respect for the differing privacy practices was particularly evident in the Commission's avoidance of the language of product quality.[204] It did not describe privacy as an aspect of product quality, but as a parameter of competition, and focused on the extent to which consumers made their

---

200. *Id.*

201. *Id.* at par. 350 and 338.

202. *Id.* at par. 437-438.

203. *Id.*

204. The one reference to privacy as an aspect of quality in the two cases comes from Microsoft's press release where privacy is described as relevant only "to the extent that consumers see it as a significant factor of quality." *See* Microsoft Press Release, *supra* note 171. This is in contrast to viewing privacy as if it were a matter of an objectively superior product feature such as safety or higher power of a car engine.

choices in the marketplace on the basis of the differences in data practices of the competing companies. It acknowledged that consumer privacy preferences varied in the marketplace, that some consumers valued it highly and others did not.

In short, it validated the conception of privacy as subjective. It was guided by its assessment of the value people placed on the pro-privacy data practices of WhatsApp or Xing, not by its own evaluation of the objective quality of these data practices. It sought to determine whether the privacy practices involved were a key determinant of market demand for the product.

In neither case did the Commission simply assert or deny that privacy was a key element of competition in markets involving the merging entities, that is, that privacy preferences were strong determinants of consumer behavior in the marketplace. This is an important distinction between asserting the possibility that privacy is a key element of competition and a finding that it is or is not a key determinant of consumer decisions.[205]

Instead, the Commission based its conclusions on investigations of the specific markets relevant to each merger review, and it reached different factual conclusions in each case. The analysis in the Facebook/WhatsApp case was fuller and more detailed, assessing the differences among the key marketplace participants and dividing them into those that were important drivers of competition and those with weaker impact. The assessment in the Microsoft/LinkedIn case was closer to mere assertion, with only a vague reference to an underlying market investigation and no assessment of other factors driving competition in the professional social media market.

Neither case was challenged by the parties involved, so we do not have a good idea of what level of evidence would be required by a reviewing court to sustain a challenge to an agency finding concerning privacy competition. However, the paucity of evidence in the Microsoft/LinkedIn case, its surface implausibility, and its lack of fit with external business assessments of marketplace drivers suggest that the level of empirical support in the Microsoft/LinkedIn case would not have been sufficient to sustain a finding of privacy as a key parameter of competition in the face of a determined challenge.

The two cases reveal the underlying empirical weakness in assessing the importance of privacy as an element of competition in merger review cases. These two merger analyses produced qualitative, hard-to-assess judgments on privacy competition that are open to speculative challenges. For instance, Stucke and Grunes speculate that privacy was an important element in the choice by Facebook users to use WhatsApp instead of Facebook Messenger.[206] That might be true. Perhaps they were worried about the extra privacy intrusion involved in one company knowing not only your social media interactions but also your messenger interactions. Or maybe they just

---

205. "The Commission did evoke privacy, noting that it *can* constitute an important dimension of competition between Facebook and WhatsApp, but concluding that they *did not* compete on this basis (i.e., privacy *was not* an important factor in the decision to use these applications)." Orla Lynsky, *Grappling with "Data Power": Normative Nudges from Data Protection and Privacy*, 20 THEORETICAL INQUIRIES L. 189, 216 (2019) (emphasis added).

206. *See* STUCKE & GRUNES, *supra* note 5, at 132.

needed the network of friends and contacts that WhatsApp had and Facebook did not. But how, other than mindreading, introspection, intuition, or speculation, can a reviewing agency make these determinations?

Also illustrating the slipperiness of the assessments involved is the Commission's attempt to show consistency between the two merger decisions despite the finding in the one case that privacy was an important parameter of competition and the finding in the other case that it was not. It raises the question of the role of external policy factors in determining the outcome of these assessments.

This lack of clarity and consistency might be thought to illustrate the inherent instability in trying to treat an intangible factor such as privacy as a non-price dimension of competition. But privacy practices are observable phenomena. It is a reasonably objective matter whether a company collects data for targeted advertising purposes or provides an opt-in choice for data collection or use.

The problem is not the intangibility of assessing a company's privacy practices. Rather, it is the difficulty of objectively assessing which factors play a crucial role in consumer purchasing decisions. To the extent that competition authorities are going to rely on assessing the relative importance of different dimensions of competition in merger reviews, they will need to develop more sophisticated empirical tools to guide their marketplace investigations. How to transform these qualitative and shifting judgments into something more empirical is a major challenge for the idea that competition policy can usefully advance privacy goals in merger reviews.

In the absence of firmer standards of evidence, the role of privacy in merger assessment might vary with shifting external policy priorities. It is worth noting that Microsoft/LinkedIn was reviewed in 2016 and Facebook/WhatsApp in 2014. During the two-year interval, the importance of privacy in European public policy discussions vastly increased, as European policymakers made the final push to pass the General Data Protection Regulation.[207] Final passage took place in April 2016, very close in time to the Commission's merger review of Microsoft/LinkedIn.[208] Merger review officials are not immune to these changes in policy emphasis and that might have given them a greater incentive in 2016 to focus on privacy as a dimension of competition than they did in 2014.

A final lesson from these two cases is that even when merger reviewing authorities take privacy competition into account, it might not be a major driver of the decision result or of any conditions devised. If the reviewing authority finds that there is little or no privacy competition in the markets under assessment in a merger review, privacy competition can play no further role in the review, even if there might be other reasons to block or condition the proposed merger.

---

207. Press Release, European Parliament, *Data protection reform - Parliament approves new rules fit for the digital era* (Apr. 14, 2016), https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era. [https://perma.cc/9ZNX-W32L].

208. *Id.*

The Facebook/WhatsApp merger review illustrates how privacy competition can become irrelevant to antitrust decision making in a case. The Commission observed the difference between the privacy practices of WhatsApp and Facebook Messenger but found that consumers largely did not make their choice of communications apps on that basis. The merger assessment then proceeded to analyze whether the merger would substantially lessen competition in each of three markets—communications apps, social networking, and online advertising—without further addressing the effect on the relatively minor privacy competition.

But the irrelevance of privacy competition to the Commission's ultimate decision is more pronounced than that. The Commission's approval of the merger without conditions would not have been different if the Commission *had* found that privacy was a key parameter of competition between Facebook Messenger and WhatsApp. The reason is that even if privacy had been important, the presence of other competitors providing large and reliable networks and/or pro-privacy data practices, the lack of entry and switching barriers, and the limited role of network effects all meant that competition in privacy would have been preserved in the post-merger world.

In the Microsoft/LinkedIn case, the Commission reached the opposite conclusion—that privacy competition was strong in the market for professional social networks. But here too, the finding was essentially irrelevant to the determination that conditions were needed to sustain competition in the market and to the crafting of appropriate conditions.

The Commission's concern in Microsoft/LinkedIn had nothing to do with privacy competition. Its concern was the dominant position that Microsoft had in the marketplace for productivity software and the likelihood that, unchecked, it would use this position to pre-install and integrate its newly acquired professional software app, LinkedIn, in a way that gave it an insuperable advantage over rival professional social networks. The previous vibrant competition between LinkedIn and other professional social networks, in particular Xing, would be substantially diminished. The presence or absence of privacy competition was beside the point in this assessment.

Moreover, in devising the remedy, the Commission did not consider any special measures to preserve privacy protection. Various commitments voluntarily limiting Microsoft's option for pre-installation and integration were sufficient to warrant Commission approval of the merger. The remedy it imposed was unrelated to the merged entity's privacy practices.

VI. CONCLUSION

Carl Shapiro makes the fundamental point that more competition might very well be the enemy of privacy, not its friend: "Indeed, it is not even clear that more competition would provide consumers with greater privacy, or better combat information disorder: unregulated, competition might instead trigger a race to the bottom, and many smaller firms might be harder to

regulate than a few large ones."[209] More competition might impel companies to outdo their rivals through ever more intensive exploitation of their consumers' information. In this view of things, privacy law is needed to counteract the harmful tendency of competition to undermine privacy, and the last thing we need to improve privacy is more competition!

But suppose Shapiro is wrong, and instead suppose that competition has driven or is likely to drive companies to provide more privacy than is required by law. Imagine that consumer demand for pro-privacy data practices is strong and some companies seek, or are on the cusp of seeking, to distinguish themselves from their rivals by aiming to satisfy these preferences. In other words, assume that there is strong privacy competition, that is, competition for consumer business based on their privacy preferences. Can merger reviews under competition law realistically preserve this privacy competition?

In principle the answer is yes. If some companies responding to strong consumer demand provide or are likely to provide more privacy protection than required by current law, competition policy authorities might be able to preserve that competition-driven privacy by blocking or conditioning a merger that would threaten their continued ability to provide that extra level of privacy protection.

However, to achieve this modest result for privacy protection, antitrust authorities must overcome high legal and factual obstacles. They need to show not only that some companies are providing or are likely to provide additional levels of privacy protection, but that a significant number of consumers make their choice to patronize these companies largely on the basis of privacy protection. This in fact is the practical meaning of the oft-repeated phrase that privacy can be a key parameter of competition in the marketplace.

But this feature of marketplace competition cannot be simply assumed. Merger authorities must demonstrate the existence of privacy competition through a fact-based market investigation, where, as we have seen from the two cases examined in this Article, the standards of evidence are unclear.

Then the reviewing authority must show that this provision of additional privacy protection is not likely to endure in the post-merger world. This could happen in a variety of ways, but the reviewing authority must establish an incentive for the merged entity to reduce the level of privacy protection below that which would have been provided in the absence of the merger. This loss of privacy protection would then be a consumer harm that could be considered in assessing the merger.

Finally, and most crucially, this consumer harm must be likely to arise because of some reduction in competitive conditions in the post-merger world. It is not enough to show that the post-merger world would be one with

---

209. Shapiro, *supra* note 31, at 79. This notion that competition might lead to a decline in an aspect of product quality like privacy is related to the ambiguous relationship between competition and product quality. Both theory and empirical research show that "changes in competition levels can have either positive or negative effects on quality." OECD Quality Report, *supra* note 56, at 7.

lower privacy protections. If the reduction in privacy protection is due to a business reassessment of consumer demand or even to the whims of the new owners, it is not determinative under merger review standards, even though it is a real loss for consumers.

The consumer harm connected to a privacy loss must be traceable to a substantial lessening of competitive forces. If there would be plenty of rivals, if entry and expansion would be easy, if network effects would pose no fundamental obstacles to entry or expansion, then, especially if privacy demand is strong in the marketplace, it is hard to see why the loss of valued privacy protections would not be quickly remedied in this fully competitive marketplace. In the presence of strong consumer demand for privacy, the merged company might have an incentive to reduce privacy protection, but vibrant marketplace competition either will block them from doing so successfully or will impel existing rivals or new entrants to fill their shoes.

Finally, it is not clear how central considerations of privacy competition would be even in these cases. All the real work in merger review might be accomplished outside a consideration of privacy preferences in assessing whether an unconditioned merger will lead to a significant loss in competitive conditions and whether there are measures short of disallowance that will maintain competition. Considerations of competition in privacy might very well add weight to these considerations in that any loss of competitive conditions will also reduce privacy competition and any steps to maintain competition will also maintain privacy competition. But privacy will not be determinative of the outcome.

It should not be a surprise that such formidable legal and factual obstacles loom in front of any attempt to use privacy competition as a key element in seeking to block or condition mergers. High hurdles are present in all attempts to block or condition mergers. Under existing competition law and jurisprudence, it is hard, and it is supposed to be hard, to do this. If that is true in general, it is not less true when privacy is a major factor in marketplace competition.

Taken together, the state of the competition law and numerous practical considerations in assessing privacy competition cast a shadow over the efficacy of merger reviews as a significant legal mechanism for maintenance of privacy protections. In this Article, I have described the considerations involved in deploying merger control resources against the increased collection and use of personal information by digital platforms and other firms. The results strongly suggest that it would be better to turn to other aspects of competition law or to privacy law itself to vindicate privacy rights.[210]

---

210. As mentioned earlier in the paper, other ways of addressing privacy issues through the application of competition law exist, namely, through treating personal data as an asset that might be monopolized in a merger and imposing privacy-preserving conditions on dominant companies. Future work will assess the barriers and obstacles to taking these avenues through competition law toward the protection of privacy.

The Roads of the Future Require a Functioning P.A.V.E.R.: How Autonomous Vehicles are More Like Your Bank Than Your Browser, and Must be Regulated Accordingly

Brian R. DeMocker*

TABLE OF CONTENTS

* J.D., May 2020, The George Washington University Law School. Thank you to my loving parents, sister, and brother-in-law for offering wisdom, support, and patience throughout my education. Thank you to my wonderful fiancée for insightfully advising me and protecting my sanity throughout both this writing process and all of law school. I could not have reached my goals without each of you. Thank you to the staff of the Federal Communications Law Journal for their patience, hard work, and assistance with this publication.

I. INTRODUCTION

It is Friday evening and you just clicked "send" on your computer, which completes a *long* week at your law firm. As your completed memorandum navigates cyberspace, your phone blinks awake to receive your verbal instruction to hail a self-driving, "autonomous" vehicle to meet you at the curb. A vehicle pulls up as you exit your building and you climb in through the opened doors. As you stretch your legs out in front of you, the screen illuminates to display a list of destination options. Brewery, brewery, cocktail bar, brewery, brewery, home. They know me too well, you muse. It is 6:45 PM and you have, after all, gone to a brewery every Friday after work. You select one of the breweries and the vehicle silently speeds toward the destination.

On your way, you check the news to find a new piece of federal legislation up for consideration called the Privacy in Autonomous Vehicles and Enforcement Regulation, or "P.A.V.E.R.," which would allow connected and autonomous vehicle users to opt out of the commercial exploitation of nonpublic personal information, such as vehicle location data, collected by connected or autonomous vehicles[1] in order to limit the information that can be used in targeted advertisements. After reading further about P.A.V.E.R., you recall that on Monday you must drive to the headquarters of a largely controversial political group in order to deliver some files related to an ongoing dispute between one of your clients and the group. You realize that if you use an autonomous vehicle, or even a connected vehicle that is not fully autonomous, your route and destination would be recorded and attached to your online marketing profile, which would cause you to begin receiving targeted advertisements relating to the controversial group. You realize that P.A.V.E.R. would actually allow you to decide that this particular errand would go unrecorded. Suddenly, P.A.V.E.R. earns you as a new fan.

Seeing as P.A.V.E.R. is not yet implemented, you weigh alternative options for keeping your errand unrecorded. You ultimately elect to rent (at your firm's expense, of course) a cheap, non-connected, and non-autonomous vehicle for the errand to avoid digital association with the controversial group, despite the fact that you have not actually driven a vehicle manually in many years.

Monday arrives and you climb into the old, non-autonomous vehicle with your files in tow. You feel a little cramped due to the presence of a steering wheel. How antiquated, you think. You put the vehicle into reverse manually and press down on the gas pedal, which makes the vehicle lurch backwards abruptly. After you gather yourself, you ease the vehicle backwards and take off down the road. After about thirty minutes of jerky driving, you glance at the right side-mirror to find a bicyclist only inches from

1. "Connected" vehicles shall refer to vehicles that have the ability to receive, process, and transmit data to other connected vehicles, infrastructure, and/or the Internet. "Autonomous" or "partially-autonomous" vehicles shall refer to vehicles with the ability to "self-drive," or operate with no or minimal driver intervention.

your vehicle. Startled and unused to manually operating a vehicle so close to another person, you jerk the wheel left, causing the non-autonomous vehicle to jump the curb and slam into a concrete barrier. After a short stay in the hospital, you are discharged. P.A.V.E.R. would have avoided this whole situation.

Just as banks and financial institutions cannot disclose certain information about customer choices and buying habits to certain unaffiliated third-party entities due to restrictions on sharing nonpublic personal information following customer opt-out,[2] autonomous vehicle manufacturers should not be permitted to disclose the data collected through regular vehicle operations (such as the vehicle's current location, home or work addresses, browsing histories on the vehicle's interfaces, or driving routes and times) to unaffiliated third-party entities unless the customer declines to opt out or unless such data sharing is necessary to properly operate the vehicle. Autonomous vehicles are much safer than conventional vehicles[3] and as such, mainstream use should be heavily incentivized. There exists, however, a data privacy concern stemming from the use of the information necessarily collected through regular autonomous vehicle (or any sort of connected vehicle) operation that could present a major barrier to mainstream autonomous vehicle use.[4] Unfortunately, there is a complete lack of federal restrictions on manufacturers' use of this information.[5] Thus, Congress should pass regulatory legislation directed at the autonomous vehicle industry in order to reduce the chilling effect that surveillance capitalism can have on individuals' freedom of expression and consumer choices, which would deconstruct barriers to the use of a vital transportation service capable of substantially reducing the number of vehicle-related injuries and deaths.[6] This paper will show how the Gramm-Leach-Bliley Act,[7] the banking and

2. 15 U.S.C. § 6802 (2012).

3. *See* Brandon Amon, *Invading the Driver's Seat: Preventing Overbearing Targeted Advertising in Connected Vehicles*, 46 HOFSTRA L. REV. 329, 353-54 (2017) (citing Jeffrey Zients & John P. Holdren, *American Innovation in Autonomous and Connected Vehicles*, WHITE HOUSE (Dec. 7, 2015, 3:53 PM), https://obamawhitehouse.archives.gov/blog/2015/12/07/american-innovation-autonomous-and-connected-vehicles).

4. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

5. Angela Stringfellow, *The Ultimate Data Privacy Guide for Banks and Financial Institutions*, NGDATA (Aug. 14, 2018), https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/ [https://perma.cc/8DGL-VKWY] ("There's currently no overarching federal law addressing data privacy in full.").

6. *See generally Maximizing the Benefits of Self-Driving Vehicles: Principles for Public Policy*, UNION OF CONCERNED SCIENTISTS (Feb. 3, 2017), https://www.ucsusa.org/sites/default/files/attach/2017/02/Maximizing-Benefits-Self-Driving-Vehicles.pdf [https://perma.cc/TP5P-V5NM] [hereinafter UNION OF CONCERNED SCIENTISTS]; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY i (Sept. 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf [https://perma.cc/822T-MDKD] [hereinafter NAT'L HIGHWAY TRAFFIC SAFETY ADMIN.].

7. 15 U.S.C. § 6801–6809 (2012).

financial industry's data privacy regulation, provides a particularly adaptable regime well-suited for use by the autonomous vehicle industry.

Section II of this paper addresses the factual and legal background of both the autonomous vehicle industry and the banking and financial industry. Section III discusses three issues. First, it argues that the banking and financial industry is subject to certain regulations regarding use of nonpublic personal information unlike other data-driven industries, such as those offering web browsing or online shopping, because the products and services offered by banks and financial institutions are considered "vital" in today's society. It also discusses how autonomous vehicles are likewise distinguishable from data-driven companies and how such vehicles are more similar to banks and financial institutions. Further, Section III discusses how the Gramm-Leach-Bliley Act provides a useable template for regulation of the autonomous vehicle industry. Section IV proposes P.A.V.E.R. as a solution to the unregulated use of nonpublic personal information by autonomous vehicle manufacturers, describes P.A.V.E.R.'s construction, and discusses other solutions proposed in relevant scholarly literature. Finally, Section V addresses questions that must still be answered before society can make a fully informed decision about how to address data privacy in the autonomous vehicle industry, and finishes with a charge to Congress to pass legislation to effectively regulate data privacy in the autonomous vehicle industry. The primary focus of this paper is on private companies' use of nonpublic personal information and does not discuss governmental surveillance applications, which have largely been found unconstitutional.[8]

II. THE FACTS AND LAWS SURROUNDING THE AUTONOMOUS VEHICLE INDUSTRY AND THE BANKING AND FINANCIAL INDUSTRY

Discussion of both the autonomous vehicle industry and the banking industry is necessary to understand the comparison made later in this paper between the two industries. The autonomous vehicle section lays the foundation for the argument that the industry is "vital" due to the ability of autonomous and connected vehicles to reduce traffic fatalities and injuries,[9] and that the use of such vehicles will become well integrated into society.[10] The banking and financial section lays the foundation for the argument that the industry is "vital" due to the deep societal integration of the use of, and financial protection by, the products and services offered by banks and financial institutions. [11] These sections also provide the background information needed to understand the later argument that the financial

8. *See, e.g.*, *Jones*, 565 U.S. at 400-13 (holding that the warrantless collection of location data through attachment of a GPS device violated the Fourth Amendment).

9. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6, at i.

10. *See infra* Section II.A.

11. *See infra* Section II.B.

industry is regulated largely due to its "vital" nature and, as such, the autonomous vehicle industry should be similarly regulated.[12]

A. The Autonomous Vehicle Industry

To best grasp the workings of the connected and autonomous vehicle industry and the vehicles themselves, inquiry into the factual and legal background is an important first step. Autonomous vehicles operate at different levels of automation, which influences the type and amount of information necessarily collected for the vehicle to function properly.[13] As vehicles become more advanced and require less human intervention, the collection and use of a larger amount of data is required.[14] There is not currently, however, any federal legislation that limits how this data can be used, despite its high risk of abuse.[15]

1. How Autonomous Vehicles Function and Inherent Privacy Threats

Automotive companies are beginning to entertain the idea that autonomous vehicles are the next step in innovation and road safety.[16] In fact, some experts say that autonomous vehicles may be the most important transportation innovation since the inception of the automobile.[17] Autonomous vehicles are those designed to transport people and cargo to a destination, requiring varying levels of reduced human intervention and focus, ranging from heavily human-controlled to fully self-driving.[18] Researchers have labeled the different levels of vehicle automation as follows: Level 0 refers to full human control; Level 1 refers to when the vehicle controls certain systems, such as braking or cruise control; Level 2 refers to when the vehicle operates using multiple automated functions, such

12. *See infra* Section III.

13. *See infra* Section II.A.1.

14. *See* William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous, and Connected Vehicles*, 31 SANTA CLARA HIGH TECH. L.J. 99, 103-04 (2015); *see also Self-Driving Cars Explained*, UNION OF CONCERNED SCIENTISTS (Jan. 26, 2017), https://www.ucsusa.org/clean-vehicles/how-self-driving-cars-work#.XDoTTM9KjzJ [https://perma.cc/7AYJ-DURS]; *infra* Section II.A.1.

15. *See infra* Section II.A.2.

16. *See generally Looking Further: Ford Will Have a Fully Autonomous Vehicle in Operation by 2021*, FORD, https://corporate.ford.com/articles/propulsion-choices/autonomous-2021.html [https://perma.cc/BJD8-46XY] (last visited Oct. 9, 2019); *see, e.g.*, Andrew Giambrone, *Ford to Test Driverless Cars in D.C. Early Next Year*, CURBED (Oct. 22, 2018, 5:32 PM), https://dc.curbed.com/2018/10/22/18010858/dc-ford-driverless-cars-autonomous-vehicles-transportation [https://perma.cc/6GNF-UGGM] (last visited Oct. 9, 2019); *Future of Driving*, TESLA, https://www.tesla.com/autopilot [https://perma.cc/5WQH-2GY9] (last visited Oct. 9, 2019); WAYMO, https://waymo.com/tech/ [https://perma.cc/F67F-R97Z] (last visited Oct. 9, 2019).

17. *See* UNION OF CONCERNED SCIENTISTS, *supra* note 6.

18. *See* Kohler & Colbert-Taylor, *supra* note 14, at 102-03; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

as steering plus acceleration and braking, but humans must remain focused and alert in the event that intervention is necessary; Level 3 refers to when the vehicle can operate safely by itself in nearly all situations and under certain conditions; Level 4 refers to when the vehicle can operate safely and autonomously in nearly all situations and under any condition; and, although some researchers end after Level 4, Level 5 refers to when the vehicle is entirely capable of self-driving in any situation and in any condition.[19]

To create a functioning autonomous vehicle that can operate at Levels 2 through 5 (and sometimes even for Level 1), vehicle manufacturers must install on-board sensor-based solutions, vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") connectivity-based solutions, or more likely a combination of both solutions, to enable the vehicle to avoid hazards in and around the roadway.[20] On-board computers can evaluate environmental and vehicular data received from on-board sensors, such as speed, acceleration, vehicle roll angle, heading, information about the surroundings, current location, and more, which is essential to the safe operation of the vehicle.[21] Connectivity-based solutions allow vehicles to determine the speed and direction of other vehicles sharing the road, and routing information about the other vehicles' destinations.[22]

While Level 1, 2, and 3 autonomous vehicles have already rolled out and are in use or in testing today,[23] fully autonomous (i.e., entirely self-driving) vehicles are still to come.[24] There are, however, data privacy concerns relevant to the Level 1, 2, and 3 V2V-capable vehicles that have already been released.[25] Juniper Research released a study in December 2018 projecting that "over 62 million vehicles will be capable of V2V . . . communication by 2023" and that by then, 60% of all new sales of vehicles in the US will have V2V capability.[26] The research also noted that long "vehicle refresh rates" (meaning the time it takes for an owner to sell or dispose of a vehicle and buy a new one), which are generally around eight to twelve years, will "hinder mass adoption" of V2V technology in the immediate future.[27] This means that there are vehicles that are already, or soon to be, on the road that have the capacity to share certain data gathered

19. *See* Kohler & Colbert-Taylor, *supra* note 14, at 102-03; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

20. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103-04.

21. *See* Michael Mattioli, *Autonomy in the Age of Autonomous Vehicles*, 24 B.U. J. SCI. & TECH. L. 277, 283-84 (2018).

22. *See* Kohler & Colbert-Taylor, *supra* note 14, at 126-27.

23. *See, e.g.*, *Future of Driving*, TESLA, https://www.tesla.com/autopilot [https://perma.cc/R5TM-59EY] (last visited Oct. 13, 2019).

24. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103.

25. *See, e.g.*, Amon, *supra* note 3, at 350-52.

26. *See Vehicle to Vehicle Communications To Be Installed in 62M Vehicles by 2023, As 56 Disrupts Established Automotive Strategies*, JUNIPER RESEARCH (Dec. 11, 2018), https://www.juniperresearch.com/press/press-releases/vehicle-to-vehicle-communication-to-be-installed [https://perma.cc/8V5B-XE83].

27. *See id.*

by the vehicle despite not requiring this V2V connectivity in order to function properly as a viable transportation option.[28]

The data gathered by an autonomous or connected vehicle would certainly aid in the vehicle's operation,[29] but the threat of data misuse may deter some individuals from using such vehicles. William J. Kohler and Alex Colbert-Taylor identified, in a 2015 article in the Santa Clara High Tech Law Journal, two major privacy concerns implicated if a private entity enjoyed unregulated control of the data generated by necessary operations of an autonomous vehicle: potentially invasive tailored advertising and private commercially-motivated route planning.[30]

The first concern, regarding advertisements, arises from what private entities can do with the data gathered from the vehicle to advance marketing interests.[31] Automobile manufacturers and other private companies have already obtained patents that address advertising inside private vehicles,[32] which indicates an interest in such advertising practices. Much like data brokers that gather information based on an individual's Internet usage to build an online advertising profile and push tailored advertising to that individual, vehicle manufacturers or other entities could achieve a similar outcome through analysis of a connected vehicle's travel habits.[33] These kinds of targeted advertisements are already in use throughout the Internet,[34] and as such it is not unreasonable to expect the practice to enter the autonomous vehicle industry. After all, in a Level 3 or above vehicle, where an individual does not need to intervene much, if at all, advertisers would enjoy a captive audience, as the vehicle's occupant or occupants would be able to browse the Internet rather than focus on the road.[35]

As previously stated, there may be nothing inherently wrong with receiving relevant, tailored advertisements. The mere possibility, however, that a third party may receive or purchase one's nonpublic personal information for targeted commercial exploitation can, according to Justice Sotomayor, have a chilling effect on individual expression.[36] While Justice Sotomayor focused her discussion in *United States v. Jones* on governmental monitoring and its effects on an individual's behavior,[37] it would be a logical leap and perhaps not that difficult to expand the scope to include non-governmental entities and the chilling effect that marketing-focused surveillance and data collection would have on an individual's behavior. Justice Sotomayor further discussed how location data could reveal details

28. *See id.*; *see generally* Kohler & Colbert-Taylor, *supra* note 14, at 120.
29. *See* Amon, *supra* note 3, at 342.
30. *See* Kohler & Colbert-Taylor, *supra* note 14, at 121-23.
31. *See id.* at 122-23.
32. *See id.* at 121-22.
33. *See id.* at 122.
34. *See id.*
35. *See, e.g.*, *id.*
36. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").
37. *See generally id.* at 413-18 (Sotomayor, J., concurring).

about an individual's family, political affiliations, professional life, religious beliefs, and sexual relations.[38] Some data privacy experts also "warn that this [type of data collection and distribution for marketing purposes] would open the door to harmful new forms of commercial surveillance."[39]

The second concern, regarding private, commercially-motivated route planning versus algorithmic routing, presents a troubling set of possibilities. Consider the ideal scenario for autonomous route planning: the vehicle, unprompted, is able to gather information from vehicle networks and Internet sources regarding weather and road conditions, pedestrian and non-autonomous vehicular congestion, and even hot-spots where anti-autonomous vehicle vandalism or violence is known to occur, and the vehicle is then able to plan a route accordingly. Consider the alternative, where a private entity controls route-planning functions: the vehicle performs the above algorithmic route planning, then incorporates the private entity's commercial interests. For example, the vehicle might route, and perhaps even select a longer route, to travel past the physical buildings of paying businesses.[40] Utilizing the individual's online advertising profile discussed above, the vehicle could select a route past businesses at which the vehicle's occupant would be most likely to stop and make a purchase.[41] Briefly exiting the realm of purely economic and commercial motivations, one can imagine another scenario where the route-controlling entity has political ties to other entities and could encourage vehicles to plan routes that travel in close proximity to the entities' political events.

2. The Laws Surrounding Autonomous Vehicles—or Lack Thereof

Although several states maintain their own data privacy regulations,[42] there is no single federal privacy law applicable to every jurisdiction in the United States that restricts the distribution or sale of data collected from an autonomous vehicle.[43] Congress has briefly entertained federal data privacy legislation applicable to autonomous or connected vehicles, but the proposed legislation would have provided little meaningful regulation and, in any case, has failed.[44]

Additionally, the Electronic Communications Privacy Act (ECPA), codified under 18 U.S.C. §§ 2510-2522 (2012), applies only to the

---

38. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *see also* Kohler & Colbert-Taylor, *supra* note 14, at 124.

39. *See* Mattioli, *supra* note 21, at 280.

40. *See* Kohler & Colbert-Taylor, *supra* note 14, at 122.

41. *See id.*

42. *See, e.g.*, Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIVACY PROFESSIONALS (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/ [https://perma.cc/9ZP8-XEG8].

43. *See* Stringfellow, *supra* note 5.

44. *See, e.g.*, H.R. 3388, 115th Cong. § 12(a) (2017) (failed); *see also* S. 680, 115th Cong. (2017) (failed).

interception of electronic communications.[45] The ECPA does not regulate what entities can do with information obtained through legal means, such as from the normal operation of an autonomous vehicle.[46] Furthermore, the Federal Trade Commission Act, codified under 15 U.S.C. §§ 41-58, applies to topics such as unfair or deceptive practices,[47] but similarly does not address what an entity may do with the sort of data collected from an autonomous vehicle.

Thus, there is currently no substantive federal law that could be applied to autonomous vehicle data privacy.[48] If autonomous vehicle manufacturers wanted to use or distribute nonpublic personal information collected from normal vehicle operations, the fact that autonomous vehicles are innately transportable across state lines would potentially force manufacturers to program vehicles to change their data sharing algorithms based on their current location.[49] And if a state passed new legislation amending its existing privacy legislation, manufacturers would need to quickly and remotely revise the vehicles' protocols for that jurisdiction in order to maintain compliance.

B. The Banking and Financial Industry

The banking and financial industry is a widely used source of products and services that is analogous to the autonomous vehicle industry in several ways discussed in future sections.[50] Consumers today frequently use banks and financial institutions, and the benefits are well established.[51] Through regular operations, these institutions also handle a large amount of nonpublic personal information, which can be abused.[52] As such, Congress passed federal legislation aimed at protecting consumers' data privacy.[53]

1. The Uses of, and Abuses by, Banks and Financial Institutions

Banks and financial institutions are widely used and heavily integrated into society.[54] According to a 2017 Federal Deposit Insurance Corporation (FDIC) survey, executed in partnership with the United States Census Bureau,

45. *See* 18 U.S.C. §§ 2510-2522 (2012).
46. *See, e.g.*, *id.*
47. *See* 15 U.S.C. §§ 41-58 (2012).
48. *See, e.g.*, Stringfellow, *supra* note 5.
49. This scenario could occur if state privacy legislation required that all vehicles (or any device capable of sharing data, for that matter) operating within its jurisdiction comply with the state privacy law.
50. *See infra* Section III.
51. *See infra* Section II.B.1.
52. *See infra* Section II.B.1.
53. *See infra* Section II.B.2.
54. *See generally* FED. DEPOSIT INS. CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 1-14 (2018), https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf [https://perma.cc/JKX5-5DU4] [hereinafter *FDIC Survey*].

approximately 6.5% of households in the United States were "unbanked" in 2017, meaning that none of the individual members of the household possessed a bank account (either a checking or savings account).[55] Importantly, the survey also found that 68.4% of households were "fully banked," meaning the members of the household maintained bank accounts with insured institutions and did not use alternative financial services during the preceding 12 months.[56] The survey also revealed a trending decline in the rate of unbanked households from 2015 to 2017.[57] As more people and households turn to checking and savings accounts for everyday transactional convenience, privacy concerns grow.[58]

Banks and financial institutions regularly collect information and data from their customers in order to deliver financial products and services.[59] If a customer uses a credit card, or even just opens an account, the institution collects information such as name, address, contact information, income, wealth data, spending habits, and the location of purchases.[60] Moreover, financial transaction information can paint a detailed picture of an individual's private life without the individual realizing just how much detail can be discerned through analysis of that data.[61] Some examples of the sort of information that can be determined through transaction history include home or work addresses, home ownership status, rental relationships, age, medical information, prescribed medication, physical body details such as height and weight, income and debt levels, product preferences, political or religious affiliations, ethnic identity, marital status, family member details, travel and vacation habits, hobbies, and criminal tendencies.[62]

Some individuals may not care if banks and financial institutions sell the individual's depersonalized online profile to marketers or data brokers. Some may even welcome targeted advertisements informed by such transactional data because the advertisements would be more relevant to the individual. Others, however, may not appreciate targeted advertisements informed by the types of transactions in which the individual engages. It is not difficult to imagine the embarrassment that could stem from a situation where an individual is browsing his or her computer in public when, surprisingly, the individual's computer is flooded with targeted advertisements for products and services that reveal the individual's secrets. Imagine a teenage daughter's parents walking past her computer and seeing advertisements for baby formula, prenatal vitamins, maternity clothes, and strollers. Imagine an individual showing his friends or family an online video,

---

55. *Id.* at 1.
56. *Id.*
57. *Id.*
58. *See* Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 946-947 (2002).
59. *See* FED. DEPOSIT INS. CORP., YOUR RIGHTS TO FINANCIAL PRIVACY, https://www.fdic.gov/consumers/privacy/yourrights [https://perma.cc/4HSV-WV2X] (last visited Sept. 20, 2019) [hereinafter *FDIC Privacy Rights*].
60. *Id.*
61. *See* Gertz, *supra* note 58, at 944-48.
62. *See id.* at 944-45.

preceded by advertisements for Viagra or genital anti-fungus medication. Imagine still an abuser becoming enraged and violent after using his victim's computer and seeing advertisements for self-defense classes, self-defense weapons, or travel websites. The above possibilities are only a few scenarios with potentially disastrous outcomes. The point stands: a relatively small amount of nonpublic personal information, such as the information derived from financial transactions, can reveal a substantial amount more about an individual's life than that individual may be comfortable sharing.

2. Legislated Data Privacy, Courtesy of the Gramm-Leach-Bliley Act

Various laws recognize the privacy concerns articulated above and the need to protect certain customer behavior.[63] Congress passed the Federal Financial Modernization Act, also referred to as the Gramm-Leach-Bliley Act,[64] 15 U.S.C. §§ 6801–6809, to regulate and enhance fair competition in the banking and financial services industry.[65] Importantly, the Act also regulates how banks and financial institutions handle individuals' nonpublic, personal information by instituting a Congressional policy under Title V of the Act, requiring financial institutions to adopt "an affirmative and continuous obligation to respect the privacy of its customers."[66] As defined by the Act, nonpublic personal information refers to personally identifiable financial information that is not publicly available and is either provided to the bank or financial institution by the customer, received by the bank or financial institution through the customer's financial transactions or use of a service provided by the institution, or somehow otherwise received by the financial institution.[67] Furthermore, the Gramm-Leach-Bliley Act states that banks and financial institutions are prohibited from disclosing this nonpublic personal information to an unaffiliated third party, unless three conditions are satisfied.[68] First, the institution must "clearly and conspicuously" notify the customer that the institution may disclose the information to the third party; second, the customer must have ample opportunity prior to the disclosure to prohibit the institution from disclosing that information; and third, the institution must inform the customer how to exercise the opt-out option.[69]

There are, however, several critical shortcomings and loopholes in the Gramm-Leach-Bliley Act. First, there is debate as to the effectiveness an opt-out option would have on an individual's privacy.[70] The result of an individual opting out is not necessarily the individual's intended outcome. Once an

63. *See, e.g.*, 15 U.S.C. §§ 6801–6809 (2012).
64. *Id.*
65. *See* Gertz, *supra* note 58, at 982.
66. 15 U.S.C. § 6801(a) (2012).
67. *See id.* § 6809(4).
68. *See id.* § 6802(b).
69. *Id.*
70. *See* Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U.L. REV. 63, 133-34 (2003).

individual opts out of the data-gathering regime, compliance with the Gramm-Leach-Bliley Act requires only that banks and financial institutions refrain from sharing certain types of information with certain unaffiliated third parties, not that the banks and financial institutions cease data collection.[71] Additionally, the Act only applies to "financial institutions," such as banks and other like-institutions that are engaged in activities that are financial in nature (for example, lending, exchanging, transferring, investing for others, or safeguarding money or securities, and much more).[72] Therefore, entities that are not primarily engaged in activity that is financial in nature, such as large data companies, need not comply with the Gramm-Leach-Bliley Act and may freely disseminate nonpublic personal information to third parties.[73]

Furthermore, the Act does not prohibit a bank or financial institution from sharing nonpublic personal information with affiliated partners, including marketing partners that are not "third party," even over a customer opt-out.[74] This means that the Act does not specifically outlaw all sharing of individuals' nonpublic personal information if the customer opts out.[75] Thus, not all nonpublic personal information can be sheltered.[76] Large data companies certainly manage and use nonpublic personal information and share or sell that data to marketers and data brokers for use with targeted advertisements.[77] Yet, despite the aforementioned shortcomings, the banking and financial industry, and specifically the Gramm-Leach-Bliley Act, provides a useful template for how to regulate the autonomous vehicle industry.

III. HOW AUTONOMOUS VEHICLES ARE MORE LIKE THE BANKING AND FINANCIAL INDUSTRY AND WHY SUCH VEHICLES NEED DATA PRIVACY LEGISLATION

As previously discussed, autonomous vehicles will receive, process, and transmit a large amount of information through normal functions and

71. *See id.*

72. *See* 15 U.S.C. § 6809(3) (2012); *see also* 12 U.S.C. § 1843(k)(4) (2012).

73. *See* 15 U.S.C. § 6809 (2012); *see also Making It Easy to Understand What Data We Collect and Why*, GOOGLE, https://safety.google/privacy/data [https://perma.cc/4P7T-3JHN] (last visited Oct. 9, 2019); *Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html? nodeId=201909010 [https://perma.cc/7RWJ-PVVL] (last visited Oct. 9, 2019); *Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy [https://perma.cc/T9GT-NTKY] (last visited Oct. 9, 2019); *How Does Facebook Show Ads on Mobile Devices and Connected TVs?*, FACEBOOK, https://www.facebook.com/help/119468292028768?ref=dp [https://perma.cc/2MKJ-8NJK] (last visited Oct. 9, 2019).

74. *See* 15 U.S.C. §§ 6802 (2012).

75. *See id.*

76. *See, e.g.*, *Ads and data*, GOOGLE SAFETY CENTER, https://safety.google/privacy/ads-and-data/ [https://perma.cc/T77D-W6HP] (last visited Oct. 11, 2019); *see also* AMAZON, *supra* note 73; *Data Policy*, FACEBOOK, *supra* note 73.

77. *See id.*

operations.[78] Autonomous vehicle users will likely be very interested in whether this data can be used to add to, or update, their online marketing profiles.[79] Additionally, those users will want to know information such as "what uses are made of such personal data, why it is being collected, how it will be used, how long it will be kept, and who will and will not have access to it[,]" as well as whether the collected data will reveal "where, when, and how a person moves from geographical place to place[.]"[80] The consequences of allowing unfettered data collection vary widely. One concern on a smaller, individual scale is that the data collected will, in aggregate, reveal additional nonpublic personal information, which can be used to push unwanted, or even invasive, targeted advertisement campaigns to individuals.[81] This data could also be used to manipulate an individual's habits, such as travel destinations or what restaurants to visit.[82] Another concern on a larger scale is that the information from autonomous vehicles could be analyzed to reveal an enormous amount of information on particular large populations of individuals, or even all users, which allows those in control of the information to enjoy significant influence over those populations.[83]

To address privacy concerns that could stunt the industry's development, autonomous vehicles should be regulated similarly to how banks and financial institutions are regulated. Because autonomous vehicles are an emerging technology capable of reducing vehicle-related fatalities and injuries, autonomous vehicle technology is "vital"—similar to how banks and financial institutions provide a "vital" service due to the practical and widely-integrated nature of the products and services provided.[84] Data privacy concerns, however, could constitute a barrier to users quickly transitioning from non-autonomous vehicles to partially or fully autonomous vehicles.[85] Because autonomous vehicles have the ability to reduce or eliminate bodily harm,[86] Congress should take steps to speed up the transition by passing data privacy legislation, which would likely calm data privacy concerns. The Gramm-Leach-Bliley Act framework could function as an adaptable template for autonomous vehicle regulation, with appropriate modifications.

78. *See* Kohler & Colbert-Taylor, *supra* note 14, at 120-21.

79. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1195-96 (2012).

80. *Id.*

81. *See id.* at 1196.

82. *See id.*

83. *See id.* at 1196-97.

84. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

85. *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

86. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

A. Industry Comparison Among Large Data-Driven Companies, Banks and Financial Institutions, and Autonomous Vehicles

To compare the autonomous vehicle industry with the banking and financial industry, we must rationalize why the law, specifically the Gramm-Leach-Bliley Act, prohibits dissemination of nonpublic personal information by banks and financial institutions to unaffiliated entities after customers opt out, but still allows sharing of such information with affiliated institutions and marketing partners.[87] We must also rationalize why, in particular, banks' and financial institutions' handling of nonpublic personal information is regulated to protect customers' privacy, while large data-driven companies such as Google, Amazon, and Facebook are subject only to self-regulation and are allowed to freely share customer and user data, including nonpublic personal information, with other entities.[88]

1. How Banks and Financial Institutions are Distinguishable from Other Data-Driven Companies

There are three possible reasons why these exceptions and allowances exist under current regulatory regimes: (1) Congress may no longer value customer data privacy surrounding nonpublic personal information, (2) the law simply has not yet adapted to the changing landscape of data usage with the emergence of large data-driven companies, or (3) banks and financial institutions actually provide a distinguishably more vital and integral role in society, and as such warrant use of special regulations. This paper argues that the third possibility provides the true rationalization for why banks and financial institutions are treated and regulated differently than large data-driven companies.

Regarding the first possibility, to explain the lack of sweeping federal legislation on data privacy, we look at the possibility that Congress reversed its expressly stated policy position in favor of protecting individuals' data privacy through the regulation of banks' and financial institutions' handling of customer nonpublic personal information.[89] If Congress *did* in fact reverse its stance on the need for data privacy following the passage of the bipartisan Gramm-Leach-Bliley Act in 1999,[90] we would expect to see at least a partial repeal of privacy statutes related to the financial industry, particularly Sections 6801 through 6809, which refer specifically to the regulation of

87. 15 U.S.C. §§ 6801–6802(b)(2)(2012).

88. *See generally* GOOGLE, *supra* note 73; *see also* AMAZON, *supra* note 73; *Data Policy*, FACEBOOK, *supra* note 73.

89. *See generally* 15 U.S.C. § 6801(a).

90. *See Gramm-Leach-Bliley Act*, CONGRESS.GOV, https://www.congress.gov/bill/106th-congress/senate-bill/900/actions?q=%7B%22search%22%3A%5B%22gramm-leach-bliley%22%5D%7D&r=1&s=3 (last visited Mar. 18, 2019) (passing the Senate by a vote of 90-8, and the House by a vote of 362-57, indicating strong, bipartisan support in the 106th Congress).

financial institutions' handling of nonpublic personal information.[91] Since the Gramm-Leach-Bliley Act (especially the sections related to protecting nonpublic personal information) is still in effect today, we can assume that Congress has not reversed its position on the importance of data privacy.

Regarding the second possibility, to explain the discrepancy between regulations on financial institutions and large data-driven businesses such as Facebook, Google, and Amazon, we consider whether the law has adapted, or will adapt, to the changing nature of online privacy expectations with the emergence of such data-driven companies. As noted, there is no sweeping federal legislation that limits what companies such as Facebook, Google, and Amazon do with the data gathered through business operations.[92] Notably, however, and following the European Union's passage of a much stricter privacy law, the General Data Protection Regulation ("GDPR"), which both standardizes European Union privacy regulations and reinforces individuals' rights in the new era of large data-driven companies,[93] policy drivers in the United States (specifically policy drivers connected to the White House) are for the first time looking to implement "a consumer privacy protection policy that is the appropriate balance between privacy and prosperity."[94] If the United States adopted similar legislation to the GDPR, and if such new legislation also sought to standardize data privacy legislation and created meaningful, enforceable, and actionable data privacy rights in the era of large data-driven companies, data privacy concerns in the autonomous vehicle industry might be alleviated.[95] If no legislation appears in the near future to respond to large data-driven companies' appetite for user data, we must look to the third possibility below.

Finally, regarding the third possibility, to explain why banks' and financial institutions' handling of nonpublic personal information is regulated, while large data-driven companies' handling is not, we look to the nature of the services and products[96] provided by the various players. Large data-driven companies, such as Google, Facebook, and Amazon, offer both products and services.[97] Google offers a range of services, such as search

91. *See* 15 U.S.C. §§ 6801–6809 (2012).

92. *See* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law.

93. *See id.*

94. *See id.*

95. *See, e.g.*, *id.*

96. Referring to services and products available at the date of this writing.

97. *See, e.g.*, *Radically Helpful Things Made By Google*, GOOGLE, https://about.google./products/ [https://perma.cc/V7HB-WFXD] (last visited Mar. 18, 2019); *What Are the Facebook Products?*, FACEBOOK, https://www.facebook.com/help/1561485474074139 [https://perma.cc/4QQ6-2MTE] (last visited Mar. 18, 2019); *Amazon Echo – Black (1st Generation)*, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa-White/dp/B01E6AO69U [https://perma.cc/XF8Z-VPQ2] (last visited Mar. 18, 2019).

engine access,[98] cloud computing,[99] music services,[100] and much more to specific products, such as phones, tablets, watches, laptops, and more.[101] Facebook offers a social media forum for online interaction and data sharing, and various other products and services.[102] Amazon provides an online marketplace for consumers and sellers to browse, order, and review products and services, as well as other products such as computer hardware and services such as online video streaming.[103]

Each of these companies acquires nonpublic personal information from its users through voluntary information input (such as filling out name, address, and credit card fields), but also through habitual action, such as purchasing behavior, social connections, exchanges of messages, and search terms.[104] Banks and other financial institutions similarly acquire data from voluntary information input (such as name, address, social security number, and more), and can similarly analyze data sets, such as buying behavior, to determine a wealth of additional nonpublic personal information about an individual.[105]

There exists, however, a characteristic of the types of products or services offered that distinguishes banks and financial institutions from large data-driven companies: the widespread and therefore vital nature of the products and services offered to the public.[106] Conversely, there exist meaningful alternatives to using data-driven companies' products (such as using private browsing,[107] "offline shopping," and using other social networking means, such as text messaging or email). Thus, it is then easier to imagine why Congress would want to regulate data privacy for users of a vital service.

2. How Autonomous Vehicles Likewise Drift into Distinguishability

As there has not been any full or partial repeal of the relevant privacy legislation contained in the Gramm-Leach-Bliley Act, it is unlikely that

98. *See generally* GOOGLE, http://google.com [https://perma.cc/P85X-WK3T] (last visited Oct. 9, 2019).

99. *See* GOOGLE, https://blog.google/products/google-cloud/cloud-covered-what-was-new-with-google-cloud-in-september-2019/ [https://perma.cc/FY68-LN4F] (last visited Oct. 9, 2019).

100. *See* GOOGLE, https://play.google.com/music/listen?u=0#/sulp [https://perma.cc/3J6S-EQQJ] (last visited Oct. 9, 2019).

101. *See generally Radically Helpful Things Made By Google*, GOOGLE, *supra* note 97.

102. *See generally* FACEBOOK, https://www.facebook.com [https://perma.cc/LZX3-WSRH] (last visited Mar. 18, 2019).

103. *See generally* AMAZON, https://www.amazon.com [https://perma.cc/DNL7-7AGS] (last visited Mar. 18, 2019).

104. *See* GOOGLE, *supra* note 97; AMAZON, *supra* note 97; FACEBOOK, *supra* note 97.

105. *See* Gertz, *supra* note 58, at 944-46.

106. *See FDIC Survey*, *supra* note 54, at 1.

107. *See, e.g.*, *Browse in Private*, GOOGLE, https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en [https://perma.cc/7AVT-JNC4] (last visited Oct. 13, 2019).

Congress has backtracked on its policy stance on protecting individuals' nonpublic personal information. If the law is soon to adapt to the era of large data-driven companies, like the European Union has with the passage of the GDPR, the autonomous vehicle industry will likely see legislation passed to regulate private companies' handling of nonpublic personal information.[108] If Congress discriminates on industry regulation of data sharing based on the type and value of products and services offered, then the autonomous vehicle industry will also likely see legislation passed both to regulate nonpublic personal information and to reduce any chilling effect that may construct disincentives to autonomous vehicle use. Such legislative action would likely be supported because autonomous vehicles are a similarly vital service due to the fact that the service significantly reduces, or even eliminates, vehicle-related injuries and fatalities.[109]

The argument arises, of course, whether a meaningful alternative would exist to the use of autonomous vehicles. It is true that no Level 4 or above autonomous vehicles (vehicles that do not require human intervention for safe operations) are on the road as of the date of this writing, and thus the obvious meaningful alternative to an autonomous vehicle would be use of a Level 0, 1, 2, or 3 vehicle. It is also true that Level 3 and above vehicles would be able to operate safely in most instances even if there were vehicles on the road operated by humans.[110] While the alternative of driving a Level 0, 1, 2, or 3 vehicle may exist today, as autonomous vehicles become more commonplace in the future, individuals may not need to manually operate a vehicle as frequently as they do today. And as safe driving habits dwindle as time passes, the Level 0, 1, 2, and even some Level 3 alternatives would become less meaningful.

To further explain, as autonomous and self-driving technology continues to integrate into vehicles and as the technology becomes more mainstream, vehicle users will become accustomed to relying on such technology for vehicle operations. This will result in vehicle users losing the safe driving habits required for operation of a Level 0, 1, or 2 vehicle simply because they will not have had the opportunity to practice those habits in a Level 3, 4, or 5 vehicle. This trend would effectively render autonomous vehicle operation (that requires little or no human intervention) vital and widely integrated into society, thereby entitling its users to data protection (at least similar to the minimal protections offered under the Gramm-Leach-Bliley Act,[111] and at most under a new regulatory regime that grants full data protection to autonomous vehicle users).

Simply put, because autonomous vehicles and non-autonomous connected vehicles will reduce or eliminate vehicle-related injuries and

108. *See generally* Meyer, *supra* note 92.

109. *See generally* UNION OF CONCERNED SCIENTISTS, *supra* note 6; *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 6 at i.

110. *See* Kohler & Colbert-Taylor, *supra* note 14, at 103; *see also* UNION OF CONCERNED SCIENTISTS, *Self-Driving Cars Explained*, *supra* note 14.

111. *See generally* 15 U.S.C. §§ 6801–6809 (2012).

deaths,[112] autonomous and connected vehicles should be considered vital products and services. The benefits of autonomous and connected vehicles include utilization of technology that (1) enables vehicles to avoid other vehicles, humans, and obstacles,[113] (2) decreases medical expenses from vehicle-related injuries,[114] and (3) reduces traffic congestion through coordinated route-finding.[115] The avoidance of bodily harm through use of autonomous and connected vehicles is just as important as securing individuals' financial privacy in the banking and financial industry, and if Congress sees a legitimate need for data protection in the financial industry, Congress should see an equally, if not more, legitimate need for data protection in the autonomous vehicle industry. And as vehicles continue to increase in autonomy level (from Level 0, 1, and 2 up to Level 3, 4, and 5), driver skill level will decrease as humans relinquish more system management and drive operations to the vehicle's computers.[116]

Indeed, in a fully autonomous vehicle world, the need for driver education may no longer exist, which only increases the vital nature of the autonomous vehicle industry. As for the connected vehicles of today, and the autonomous and connected vehicles of the near future, the immediate benefits of crash avoidance[117] and traffic fatality and injury reduction[118] are sufficient to characterize the autonomous vehicle industry as "vital." Even if the autonomous vehicle industry is not considered "vital," the reasons posed still justify the argument for Congressional passage of legislative regulation to reduce the chilling effect of surveillance capitalism and incentivize autonomous vehicle usage because such vehicles can save lives, reduce vehicle-related injuries, and shorten commutes.[119]

B. The Adaptable Gramm-Leach-Bliley Template

The search for an adaptable regulatory framework brings forth the banking and financial industry. While the Gramm-Leach-Bliley Act may have flaws,[120] it is a good starting point because it regulates the use of nonpublic personal information in an industry fairly analogous to the autonomous vehicle industry.[121] Further, while the "flaws" under the Gramm-Leach-Bliley

112. *See* Juniper Research, *supra* note 26.
113. *See* Mattioli, *supra* note 21, at 279.
114. *See id.* at 279.
115. *See* Amon, *supra* note 3, at 353-54.
116. *See generally* Mich. Dep't of Transp., Impact of Automated Vehicle Technologies on Driver Skills (2016), http://www.cargroup.org/wp-content/uploads/2017/02/IMPACT-OF-AUTOMATED-VEHICLE-TECHNOLOGIES-ON-DRIVER-SKILLS.pdf. [https://perma.cc/DP24-JYAT].
117. *See* Mattioli, *supra* note 21, at 281-82.
118. *See* Juniper Research, *supra* note 26.
119. *See* Amon, *supra* note 3, at 353-54.
120. Such flaws include allowing banks and financial institutions to freely share their users' nonpublic personal information with the institutions' affiliates and marketing partners, even over a user's opt-out.
121. *See generally* 15 U.S.C. §§ 6801–6809 (2012).

Act may not sit well with certain users of banks or financial institutions,[122] the allowances granted by the Act may in fact function to protect the customer. It is possible that such information sharing between banks or financial institutions and their affiliates or marketing partners actually enables the institutions to offer tailored protective services and financial safeguards based on an individual's financial habits.

Thus, this framework would apply well to the autonomous vehicle industry, as the sharing of nonpublic personal information between vehicle manufacturers and their affiliates would be essential to the operation of the vehicle itself due to functions requiring connectivity.[123] Furthermore, sharing nonpublic personal information between autonomous vehicle manufacturers and marketing partners would allow manufacturers to present users with new features of the ever-developing product that best fit, and are most relevant to, the user's preferences and habits. Also, under the adapted Gramm-Leach-Bliley framework, the autonomous vehicle manufacturer would be able to pass along operational data, which would likely include nonpublic personal information, [124] to entities such as Congress, the Department of Motor Vehicles, the National Highway Traffic Safety Administration, and more in order to construct an overall picture of how autonomous vehicles are used, which can in turn provide valuable insight into how to improve the transportation system as a whole. Ideally, autonomous vehicle manufacturers would be willing to share the data with each other in order to work together to create a safer, more comfortable, and more efficient vehicle; however, "such data can give individual automakers a competitive edge,"[125] and is thus unlikely to occur.[126]

Of course, just like under the Gramm-Leach-Bliley Act,[127] autonomous vehicle users should be able to opt out of the information sharing mechanism between manufacturers and unaffiliated entities. As about 95% of customers of banks and financial institutions have declined to opt out under the Act, due to apparent lethargy when faced with the task of altering a default privacy setting,[128] it is possible that a similar percentage of autonomous vehicle users would also decline to opt out of the data sharing mechanism, which would allow regulatory bodies and transportation and safety entities to analyze data to research and implement system-wide improvements.

Thus, to maximize transportation safety, while incorporating data privacy concerns, Congress should legislate the use of vehicle data to allow a larger group of individuals, both data privacy-apathetic and data privacy-concerned, to enjoy the many benefits of autonomous vehicles.

---

122. *See* Gertz, *supra* note 58, at 983-84.
123. *See* Amon, *supra* note 3, at 342.
124. *See* Mattioli, *supra* note 21, at 288.
125. *Id.* at 279.
126. *See id.*
127. *See* 15 U.S.C. § 6802(b) (2012).
128. *See* McClurg, *supra* note 70, at 135.

IV. PROPOSED SOLUTION: "P.A.V.E.R."

Regulatory legislation passed by Congress is essential to deconstruct barriers to connected vehicle use (by avoiding the chilling effects of surveillance capitalism on purchases of such vehicles), similar to those possibly obstructing society's full embrace of the autonomous vehicle industry, so that more consumers buy vehicles with vehicle-to-vehicle ("V2V") capacity, which will in turn result in an increase in lives saved and injuries avoided.[129]

A. How the Adapted Gramm-Leach-Bliley Regulation ("P.A.V.E.R.") Would Work with the Autonomous Vehicle Industry

If Congress chooses not to pass sweeping federal privacy laws, similar to the General Data Protection Regulation in the European Union, and the U.S. maintains its current patchwork framework for data privacy regulation, Congress should implement an adapted Gramm-Leach-Bliley regulatory regime to the autonomous vehicle industry that focuses on the protection of users' nonpublic personal information. The proposed statutory regulation, which could be called the Privacy in Autonomous Vehicles and Enforcement Regulation, or "P.A.V.E.R.," would closely mirror the Gramm-Leach-Bliley Act, as codified under 15 U.S.C. §§ 6801–6809.[130] The purpose of P.A.V.E.R. would be to safeguard vehicle users' nonpublic personal information, while still allowing for fully functional operation of the vehicle to the extent necessary to reduce or eliminate bodily harms caused by vehicles.

Section 1 of P.A.V.E.R. would outline Congress's policy stance regarding the need to protect autonomous vehicle users' nonpublic personal information. It would also outline the unambiguous reasons for implementing P.A.V.E.R., including, similar to the Gramm-Leach-Bliley Act, the need to protect the "security and confidentiality of customer records and information," the need to "protect against any anticipated threats or hazards to the security or integrity of such records," and the need to "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[131]

Section 2 of P.A.V.E.R. would outline the vehicle manufacturers' disclosure obligations regarding data sharing policies. This provision would operate similarly to the corresponding Gramm-Leach-Bliley section in that manufacturers must provide notice of their sharing practices of users' nonpublic personal information with the manufacturers' marketing partners, affiliates, and other unaffiliated third parties in order to promote the manufacturers' business interests.[132] Just like in the Gramm-Leach-Bliley

129. *See* Juniper Research, *supra* note 26.
130. *See generally* 15 U.S.C. §§ 6801–6809 (2012).
131. *Id.* §§ 6801(b)(1)–6801(b)(3) (2012).
132. *See id.* § 6802.

Act,[133] if the vehicle user wishes to limit sharing of his or her own nonpublic personal information, Section 2 of P.A.V.E.R. would contain an opt-out mechanism (which must be clearly communicated to the customer) whereby the manufacturer must cease sharing that user's nonpublic personal information with unaffiliated third-party entities. Different from the operation of the corresponding Gramm-Leach-Bliley Act provision, [134] under P.A.V.E.R., the manufacturer must also cease sharing nonpublic personal information with affiliates and marketing partners. Note, however, that, § 6802(e) of the Gramm-Leach-Bliley Act also does not prohibit disclosing nonpublic personal information to unaffiliated third-party entities if it is "necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with . . ."[135] other services offered or maintaining or servicing the vehicle's hardware or software.[136] As such, similar to that corresponding provision,[137] such data sharing would be allowed if it proves essential to the vehicle's fundamental operation as outlined by the rulemaking bodies in Section 4 of P.A.V.E.R.[138] This is necessary to close the loophole in the Gramm-Leach-Bliley Act that can be exploited by some banks and financial institutions that allow such institutions to simply designate certain entities as "marketing partners" and continue business as usual. Further, and different from the Gramm-Leach-Bliley Act, this statute would also prohibit any downstream manufacturers or entities engaged in pre-sale handling of the vehicle from installing data collection devices or software, but would not prohibit aftermarket alterations. This section would additionally apply to domestic importation of autonomous or connected vehicles manufactured or handled by foreign entities, if the vehicles are intended for sale, or are actually sold, in the United States.

Section 3 of P.A.V.E.R. would set forth a requirement for autonomous vehicle manufacturers, at the time of the establishment of a customer relationship, to disclose to the customer the data privacy policy implemented in the vehicle, similar to the corresponding Gramm-Leach-Bliley provision.[139] This provision is necessary to ensure that the buyer is fully informed.

Section 4 of P.A.V.E.R., again, similar to the corresponding provision in the Gramm-Leach-Bliley Act,[140] would set forth the rulemaking power of the relevant federal agencies and administrations. Here, the Federal Trade Commission shall have the authority to prescribe such regulations as may be necessary to carry out the purposes of this subtitle with respect to any autonomous or connected vehicle manufacturer, as well as pre-sale entities that handle such vehicles. Notwithstanding the authority of the Federal Trade Commission, the Department of Transportation (and specifically the National

133. *See id.*
134. *See id.*
135. *Id.* § 6802(e).
136. *See id.*
137. *See id.*
138. *See, e.g.*, *id.*
139. *See* 15 U.S.C. § 6803 (2012).
140. *See id.* § 6804.

Highway Traffic Safety Administration, because it is an enforcement agency dedicated to avoiding bodily harm "through enforcing vehicle performance standards and partnerships with state and local governments"[141]) shall have the authority to prescribe such regulations as may be necessary to carry out the purpose of this subtitle with respect to any autonomous or connected vehicle manufacturer.

Section 5 of P.A.V.E.R., like the corresponding Gramm-Leach-Bliley Act provision,[142] would handle enforcement. The Federal Trade Commission and the Department of Transportation (especially the National Highway Traffic Safety Administration) shall enforce the regulations adopted pursuant to the statute generally. The U.S. Customs and Border Protection office will have the authority to inspect any imported autonomous or connected vehicles to ensure that such vehicles are imported by foreign manufacturers or other foreign entities that both have import permits and are certified to distribute vehicles in compliance with P.A.V.E.R.

Section 6 of P.A.V.E.R. would outline how P.A.V.E.R. interacts with other federal and state laws. Section 6 would also combine two sections in the Gramm-Leach-Bliley Act that correspond with this subject matter. In particular, just like the corresponding Gramm-Leach-Bliley provision, P.A.V.E.R. would only supersede inconsistent state laws, not more restrictive regulations.

Finally, Section 7 of P.A.V.E.R. would include relevant definitions, including, for example, the definition of a "manufacturer," and the definition of the terms "connected" and "autonomous" as they relate to vehicles.

B. Other Proposed Solutions to Data Privacy Issues

There are some legal scholars that view the Gramm-Leach-Bliley Act as insufficient to protect consumers' data privacy concerns.[143] Some call for a change to the Act's data sharing framework, and would prefer that consumers be opted-out of data sharing by default, rather than the Act's current default where customers are opted-in,[144] in order to avoid interfaces "deliberately designed to deter people from exercising their rights."[145] In fact, there is discussion by some scholars that collecting and selling "an extensive consumer data profile without consumer consent should be actionable under the privacy tort known as appropriation."[146] This notion, however, appears not to be explicitly supported by Congress as is evidenced both by the Gramm-Leach-Bliley Act's allowance of disseminating information under certain circumstances, even with customer opt-out,[147] and by the lack of

141. *The National Highway Traffic Safety Administration is Responsible for Keeping People Safe on America's Roadways*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/about-nhtsa [https://perma.cc/K8Q4-N252] (last visited Oct. 9, 2019).

142. *See* 15 U.S.C. § 6805 (2012).

143. *See, e.g.*, McClurg, *supra* note 70, at 133-37.

144. *See id.*

145. *See id.* at 135.

146. *See id.* at 69.

147. *See* 15 U.S.C. § 6802(b) (2012).

legislation pertaining to data use by large data-driven companies such as Google or Facebook.[148] Still, other legal scholars believe that data collection for online profiling (especially for targeted advertising purposes) constitutes an invasion of privacy that falls under a different privacy tort.[149] There has been no enforcement in the federal courts, however, of such proposed policies (although there is some state legal action towards this effect).[150] This evidence, as applied to the autonomous vehicle industry, indicates that it is unlikely, under today's common law or statutory framework, that autonomous vehicles would be subjected to a stricter data handling standard than large data-driven companies, which is why P.A.V.E.R. is needed.

More specific to the autonomous vehicle industry, there is actually some evidence that Congress previously split in its policy position on how to handle data sharing with connected vehicles.[151] This is evidenced by prior (but failed) Congressional consideration of conflicting legislation: one bill to "allow drivers to opt-out of vehicle location tracking altogether,"[152] and another bill that would "require mandatory data-sharing between automakers"[153] in order to streamline collision avoidance.[154] It seems obvious that *some* location tracking would be necessary for the products to function properly and to navigate the vehicle from one location to another. Thus, a complete opt-out of vehicle location tracking seems counterproductive to the goal of autonomous transportation. Conversely, if there was a statutory requirement for data sharing between automakers, competition could be dampened between manufacturers,[155] resulting in heavier scrutiny of the vehicle data in an attempt to analyze customer data to more effectively promote products,[156] which can ultimately lead to the chilling effect on individuals' freedoms of expression and association that Justice Sotomayor discussed in *United States v. Jones*.[157] P.A.V.E.R. would remove this chilling effect by allowing users to opt out of data sharing for marketing purposes, but compromise by allowing some data sharing for vehicle operation purposes.

Other legal scholars discuss the idea that connected and autonomous vehicle manufacturers should be forced to install the ability to interact with a portal that allows users to read manufacturers' privacy statements and either opt in or opt out of data sharing directly from the screen.[158] This solution to data privacy concerns is problematic because it substantially infringes on manufacturers' design autonomy. Rather than legislating the means by which users can interact with vehicles, Congress should legislate how manufacturers

148. *See* Meyer, *supra* note 92.
149. *See, e.g.*, Gertz, *supra* note 58, at 1004-05.
150. *See* Meyer, *supra* note 92.
151. *See* Mattioli, *supra* note 21, at 280.
152. *Id.*
153. *Id.*
154. *See id.* at 279.
155. *See id.* at 295.
156. *See id.* at 279.
157. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also* Mattioli, *supra* note 21, at 293.
158. *See* Amon, *supra* note 3, at 360-61.

handle nonpublic personal information while, importantly, allowing manufacturers the freedom to design an optimal vehicle that complies with the regulation. No matter the regulatory approach, the need for relevant data privacy law (whether common law or statutory regulation) is a prevailing element of many of the other proposed solutions both to the autonomous vehicle data privacy issue and to the perceived shortcomings of the Gramm-Leach-Bliley Act.[159]

V. CONCLUSION

Overall, there are still several questions that must be answered to provide an adequate solution to the issue of connected and autonomous vehicle data privacy. First, society must decide how much weight to give to data privacy concerns, which must then be adopted by Congress in order to accurately represent that societal stance. Although many privacy scholars and data experts have written on the issue, if society, for the most part, is not as concerned with data privacy as the experts are, then data privacy regulations may be largely unnecessary. Second, the issue of timing must be addressed. Although vehicle manufacturers are in the process of rolling out autonomous vehicles,[160] transportation users are not yet heavily exposed to such vehicles, and may not yet feel that the sanctity of their nonpublic personal information is truly compromised. Conversely, connected vehicles capable of similar data collection are increasingly prevalent in society.[161] Although some may see the issue of vehicle-related data privacy as an issue for the future, careful monitoring of the industry's progress is necessary to decide when regulation is needed, and allowing ample time to formulate and pass such regulations must be taken into account.

Nonetheless, just as commerce and financial security would likely crumble without banks, so too would future transportation systems suffer from increased dependency on autonomous features without autonomous vehicles. As such, both the financial industry and the autonomous vehicle industry qualify as vital industries (especially in the near future), but only the financial industry has regulation that deconstructs barriers to use. While financial security is extremely important, so too is the avoidance of bodily injury and death due to autonomous vehicles' superior safety capabilities. Further, as is discussed in the introduction,[162] individuals must have the ability to control how vital industry entities, such as autonomous vehicle manufacturers, use their nonpublic personal information in order to streamline

159. *See generally* Mattioli, *supra* note 21, at 277-98; Glancy, *supra* note 79, at 1171-1239; McClurg, *supra* note 70, at 63-143; Gertz, *supra* note 58, at 944-1018; Amon, *supra* note 3, at 329-61; Kohler & Colbert-Taylor, *supra* note 14, at 100-38.

160. *See, e.g.*, Giambrone, *supra* note 16.

161. *See* Juniper Research, *supra* note 26.

162. *See supra* Section I.

the transition to "safer, smarter, and more efficient roadways."[163] Thus, the roads of the future require P.A.V.E.R.

163. *See* Amon, *supra* note 3, at 361.

Unpacking the Affirmative Act Distinction: An Analysis of the Applicability of Carpenter v. United States to Location Data Stored by Ride-Hailing Companies

Conor Kelly*

TABLE OF CONTENTS

*J.D., May 2020, The George Washington University Law School; B.A., with high distinction, History and Government, May 2016, University of Virginia. This Note is dedicated to my parents: my father, Peter Kelly, and mother, Ellen O'Brien Kelly. Without their enduring support and love, I would not have had the good fortune to pursue a career in the law. Their grace, compassion, sensibility, and heart are ideals that I strive to bring to everything that I do. I must add a final and immesaurable thank you to the staff of the Federal Communications Law Journal for their tireless and brilliant editorial work.

I. INTRODUCTION

Reacting to the Supreme Court's recent opinion in *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018), Lior Strahilevitz, professor at the University of Chicago Law School, posed the following hypothetical:

> Witness sees [an] Uber black car speeding away from hit & run accident scene in [New York City] but doesn't see [the] plate or driver. [The government] wants Uber to give it names of Uber drivers [and possibly their passengers] who were near [the] scene at the time [of the accident]. After Carpenter, does the government now need a search warrant?[1]

This Note seeks to provide at least one way of thinking about–and possibly an answer to–that very question. It will address the Supreme Court's decision in *Carpenter v. United States*, in which the Court held that accessing personal location information stored by a service provider on an individual's cell phone constitutes a search under the Fourth Amendment, and the application of the principles announced and discussed in that opinion to the context of ride-hailing mobile applications, particularly Uber.[2] In so doing, it will argue that the Court has good reason in this context to read the *Carpenter* decision beyond the strict parameters of its facts. Specifically, in situations where the government seeks access to stored location information from third-party ride-hailing applications (e.g. Uber), courts should apply a multi-factor analysis, proceeding from the baseline principles articulated in *Carpenter*, looking to such factors as the type of record being collected, the pervasiveness of the data at issue, the sophistication of the technology, and the degree to which individuals are able to freely consent to the sharing of their personal location information in a digital setting.

Section I will begin by outlining the contours of the Fourth Amendment and exceptions to the warrant requirement. Section II will then seek to explain *Carpenter* in the context of Fourth Amendment case law and draw principles and future lessons from the decision itself. Section III will consider how ride-hailing apps function, how Americans think about privacy in the digital realm, and how these principles, both narrow and broad, might come into play in future cases. Finally in Section IV it will argue that courts should extend the rationale of *Carpenter* to require that in order for the government to access user location information gathered by ride-sharing applications in any situation it must first acquire a warrant. Doing so would be a doctrinally sound extension of *Carpenter*'s holding and would reflect a broader policy goal of ensuring that the law reflects evolving, modern expectations of privacy in an increasingly digitally interconnected social

---

1. Lior Strahilevitz, *The Path to Carpenter v. United States and Possible Paths Forward*, TECHNOLOY ACAD. POL'Y (July 23, 2018), https://www.techpolicy.com/Blog/July-2018/Path-to-Carpenter-v-United-States-and-Possible-Pa.aspx [https://perma.cc/PXT8-48H7].

2. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

sphere where intensely personal information is communicated in the furtherance of simple tasks.

II. BACKGROUND: THE FOURTH AMENDMENT AND EXCEPTIONS TO THE WARRANT REQUIREMENT

The Court's holding in *Carpenter* aligns with the Court's frequent assertion that "the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable' under the Fourth Amendment – [and] subject only to a few specially established and well-delineated exceptions."[3] In *Carpenter*, police had made use of an already existing statutory scheme to gain access to a voluminous sum of personal data gathered by an individual's cell phone and stored by his service provider.[4] In the case of stored location information in the ride-hailing context, the potential route to accessing such data may well be more complicated, but no less insidious. As is well known, however, there are several exceptions to the warrant requirement that are "jealously and carefully drawn."[5]

Perhaps most importantly, Fourth Amendment rights, like several other constitutional rights, may be waived when one consents to search of his or her person or premises by officers who have not complied fully with the Fourth Amendment.[6] In the context of everyday, in-person citizen to police encounters, this plays out in what is perhaps a predictable and familiar manner. In a previous case explaining voluntary consent, for example, police had stopped a car and asked its occupants if they could search the vehicle–the defendant simply replied "Sure, go ahead."[7] The Court found no Fourth Amendment violation, noting that one of the defendants even attempted to aid in the search.[8] Given such facts, it may well seem apparent that such an exception reasonably furthers legitimate police interests.

The ever-increasing attenuation of the personal, immediate interaction between individual and law enforcement, however, adds a vexing complication to the familiar consent exception known as the third party doctrine: law enforcement can obtain consent from a person or entity other than the person who is being searched.[9] Traditionally, the Supreme Court held that third party consent was sufficient if that party "possessed common authority over or other sufficient relationship to the premises or effects sought

3. Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (quoting Katz v. United States, 389 U.S. 347, 347 (1967)); G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 358 (1977).

4. 18 U.S.C. § 2703(d) (2012).

5. Jones v. United States, 357 U.S. 493, 499 (1958).

6. *See* Amos v. United States, 255 U.S. 313, 317 (1921).

7. Schneckloth v. Bustamonte, 412 U.S. 218, 221 (1973); *see also* Smith v. Maryland, 442 U.S. 735, 739 (1979).

8. *Schneckloth*, 412 U.S. at 221.

9. *See* Illinois v. Rodriguez, 497 U.S. 177, 183 (1990).

to be inspected."[10] Now, however, actual common authority is no longer required.[11] Prior to the advent of the digital age, the third-party consent question most often arose in the context of relatively immediate interpersonal interactions: a landlord agreeing to the search of an apartment, a hotel clerk allowing the search of a guest's room, or a babysitter who allows police to search the house .[12] Now, with private companies having access to a wealth of digital information about individuals' daily lives, the same question requires a different kind of thinking. This note in particular seeks to address how the Court might think about the third-party consent exception in an as-yet unaddressed area: user location information stored by ride-hailing companies.

III. *CARPENTER V. UNITED STATES*: WHAT SHOULD THE PROPER POST-CARPENTER TEST BE FOR NEW TECHNOLOGIES?

It is this issue that brings us to *Carpenter*, the Court's most recent and significant pronouncement on the third-party doctrine and on the application of the Fourth Amendment to new types of technology and stored information. What this Note argues is that the *Carpenter* Court, despite overtures to the contrary, provided a blueprint for how to address the question of whether police gaining access to other types of stored location information constitutes a search under the Fourth Amendment.[13] In the case itself, the Court professed to seeking a narrow solution, whereby a limitation to the third-party consent doctrine in the digital era was recognized when the type of record at issue was collected automatically and was comprehensive in its reach into the intimate details of an individual's life.[14] This section will turn first to the facts of *Carpenter* itself and its reasoning, before providing a more detailed consideration of its discussion of the third-party doctrine and recent cases, and then turning to contrasting evaluations of *Carpenter's* rationale.

Police in *Carpenter* had arrested four men suspected of committing a series of robberies.[15] One of the group provided officers with the cell phone numbers of the other alleged accomplices, including Carpenter's number.[16] Acting on this data, the FBI obtained court orders through the Stored Communications Act whereby law enforcement only had to put forward "specific and articulable facts" in order to gain access to Carpenter's location data from his service provider.[17] The collected information was voluminous–

10. United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that valid consent existed where police searched the bedroom of defendant and woman with whom he was living agreed to the search).

11. *See, e.g.*, *Rodriguez*, 497 U.S. at 184 (1990).

12. *See* Chapman v. United States, 365 U.S. 610, 612 (1961); Stoner v. California, 376 U.S. 483, 485 (1964); United States v. Sanchez, 608 F.3d 685, 689 (10th Cir. 2010).

13. *See Carpenter*, 138 S. Ct. at 2220 (noting that "[the Court's] decision today is a narrow one . . . .").

14. *See id.* at 2217.

15. *Id.* at 2212.

16. *Id.*

17. *Id.* (quoting 18 U.S.C. § 2703(d)).

it showed a comprehensive pattern of Carpenter's personal movement over a period of weeks, tracked based on his phone automatically sending signals to cell towers (a process colloquially referred to as "pings.").[18] As suspected, for the crimes in question the data showed Carpenter to be in the immediate vicinity of the robbed locations for each of the alleged incidents.[19] The data took center stage at his trial and, despite numerous attempts to suppress, its introduction led to his conviction.[20]

Presented with the question of whether the police search of the stored location information, collected by the service provider, constituted a search under the Fourth Amendment, the Court answered in the affirmative. It began its analysis by reflecting on the centrality of cell phones in modern American life, noting that "[c]ell phone location information is detailed, encyclopedic, and effortlessly compiled."[21] In the digital age, this would seem a necessary preface to the basic conception of the Fourth Amendment as protecting the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[22] While the opinion itself disavows any affirmative implications for other types of technology, its suggestion at various points that future analyses will be highly fact-specific is worth noting.[23] The Court's emphasis on the intimacy of personal digital data, even when held or (in theory) owned by third-party companies, belies a more fundamental aversion to modes of police surveillance that simply co-opt existing third-party technology. Much of the Court's opinion actually appears to rely on the fact that while the cell-site location information ("CSLI") at issue in the case might not have been extremely pervasive, the technology itself is headed in an incredibly sophisticated and pervasive direction.[24] The introduction of new technologies, new devices, and new tracking technologies only serve to reinforce the basic point that this new digital environment constitutes an essential aspect of Americans' personal lives.

A. The Third-Party Doctrine and Carpenter

To an outside observer, the Supreme Court's Fourth Amendment jurisprudence certainly seems convoluted. Even in *Carpenter* itself, members of the Court could not avoid quibbling over whether it might be best to return to a property-based conception of the Amendment's protections.[25] But in the main the Court has remained true to the fundamental precept that "[T]he Fourth Amendment protects people, not places," if not without some

18. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
19. *See id.*
20. *See id.* (the government had claimed that the records in question had "clinched the case.").
21. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).
22. *Id.* at 2213 (quoting U.S. CONST. amend. IV, § 1).
23. *See id.* at 2221-22.
24. *See Carpenter*, 138 S. Ct. at 2218 (citing *Kyllo v. United State*s, 533 U.S. 27, 36 (2001)).
25. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (Kennedy, J., dissenting); *see also Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (urging a return to a property-based conception of the Fourth Amendment's protections).

detractors from both sides of the legal spectrum.[26] While *Carpenter* might have presented a novel question, it relied in good part on history and tradition, holding clearly that Fourth Amendment analysis "is informed by historical understandings 'of what was deemed an unreasonable search and seizure when the Fourth Amendment' was adopted."[27] The amendment's protections work to "secure 'the privacies of life' against 'arbitrary power."[28] Perhaps more importantly, the Court reiterated that "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance."[29] Summarizing the Court's development of Fourth Amendment jurisprudence in *Carpenter*, Chief Justice Roberts explained that the Court has, since its decision in *Katz v. United States*, "expanded [its] conception of the Amendment to protect certain expectations of privacy."[30] In so doing, the Court began to develop a balancing scheme designed at least in part to respond to emerging societal privacy concerns in an increasingly digital and interconnected world, where personal information is collected and shared as a necessary part of everyday life.[31]

In seeking to solve questions involving "personal location information maintained by a third party," the Court stated that its analysis will be informed by two related "lines of cases."[32] The first, perhaps predictably, concerns what the Court has said about what an individual's expectation of privacy is in his physical location and movements.[33] Most recently, in *United States v. Jones*, "five Justices agreed that . . . privacy concerns would be raised by . . . [the government] conducting GPS tracking of [Jones'] cell phone."[34] The Court in *Carpenter* held that an individual has a reasonable expectation of privacy in one's physical location and movements.[35] The "second set of decisions" refers to the so-called third-party (consent) doctrine, which attempts to define the distinction between "what a person keeps to himself and what he shares with others."[36] In essence, the third-party doctrine holds that there is no "legitimate expectation of privacy" in information voluntarily given to a third-party vendor.[37] In *United States v. Miller*, the Court made clear that this also applies "even if the information is revealed on the assumption that it will be used only for a limited purpose."[38] The doctrine's analysis necessarily includes "the nature of the particular documents

26. Katz v. United States, 389 U.S. 347, 351 (1967). *But see* Kyllo v. United States, 533 U.S. 27, 42 (2002) (Stevens, J. dissenting).
27. *Carpenter*, 138 S. Ct. at 2214 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).
28. *Id.* (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
29. *Id.* at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).
30. *Id.* at 2210.
31. *See id.* at 2210-11.
32. *Id.* at 2215.
33. *Id.*
34. *Id.* (citing *United States v. Jones*, 565 U.S. 400, 430 (2012)).
35. *Id.* at 2212.
36. *Id.* at 2216.
37. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
38. United States v. Miller, 425 U.S. 435, 443 (1976)

sought."[39] In *Smith*, for example, the Court considered the use of a "pen register," a type of wiretapping device used to record outgoing calls from a landline phone.[40] There the Court declined to extend the Fourth Amendment's protections, finding instead that the device had "limited capabilities" and that individuals don't really maintain a "reasonable expectation of privacy in the numbers they dial."[41]

In a modern world defined more by the ubiquity of cellphones than rotary phones and pen registers, however, Americans may well view the same question differently. Indeed, Justice Marshall in dissent in *Smith* presaged many of the concerns with the third-party doctrine that the Court later touched on in *Carpenter*, stating forcefully that he "remain[ed] convinced that constitutional protections are not abrogated whenever a person apprises another of facts valuable in criminal investigations."[42] Notably, Justice Marshall pointed out that "inherent in the concept of assumption of risk is some notion of choice."[43] In order to be thought of as taking on the chance that one's personal information might ultimately be accessed by the government, one must have an actual, even-handed choice in the matter; and yet "unless a person is prepared to forgo the use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[44]

In *Carpenter*, the Court seems to have sought a middle ground. While not jettisoning the idea of consent entirely, the Court endeavors to develop a way in which consent can be thought of in a useful way in the digital context. In this effort, the Court offers the notion of "affirmative act" as a plausible way of determining consent in an increasingly convoluted technological environment.[45] The Court mentions this idea of an "affirmative act" in attempting to explain why it did not make sense to think of Carpenter as somehow consenting to the sharing of his personal location information given the fact that at no point did he have to expressly agree to said sharing.[46] A person carries his cell phone simply as a fact of life, the Court reasoned, and as such it cannot be said that an individual engages in an "affirmative act"

39. *Id.* at 442.

40. *See Smith*, 442 U.S. at 742. It is worth noting, further, that a pen-register tracks only outgoing phone numbers. As such, while it remains a wire-tapping device in the technical sense, this meaning may not accord with modern perceptions of what wiretapping might entail.

41. *Id.* at 742-43; *see also Carpenter*, 138 S. Ct. at 2215 (quoting *Smith*, 442 U.S. at 742).

42. *Smith*, 442 U.S. at 748 (Marshall, J., dissenting).

43. *Id.*

44. *Id.*

45. Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

46. *See id.* at 2211.

consenting to the sharing of highly personal data.[47] The Court in *Carpenter* then began its reasoning for declining to extend the third-party doctrine to cell-site location information ("CSLI") by noting that the technology of CSLI itself was "qualitatively different" and "unique."[48] In assessing whether the "logic" of the third-party doctrine should apply to CSLI, the Court holds out a slightly refined notion of consent as a basis for determining when and where to apply the third-party doctrine to evolving, modern technologies.[49] This necessarily involves an assessment of the ways in which the nature of the technology at issue affects the consent question. One can see this in the way that the Court cites the "qualitatively different" nature of CSLI, where it appears to suggest that the analysis is more-or-less case-by-case.[50] While in doing so the Court refrains from engaging in the sweeping type of constitutional pronouncement which might stir the hearts of privacy advocates, it at least purports to be attentive to the various and perhaps uncontemplated ways in which new technologies (each with their own applications) may fall within or outside of the third-party doctrine depending on their precise characteristics.[51]

What is more, the Court's discussion of the question of when to apply the third-party doctrine centers on the issue of increased technological sophistication: the wireless carriers at issue in the case are "ever alert" and possess "nearly infallible" memories.[52] And yet "an individual's reduced expectation of privacy in information knowingly shared with another 'does not mean that the Fourth Amendment falls out of the picture entirely."[53] Paramount, the Court intimated, is the pervasiveness of the technology itself and whether there are any inherent limitations on how far the technology in question might reach.[54] This multi-factor approach has the advantage of allowing the Court to mold its analysis to the circumstances as required; indeed, it is the same type of approach that allowed a majority of the Court to find that a "longer term GPS monitoring of . . . a vehicle traveling on public streets constitutes a search" in *United States v. Jones*.[55]

Underneath the surface in the Court's discussion of the third-party doctrine and its refusal to extend the doctrine to the "qualitatively different"

---

47. *See id*. It is worth noting, in this light, that the Court's opinion does not emphasize nor even make reference to Carpenter's act of signing a cell phone contract with his service provider as perhaps constituting an "affirmative act" sufficient to qualify as consent to location sharing. This might tend to suggest that the similar act of signing a privacy policy or analogous document in the ride-hailing context is not itself dispositive on the question of consent. This is in contrast to the dissents of both Justice Kennedy and Justice Thomas, who make a point of emphasizing Carpenter's act of signing a cell-phone contract as critical. *See id.* at 2225 (Kennedy, J., dissenting); *id.* at 2235 (Thomas, J., dissenting) ("Neither the terms of his contracts nor any provision of law makes the records his.").

48. *Id.* at 2212.

49. *Id.*

50. *Id.*

51. *See id.* at 2220.

52. *Id.* at 2221.

53. *Id.* (quoting *Riley v. California*, 134 S. Ct. 2473, 2488 (2014)).

54. *See id.* at 2222.

55. *Id.* at 2220 (Alito, J., concurring in the judgment) (citing *United States v. Jones*, 565 U.S. 400, 430 (2012)).

category of CSLI is the notion that the doctrine itself may have made sense at a time when tracking technology was far less sophisticated but perhaps cannot stand with the same force in the modern, digital age. Indeed, the notion that modern GPS tracking or other surveillance technologies might have sufficient "limiting capabilities" so as to justify application of the doctrine (as the pen register did in *Smith*) seems rather quaint given the proliferation of these technologies.[56] The Court's consideration of the subject raises a point originally made by Justice Marshall in dissent in *Smith*–namely the idea that no matter the extent of the invasion, one may well think that the breach itself cannot be thought of as the product of free and voluntarily provided consent where the technology in question constitutes a personal or professional necessity.[57]

As such, the Court's analysis of the "second rationale" behind the third-party doctrine–voluntary exposure–is necessarily tied to its consideration of the pervasiveness and sophistication of the technology at issue.[58] Noting the unique qualities of CSLI, the Court posited that the concept of voluntary exposure simply does not make complete sense when applied to CSLI.[59] For a start, the Court noted that "[c]ell phone location information is not truly 'shared' as one normally understands the term."[60] The Court then relied on its decision in *Riley* to argue that because cell phones are so ubiquitous, such an "insistent part of daily life," they are "indispensable to participation in modern society."[61] Simply put, it cannot be categorically asserted that an individual has "voluntarily exposed" himself to surveillance by virtue of his carrying a cell phone in public–as doing so is no different from his waking up in the morning and walking out the door. It is in this context that the Chief Justice explains that because Carpenter had not engaged in any "affirmative act" consenting to exposure of his personal location information but had instead simply existed in public with his phone on his person–as everyone does–he cannot be thought of as having agreed to invasive sharing of his personal location.[62]

The precise issue of whether an individual engages in an affirmative act consenting to the conveyance of his personal location information stored by a ride-hailing company, therefore, seems to pose a more difficult, closer question. The Court's explication of the "affirmative act" concept in *Carpenter* is, admittedly, rather terse and perfunctory; the term itself appears only once in the opinion, where the Court explains that a "cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up [the phone]."[63] As such, the Court reasons, one does not "truly share" cell phone location information in the ordinary

56. *Id.* at 2215 (citing *Smith v. Maryland*, 442 U.S. 735, 742 (1979)).
57. *See Smith*, 442 U.S. at 748 (Marshall, J., dissenting).
58. *Carpenter*, 138 S. Ct. at 2215.
59. *Id.*
60. *Id.* at 2220.
61. *Id.* (citing *Riley v. California*, 134 S. Ct. 2473, 2476 (2014)).
62. *Id.* at 2220.
63. *Id.*

sense.[64] The Court adds that this notion of one not truly sharing CSLI is bolstered by the fact that cell phones as a technology are incredibly "pervasive" to the point that having one is "indispensable to participation in modern society," negating the idea that free choice might have been possible.[65] Nonetheless, the Court admits that its use of the term "affirmative act" is meant to nod at the Court's discussion of assumption of risk in *Smith*, noting that "virtually any activity" on one's cell phone creates CSLI and that, "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[66]

B. How Lower Courts Have Been Implementing Carpenter: Teasing Out Lessons from Recent Interpretations

In *Carpenter*'s wake, lower courts have not had a terribly fulsome opportunity to consider its potential implications. Many recent decisions have sought simply to delineate situations where *Carpenter* clearly does not apply; consider a recent district court opinion in *People v. Torres*, which simply noted that *Carpenter* does not "address the constitutionality of search conditions imposed pursuant to probation or parole."[67] In *Torres* and similar cases, lower courts seem to be paying a good deal of attention to the nexus between the place where the search is conducted (as being somewhere where a law enforcement officer could otherwise lawfully be) and the sophistication of the technology being employed to obtain the evidence in question.[68] This seems to be in line with the principles distilled from *Carpenter*, where the Court devoted much of its discussion to the sophistication of CSLI technology and to whether the concept of voluntary exposure is tenable in the context of providing location information to third parties. The defendant in *United States v. Kubasiak*, for example, sought to use *Carpenter's* reasoning to assert that using a video camera to record a person's backyard 24 hours a day over several months violates reasonable expectations of privacy–but the Court there held that this argument ignores a critical element of the Court's reasoning in both *Jones* and *Carpenter*: because the surveillance camera was fixed, it could observe the defendant in only one location (i.e. his backyard).[69] This same argument has also been rejected in the case of pole cameras.[70]

It should be noted that the analysis, as the Court urged in *Carpenter*, centers here on the perceived pervasiveness of the technology, looking to what area is being intruded upon and what if any steps individuals have taken

---

64. *Id.*
65. *Id.*
66. *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)).
67. People v. Torres, Super. Ct. No. SCN362581, 2018 WL 5004764, at *26 (Cal. Ct. App. Oct. 16, 2018)
68. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *3 (E.D. Wis. Oct. 05, 2018).
69. *Id.* at *4.
70. *See* United States v. Houston, 813 F.3d 282, 285 (6th Cir. 2016).

to prevent such intrusion. These recent cases seem consistent with the growing perception that tracking or surveillance technology that follows an individual constantly is sufficiently concerning so as to be constitutionally significant.[71] Static surveillance, as was at issue in the previously mentioned cases, seems to be something that people find inherently less invasive; when surveillance follows you, and the government can potentially gain access to a type of technology that keeps track of one's physical location over several places, such as one's destinations of travel, route of travel, among others, individuals seem more prepared to consider that invasion as infringing upon their basic rights and personal dignity.[72]

Some of these very recent considerations of *Carpenter* should offer a clue for the future. Lower courts have thus far had relative success in undertaking the type of multi-factor analysis urged in *Carpenter*, focusing on how much of an aggregate account of a person's life the technology in question seems to capture and whether it is similar in sophistication to that described in *Carpenter*–i.e. the "intimate details of everyday movement."[73] Lower courts in the wake of *Carpenter* seem to be suggesting a constitutionally significant nexus between the place where the information is being collected, whether such place is somewhere a law enforcement officer could otherwise be lawfully, the sophistication of the technology used to acquire the information (including whether that technology will grow more invasive), and just how aggregate of a picture the technology captures of a person's daily life.[74] The greater the nexus, the reasoning appears to be, the more likely a person can be considered to have a reasonable expectation of privacy in such information that is "voluntarily" conveyed to a third party.[75] This approach is in line with the multi-factor, fact-specific approach of *Carpenter*. As such, courts in the post-*Carpenter* world should endeavor to take into account the implications of technological growth for purposes of assessing expectations of privacy and consent.

If thought of this way, this string of factors offers a principled way of determining where the Court should apply sensible exceptions to the third-party doctrine in light of developing technology, weighing such factors as pervasiveness and advancing technological sophistication against the issue of whether an individual can be considered as engaging in an "affirmative act" consenting to the sharing of one's location information.[76] This argument applies with force to the ride-sharing context. Based on the Court's rationale in *Carpenter*, a warrant should be required to access individuals' location information when the technology at issue is both pervasive enough to reveal

---

71. *See Carpenter*, 138 S. Ct. at 2216; *cf.* United States v. Jones, 565 U.S. 400, 430 (2012).

72. *See* Aaron Smith, *Shared, Collaborative, and On Demand: The New Digital Economy*, PEW RES. CTR.: INTERNET AND TECH. (May 19, 2016), http://www.pewinternet.org/2016/05/19/the-new-digital-economy/ [https://perma.cc/AQ5N-XBAX].

73. *See Carpenter*, 138 S. Ct. at 2217.

74. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761 at *3-4 (E.D. Wis. Oct. 05, 2018); *cf.* United States v. Jones, 565 U.S. 400, 406 (2012).

75. *Carpenter*, 138 S. Ct. at 2216.

76. *Id.* at 2214.

intimate details of one's life (and promises to grow more sophisticated) and when circumstances strongly suggest that an individual could not be thought of as providing genuine consent to the sharing of that information.

C. Varying Assessments of Carpenter and its Implications

The *Carpenter* decision's muddling of the third-party doctrine gained immediate attention. Orin Kerr, a noted Fourth Amendment scholar, has noted that the *Carpenter* opinion seems to go so far as to introduce what he calls an "equilibrium-adjustment cap" on the third party doctrine.[77] By this, it is meant that the decision aims to adjust the scope of the amendment's protections in light of new facts and technology in order to maintain a baseline level of liberty against unjustified intrusions of government power.[78] As Kerr aptly suggests, *Carpenter* appears to say that where the third-party doctrine would seem to give the government unduly expansive powers, the doctrine itself should not apply; this distinction, he notes, is borne out by the text of the opinion itself, where the Court notes that there is "a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected . . . today."[79] It is a distinction worth noting, for the future debate on this issue may well center on how "exhaustiveness"–or, to put it another way, technology's pervasiveness–is to be defined.

Much discussion in the wake of the Court's pronouncement has attended to what, if any, other types of location information might be implicated either by the ruling itself or by suggestions that one might reasonably draw from the Court's reasoning.[80] Kerr himself, in a draft chapter of a new book on the Fourth Amendment in the digital age, has recently put forth the argument that the user-location records of ride-hailing services do not constitute examples of data collection that should trigger a search.[81] Kerr argues, in the main, that *Carpenter* should apply to Internet (digital) records once three requirements are satisfied: the records must "exist because of the digital age," they must be "created without meaningful voluntary choice," and they must "tend to reveal the privacies of life."[82] He proceeds to argue, albeit briefly, that Uber location records do not satisfy this test at least under the

---

77. Orin S. Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE BLOG (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/P7W6-6UPG] [hereinafter Kerr, LAWFARE BLOG]; *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 490-91 (2011).

78. *See* Kerr, LAWFARE BLOG, *supra* note 77.

79. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2216).

80. *See, e.g.*, Andrew Guthrie Ferguson, *Future Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [http://perma.cc/W8B4-7CTR].

81. Orin S. Kerr, Implementing Carpenter, THE DIGITAL FOURTH AMENDMENT (Oxford University Press, forthcoming) (2019), USC Law Legal Studies Paper No. 18-29, https://ssrn.com/abstract=3301257 [https://perma.cc/5GUF-FE8F] [hereinafter Kerr, THE DIGITAL FOURTH AMENDMENT].

82. *See id.*

second prong and potentially under all three.[83] The remainder of this Note, accordingly, will seek to demonstrate why that view does not constitute the best reading of *Carpenter* as applied to ride-hailing location data records. To begin with, it will argue that the proper post-*Carpenter* test is not as narrow as Kerr suggests. It will first explicate the functioning of ride-hailing apps and look to prevailing attitudes concerning such apps' collection of data. Having done so, it will turn to what this Note considers the proper test for *Carpenter* searches and argue why ride-hailing location data meets that test. In particular, it will endeavor to explain why Carpenter's affirmative act distinction proves unhelpful in this context and why looking for meaningful voluntary choice is not fully satisfactory when many individuals in fact rely on ride-hailing services for freedom of movement.[84] In order to consider how a broader reading of *Carpenter* would apply to the ride-hailing context, it will first be necessary to consider the precise functioning of these services.

IV. THE PROLIFERATION OF RIDE-HAILING APPLICATIONS IN AMERICAN LIFE AND IMPLICATIONS FOR POLICE SURVEILLANCE

Because the precise legal questions involved appear to turn on application of the third-party doctrine and specifically on an analysis of how *Carpenter's* affirmative act distinction holds up in the ride-hailing context, it will first be necessary to consider the precise manner in which ride-hailing applications operate, and the degree to which individuals understand how ride-hailing companies function and their expectations of privacy in information collected by those companies in the course of soliciting their services. Having done so, Section IV will argue that in light of the relative sophistication and pervasiveness of ride-hailing services, the way in which individuals interact with said services, and the complications attendant to consent in the digital realm, a person does not truly consent to the sharing of their personal location information when using a ride-hailing service.

Ride-hailing apps have transformed from a relatively novel concept to an increasingly present role in American life within a span of less than a decade, particularly for young urban Americans.[85] Uber is now a 15-billion-dollar company with over 750,000 drivers in the United States alone.[86] What is more, these apps offer and provide something that taxi companies cannot: individualized, location-based services with a pre-set charge.[87] Indeed, this rise to prominence has been so rapid as to generate relatively little litigation involving direct police action.[88] And yet one-in-five Americans have used a

83. *See id.*
84. *See* Smith, *supra* note 72.
85. *See id.*
86. Sara Ashley O'Brien, *Uber Has More Work to Do Winning Over Drivers*, CNN BUSINESS (Dec. 18, 2017), https://money.cnn.com/2017/12/18/technology/uber-drivers-180-days-of-change/index.html [https://perma.cc/EKT3-4YB6].
87. *See* Smith, *supra* note 84.
88. *Id.*

ride-sharing app.[89] Coverage is highly concentrated in cities and relatively sparse in rural areas–only three percent of rural residents have used such an app.[90] And while the tracking technology used by these companies to gather users' locations has only grown more sophisticated, until the Court's decision in *Carpenter* this past term, a potential constitutional problem with obtaining access to this information may well have seemed remote.[91] Such expansion makes it all the more likely that courts will have to address difficult legal questions related to the privacy of information shared with and processed by such companies, just as courts have had to address a variety of questions surrounding the privacy of information stored by cell phone companies as those companies have grown more technologically sophisticated and put out increasingly high-tech products.[92]

In principle, the technology at issue in *Carpenter*–CSLI–and the type of GPS technology used by ride-hailing companies such as Uber are remarkably similar. Indeed, insofar as GPS tracking provides the same type of data–i.e. an individual's location over time–it parallels the type of GPS device at issue in *United States v. Jones*.[93] Whenever an individual walks or otherwise exists in public, that person's cell phone routinely sends or "pings" location signals to nearby cell towers; using the information gathered from several cell towers, it is possible to "triangulate" a phone's location (and thereby, almost invariably, a person's).[94] In this basic respect, the precision of the respective technologies is almost exactly parallel. Uber, as a typical example:

> [C]ollects location information when the Uber app is running in the foreground. In certain regions, Uber also collects this information when the Uber app is running in the background of your device if this collection is enabled through your app settings or device permissions.[95]

This is distinct from the "ping" function of almost all modern cell phones. Location tracking in the ride-hailing context arises when that particular service is solicited by the phone user–not so with ordinary "pings" to cell towers; put in simpler terms: if someone has started running the Uber app on a phone in order to solicit a car, that person's location will be tracked.[96]

---

89. *Id.*

90. *Id.*

91. *See, e.g.*, Andrew Hawkins, *How Uber Moves the 'Blue Dot' to Improve GPS Accuracy in Big Cities*, THE VERGE (Apr. 19, 2018), https://www.theverge.com/2018/4/19/17252680/uber-gps-blind-spot-shadow-maps [https://perma.cc/7A9B-YNZ5].

92. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2476 (2014) (holding that police must obtain a warrant before conducting a search of an individual's phone and its contents).

93. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (where the Court concluded that the placing of a physical tracker on a car constituted a search).

94. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

95. *See Privacy Policy*, Uber Technologies, Inc. (May 25, 2018), https://privacy.uber.com/policy [http://perma.cc/RW94-HYDR].

96. *See id.* (noting that "if you are a rider and have provided permission for the processing of location data, Uber collects location information when the Uber app is running in the foreground. In certain regions, Uber also collects this data when the Uber app is running in the background of your device if this collection is enabled through your app settings or device permissions.").

Moreover, unless that individual has not deliberately disabled the tracking function through accessing the app settings, the app will continue to track a user's location "in background," even though the person may be doing other things on the phone such as texting or calling.[97] This means that so long as the user has not specifically closed that app, one's location will be tracked for a brief period; for Uber, until as recently as 2017 this meant that users continued to be tracked for a short window after they left vehicles and entered buildings.[98]

Uber, to its credit, seeks to provide law enforcement authorities with guidance regarding what procedure the company will follow in the event that police contact the company for information. Its guidelines, however, are unsettlingly permissive. According to Uber's "Guidelines for Law Enforcement Authorities," police must create an online account through the "Uber Law Enforcement Response Team" and submit any requests for information through an online portal.[99] In one subsection, Uber states the following:

We require a subpoena issued in connection with an official criminal investigation to compel the disclosure of basic information. A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel our disclosure of certain communications between people using Uber or GPS location information.[100]

The policy goes on to state that:

> Exceptions to these requirements may be available for emergency and exigent requests, where a user has provided consent, or–for requests that do not require a warrant–where other legal or regulatory standards apply.[101]

This vague reference to "consent" without express definition of the term makes Uber's policy ripe for abuse, threatening to swallow the company's self-imposed requirements.[102] By its own terms, Uber's policy does clearly delineate the circumstances in which a user would be understood as having provided consent. Must the user expressly agree? Is his or her use of the app enough? These would seem to be important questions but their resolutions are left unclear. The lack of a clear definition of what is meant by consent in this

97. *See id.*

98. *See* Laurel Wamsley, *Uber Ends Its Controversial Post-Ride Tracking of Users' Location*, NAT'L PUB. RADIO (Aug. 29, 2017, 05:41 PM), https://www.npr.org/sections/thetwo-way/2017/08/29/547113818/uber-ends-its-controversial-post-ride-tracking-of-users-location [https://perma.cc/SRV9-QYQE].

99. *Uber Guidelines for Law Enforcement Authorities – United States*, Uber Technologies, Inc. (last visited Feb. 28, 2019), https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=guidelines-for-law-enforcement.

100. *Id.*

101. *Id.*

102. *Id.*

context necessarily raises the issue of how that very concept is to be understood in the digital age.

If a user does not exercise the option to disable the tracking function of the Uber app, the resulting location data can provide an extensive window into a person's physical movements over a prolonged period, similar to the CSLI data profile at issue in *Carpenter*.[103] Uber keeps location data about past rides stored off-site.[104] During each ride, Uber stores a number of data points, the most salient of which are: a user's pickup location, drop-off location, precise route path, and duration of trip.[105] Interestingly, available data tends to show that a majority of adults say they are either not too confident or not at all confident that records of their activity maintained by their own cellular telephone company would remain private and secure.[106] While Americans understand that "modern life won't allow them to be 'left alone' and untracked, they do want to have a say in how their personal information is used."[107] 74 percent say it is "very important" to be in control of who can get personal information and 65 percent say it is "very important" to control what personal information is collected.[108] In terms of how aware people are of how their information will be used once shared, 47 percent of people said they were unsure of how their personal information would be used by companies; 91 percent of adults either agree or strongly agree that consumers have lost control of how personal information is collected and used by companies.[109] Indeed, this would seem to undercut the notion that individuals have true choice in the digital realm; if individuals see that they are provided the option of allowing or disallowing location tracking but already believe that they do not have free control over that choice, it undermines the concept of consent in this context.

In terms of the sensitivity of personal location information, 50 percent of people state that the details of one's physical location over time are "very sensitive," and another 32 percent agree that such information is "somewhat sensitive."[110] These attitudes involve implicit assumptions about "privacy tradeoffs," including the "likelihood of getting spam, the risk of data breaches, [and] the special intimacy tied to location data."[111] The most strongly negative reactions in this poll came in the context of scenarios involving the sharing of personal location data. One respondent even went so

---

103. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (explaining how CSLI tracks personal movements over a prolonged period).

104. *See Privacy Policy*, *supra* note 95 (discussing information created when individuals use the service, including "location, usage, and device information.").

105. *See id.*

106. *See The State of Privacy in America*, PEW RES. CTR. (Jan. 20, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/9CAN-UYUW].

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR.: INTERNET AND TECH. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ [https://perma.cc/Z9F9-SVT9].

far as to say that he "continually den[ies] location services" on his smartphone out of a desire to block ads.[112] It would be concerning indeed, in this light, for location data to be collected ostensibly so that a ride-hailing company can improve its service or lower rates, but then also employed for police to have a more efficient tracking system for people without expressly violating privacy rights.

V. APPLICATION OF CARPENTER'S RATIONALE TO RIDE-HAILING LOCATION DATA

A. Technological Sophistication and Pervasiveness: Records of the Digital Age and Privacies of Life

Under the proper post-*Carpenter* framework, the Court should turn first to a consideration of how pervasive and sophisticated a particular tracking technology is. This is borne out by the Court's fact-heavy discussion in *Carpenter* itself, detailing the precise functioning of CSLI and how much data it captures.[113] It is also borne out by the Court's attention to the fact that the CSLI technology at issue in the case was then just beginning to grow in sophistication and capability: only getting better, more sophisticated, and better able to see exactly where an individual has travelled.[114] As such, the Court need not be tied to the exact mechanics of the technology with which it is faced and can instead take notice of the abstract, big picture: to what degree of sophistication a technology can reasonably be thought of as heading. This type of broader approach takes account of increasing technological sophistication in a way that is inherently more pragmatic, treating new forms of technology and tracking for what they actually are: substantively different settings entirely, where old modes of thinking may not necessarily translate neatly. Now, Prof. Kerr says that the first consideration in post-*Carpenter* cases in the digital sphere should be whether the records at issue exist "because of the digital age."[115] Although his framework takes account of such issues as sophistication and pervasiveness later on, this specific formulation risks making the analysis overly narrow. Moreover, the very answer to that question requires a definition of the "digital age" and its consequences.

Opponents such as Kerr also point out that because cab companies have compiled records of trips in the past, courts now need not be concerned about Uber location records as a new type of data record.[116] Yet this misses the forest for the trees. In pulling back to a broad level of abstraction, this argument seeks to indicate that this type of record, in its most basic form, in fact has a long history. But in so doing it clouds the nature of the technological revolution that enabled Uber to track and collect user data. Uber in fact collects extremely precise information: where an individual called for a ride,

112. *Id.*
113. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
114. *Id.* at 2215.
115. Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.
116. *Id.*

where that individual was picked up, how long the ride to the destination took, and what exact route that individual used.[117] That precision and sophistication is itself possible because of the advent of GPS technology and the feasibility of recording that information digitally. It would certainly be unrealistic to expect a cab company as recently as the 1980s to be capable of compiling such extensive information.

When one takes full stock of the nature of the information that ride-hailing services collect, moreover, it seems doubly unrealistic to think that records of one's comings and goings will not "tend to reveal the privacies of life" in the same way as CSLI data that shows one's location over a period of weeks.[118] Having access to the details of an individual's trips to and from specific locations, at specific times and along exact routes may indeed provide a window into that person's intimate associations and affiliations. In this respect, it would seem a vapid distinction to say that CSLI data is pervasive enough to risk revealing one's personal associations and yet the records of where an individual chooses to travel is not at least similarly revealing. If, as the *Carpenter* Court held, the "mapping [of] a cell phone's location over the course of 127 days provides . . . an intimate window into a person's life," and if further it is true that this window reveals "familial, political, professional, religious, and sexual associations," then it is difficult to imagine how a comprehensive record of one's Uber trips over the course of even one or two weeks would not also tend to reveal an individual's political, professional, and personal associations.[119] This may well include, as Justice Sotomayor aptly points out in her concurrence in *Jones*: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club . . . the gay bar and on and on."[120] One would be hard pressed indeed to find that ride-hailing location records don't tend to reveal intimate associations in the same way as GPS data did in *Jones*.

B. The Affirmative Act Distinction in the Ride-Hailing Context: How to Assess the Consent Issue as Applied to Ride-Hailing Location Data

Given the similarities outlined earlier between CSLI and the GPS location information stored by Uber and similar ride-hailing applications, the remaining question of whether a user of a ride-hailing app can be thought of as consenting to the sharing of his or her physical location information comes to the fore. Under the *Carpenter* framework, the question in the digital, ride-hailing records context turns on the Court's usage of the phrase "affirmative acts" and its analysis thereof.[121] The crux of the Court's argument was that

---

117. *See Privacy Policy*, *supra* note 95 (discussing information created when individuals use the service, including "location, usage, and device information.").

118. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

119. Carpenter v. United States,138 S. Ct. 2206, 2217 (2018); *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

120. *Jones*, 132 S. Ct. 565 U.S. at 415 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-42 (2009)).

121. *Carpenter*, 138 S. Ct. at 2214.

Carpenter did not engage in any "affirmative act" consenting to his constant tracking by his phone company but instead simply carried his phone on his person, as most people do; as such, he cannot be thought to have "agreed" or "consented" to his tracking in any traditional or even ordinary sense.[122] As mentioned, Orin Kerr interprets the Court's discussion of the same subject to contend that a user of a ride-hailing app does in fact engage in "meaningful voluntary choice" when using the service so as to lose Fourth Amendment protection.[123] Among the reasons he offers for why a user does in fact provide meaningful consent in this setting is the notion that users remain free to exercise other, less invasive travel options such as taxi cabs, buses, subways, or personal vehicles.[124]

Such questions necessarily raise the issue of what the very notion of "being free" means in the context of digital interactions. The concept of voluntary exposure in the ride-hailing context poses new questions and several factual distinctions from the CSLI-*Carpenter* context. Whereas individuals owning a cell phone carry their phones with them in public as a fact of life, all individuals need not download a ride-hailing app or otherwise engage in that service as a part of existing in society in the same way. A user of a ride-hailing service, moreover, might be thought of as engaging in several "affirmative acts" consenting to exposure of location information, including the act of downloading the app itself and failure to exercise the option of disabling automatic GPS tracking. It certainly is also true to an extent that in at least some instances users will remain free to solicit other travel options. What these and other distinctions fail to take stock of, however, is the fact that many individuals in fact rely or may in time rely on such services for personal freedom.[125] As the Court mentioned in *Carpenter*, and as Justice Marshall suggested in dissent in *Smith*, in considering whether a particular type of location information is "truly shared as one normally understands the term," attention must be given to whether an individual had actual, free choice in exercising the affirmative acts previously described.[126]

Assessing consent in this context requires a wide-angle lens. The percentage of people actively employing the use of a ride-hailing app is far from ubiquitous.[127] While ride-sharing applications function in a distinct way to the ordinary carrying of a cellphone, lower courts do not seem to have analyzed thus far whether that distinction is enough of a difference to warrant a different constitutional outcome.[128] Comparing any particular technology or

122. *Id.* at 2219-20.

123. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

124. *See id.*

125. *See* Smith, *supra* note 72 (explaining that 80% of users feel than ride-hailing apps offer good job options for those wanting flexible work schedules, as well as a routinely cheaper method of transport that traditional cab services).

126. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); *see also* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting).

127. *See* Smith, *supra* note 72 (noting that 15 percent of American adults have used a ride-hailing service).

128. *See* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *3-4 (E.D. Wis. Oct. 05, 2018) (finding no reason to extend protection to minimally invasive technologies).

service to the cell phone, however, is not in an especially useful distinction given the uniquely ubiquitous status of that technology. A broader view is necessary to inform the discussion and to reveal how the interactions and perceptions of Americans in the digital realm color the analysis of consent.

It might be useful for a court to use the kind of analysis undertaken in *Kubasiak* to inform its consideration of whether the third-party doctrine should apply.[129] The *Carpenter* Court certainly seems to be saying that in determining whether to apply the third party doctrine, a number of factors matter, including: sophistication of technology, the breadth of information collected, the personal and intimate detail of one's physical movements, among others.[130] By focusing on these factors, the *Carpenter* Court was able to make clear the stakes involved: access to technology that keeps an exacting track of an individual's precise location over several days (and weeks) implicates privacy concerns in a way that society is apt to regard as unreasonable.[131] This is quite similar to the nexus idea suggested earlier. That is to say, the most sensible post-*Carpenter* approach would seem to be undertaking an intense analysis of the mechanisms of the technology in question and making a determination of just how intrusive it might be.[132]

As argued, in the ride-sharing context each factor seems to tip the balance in favor of privacy and protection. The standout contravening factor, then, would appear to be the fact that users must download and thereby seemingly consent to a ride-hailing service's tracking system. The question, as such, seems to become whether an individual's failure to disable location information tracking constitutes an "affirmative act" that can be seen as constituting consent to ride-hailing location tracking.[133] Failing to do so, or failure to exercise other potential affirmative acts (such as choosing to take the bus), however, should not constitute an affirmative act under the *Carpenter* framework because it is both inconsistent with the way the Court discusses privacy expectations in that case and because doing so would constitute a misguided way of thinking about the interaction between individuals and modern digital technology.

While perhaps no technology may rise to the level of ubiquity and personal significance as that achieved by the cell phone, ride-hailing apps have become a key element of the American digital landscape and in in the lives of their users; by overwhelming margins, users of such services agree that the services themselves save users time and stress, provide decent work for those who desire flexible hours, and serve as a critically important option for older adults with limited mobility.[134] Ride-hailing services for many individuals serve vital interests of personal autonomy, work freedom,

---

129. *See id.*

130. *Carpenter*, 138 S. Ct. at 2220-21 (detailing the ways in which CSLI offers a deeply personal look into an individual's physical movements).

131. *See id.*

132. *See* Ferguson, *supra* note 80 (suggesting an ad-hoc approach might be best suited to modern developments).

133. *Carpenter*, 138 S. Ct. at 2220.

134. *See* Smith, *supra* note 72.

mobility, and personal safety.[135] Interestingly enough, however, the same study previously cited found that the issue of privacy concerns "largely fails to register with ride-hailing users," with users rejecting "by a five-to-one margin" the "notion that these services collect too much personal information."[136] Those who use such services on a less-than-weekly basis are largely unsure on the same question.[137] Indeed, this might be read as reflecting broader public skepticism at being able to realistically preserve privacy upon entering and engaging with the digital realm.

Another relevant consideration in this context is the way in which Americans writ large think about their interaction with new ride-hailing services. An inherent assumption of the third party doctrine as announced in both *Smith* and *Miller* is that, as the *Carpenter* Court surmised, individuals have reduced expectations of privacy in information conveyed to third parties.[138] As Justice Marshall's dissent in *Smith* seems to have presaged, it is becoming increasingly apparent that Americans are in fact becoming more closely guarded in terms of information that they provide to third parties; Pew Research shows that a majority of Americans remain wary of the growth of surveillance: a majority (57 percent) consider it unacceptable for the government to monitor the communications of U.S. citizens.[139]

With this context in appropriate focus, it would seem that the very concept of consent in the context of the digital interaction is a somewhat shaky one. Indeed, given the way in which people interact with modern technology, the affirmative act distinction fails to serve as a completely satisfactory effort at line-drawing. Individuals are rarely if ever asked, and yet are apparently expected, to consent to constant location tracking as a fact of life. The notion that individuals forfeit Fourth Amendment protection by somehow choosing to solicit a ride-hailing service that utilizes location tracking fails to take proper cognizance of individuals' relation to the digital realm. Because ride-hailing services for many individuals broaden the ability and access to travel so as to enable increased mobility and thereby greater personal autonomy, can it truly be said that such an individual engages in a genuine choice to reveal one's location data through the use of a ride-hailing service?[140] Is that choice not thrust upon them as a result of circumstances outside of any one individual's control? One may indeed counter that an individual retains the option of not soliciting the service at all, as Kerr contends, but for individuals who rely on such services for basic autonomy that would seem to ring hollow.[141]

Consider also the sheer volume of interaction that individuals undertake with digital applications and the attendant wealth of user-agreements that a user must encounter: one study in particular indicates that for the average

---

135. *See id.*
136. *Id.*
137. *Id.*
138. *Carpenter*, 138 S. Ct. at 2215.
139. *See* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting); *see also The State of Privacy in America*, *supra* note 106.
140. *See* Smith, *supra* note 72.
141. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

American interacting in the digital realm, it would take 76 eight-hour work days to read all the privacy polices one encounters in a year.[142] Would it not be reasonable to say, therefore, that meaningful consent in this area is a hollow term so long as Americans do not have another feasible option but to participate in the digital sphere? Richard Epstein, along these lines, argues that "[t]he automated nature of ubiquitous and involuntary [digital] connection undercuts the consensual nature of the exposure."[143] This goes to the same point: the digital world, with all of its connections, requires individuals, to engage both instantly and fully in order to function in the same fashion as everyone else. If the initial decision to engage is itself not truly voluntary, then the idea that someone can somehow provide meaningful consent in each minute interaction, especially when such an interaction involves location tracking, seems to fail.

To argue that an individual somehow consents to revealing personal information simply through using a ride-hailing service when he or she has other options available also does not accord with many of the Court's prior statements on this issue. At least one amicus brief in *Carpenter*, for example, emphasized a point made by Justice Sotomayor in her concurrence in *Jones* that "[t]he third-party doctrine's central tenet . . . does not . . . accord with the expectations most people have when transmitting information for a specific purpose."[144] One might readily think of a ride-hailing app in a similar fashion; a user of such an app expects to convey location information specifically so as to enable the trip in question and in all likelihood does not expect to have his or her whereabouts become, by virtue of the limited trip, public knowledge.

Even prior to the Court's recent expression of doubt towards the third-party doctrine, at least some commentators were beginning to recognize the growing failure of the doctrine to accord with developing, modern expectations of privacy. With regard to stored location information, one scholar at least has pointed out that it is "unreasonable to consider data somehow 'not private' if the information, like CSLI, is generally exposed only to automated systems rather than human employees."[145] Indeed, in the ride-sharing context–location data is similarly stored in an off-site automated program, tending to diminish the notion that the location data is not private by virtue of its sharing with a third party.[146] That thinking extends to the idea

142. Lorrie Faith Cranor & Aleecia McDonald, *The Cost of Reading Privacy Policies*, 4:3 I/S: A JOURNAL OF L. & POL'Y FOR THE INFO. SOC'Y 546, 554-58 (2008); *see also* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/JJ8A-6KVU].

143. *See* Richard A. Epstein, *Privacy And The Third Hand: Lessons From The Common Law Of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1206 (2009).

144. *See* Brief of Scholars of Criminal Procedure and Privacy in Support of Petitioner, p. 16, Carpenter v. United States, 138 S. Ct. 2210 (2018) (quoting *United States v. Jones*, 565 U.S. at 417 (2012) (Sotomayor, J., concurring)).

145. *Id.* at 17 (quoting Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 611-27).

146. *See Privacy Policy*, *supra* note 95.

that the doctrine even properly applies in situations where the government simply seeks to compel the production of evidence rather than conduct a search.[147] Here, the implications of holding that the government does not always need a warrant in order to collect stored location information obtained through third parties would be grave indeed. In effect, the government could simply outsource a highly sophisticated system of surveillance created and deployed by ride-hailing companies with thousands of employees, all while avoiding the costs of developing new tracking technology and being subject to exactly none of the privacy rights that citizens have come to expect; it is a concern that tracks with the Court's recent expression of skepticism of broadly invasive surveillance techniques.[148]

This would seem to be supported by data detailing how few people actually understand how ride-sharing apps collect user data; statistics cited above show that few if any users of Uber actually are aware of how the app stores their location data and few if any are aware that there is an option for disabling the tracking function.[149] It is reasonable to think that individuals might be unaware of such options precisely because they understand that in order to participate in the modern digital public environment on an even plane with others, they cannot simply detach themselves from its pervasive interconnectedness; this is especially true for individuals who actually need ride-hailing services to enable work freedom.[150]

And yet this very point seems to admit of something of a sliding scale of voluntary exposure and expectations of privacy. Should the notion that an individual at least has somewhat practical access to alternate forms of transportation, for example, matter in how a court conducts its analysis? Admittedly, an individual might easily find alternative forms of transport–be they public (subway, public bus) or semi-private. Indeed, this forms a key part of Kerr's argument for why Uber-location records would not be protected.[151] While individuals who may actually rely on private ride-hailing apps for freedom and mobility might have a stronger claim to be considered as not engaging in voluntary exposure by virtue of their use of such apps, can the same truly be said for individuals not reliant on such apps for personal travel? In the case of such individuals, the fallback necessarily seems to be the foundational expectation that one has a reasonable expectation of privacy in the intimate details of physical location and movement, as articulated in *Carpenter*.[152] Indeed, if the nature of the physical movement in itself is indistinguishable between the two classes of individuals, whereas the reasons

147. *See, e.g.*, Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 121 (2002).

148. *See* Riley v. California, 134 S. Ct. 2473, 2478 (2014) (holding that the government must obtain a warrant to search the contents of an individual's cell-phone); *see also* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine does not make sense in a world of rapidly expanding technologies and shifting privacy expectations).

149. *See* Smith, *supra* note 72.

150. *See id.*

151. *See* Kerr, THE DIGITAL FOURTH AMENDMENT, *supra* note 81.

152. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

for engaging in such transport may be different, perhaps there can be no tenable difference between the two.

When thinking of the issue principally in terms of consenting to the tracking itself, much of the reasoning of *Carpenter* translates to this new context. The concept of affirmative acts may yet be a principled distinction for some types of technology, where it might be possible to hold individuals to a clearer, more express standard of consenting to tracking. In the context of personal travel, however, where physical location is implicated, the affirmative act distinction fails to capture the full breadth of how people interact with modern technology and what their expectations are. To say that a user retains other, less personally invasive options does not capture the breadth of the problem and fails to take stock of the challenges and realities consumers face in the digital world.

VI. CONCLUSION: RE-CONCEPTUALIZING PRIVACY IN STORED LOCATION INFORMATION IN THE DIGITAL AGE

This Note is not meant to suggest or urge that the same conclusion should follow in the context of other types of stored location information. Instead it argues in sum that in the future analyzing questions of this sort not only depends upon a detailed analysis of the type of technology at issue and just how personal the information collected through it is, but also on a fundamental rethinking of the idea of consent itself in the context of new technologies in light of the way that the modern citizen engages with an ever-expanding grid of collected information. To his credit, Kerr seems to agree that measured analysis of a given technology's pervasiveness and sophistication is critical in this context. What his analysis seems to miss, however, is a framing of the consent question that makes intuitive sense in light of modern, personal interactions in the digital sphere. The affirmative act framework may yet prove to be a useful basis for distinguishing when a particular user of a technology can be thought of as having consented to tracking or other revealing of personal information in such a way as to provide an exception to the Fourth Amendment's requirements. In the context of the ride-hailing app, however, it fails to provide a fully satisfactory way of framing the issue.

Carpenter itself was a narrow decision, and while this Note argues it can be read more broadly there may yet be room for principled distinctions where the Court allows for limited, required disclosures.[153] Arguments limiting *Carpenter* to its facts risk overlooking the ways in which tracking methods used by ride-hailing services intrude into the personal sphere; CSLI was often indicative of the "general area" someone was in, but rarely ever indicative of the exact places someone had been and exact routes of travel.[154] As courts continue to grapple with the question of just how sophisticated and pervasive a particular technology must be before protection can be extended,

153. *See id.* at 2214-15.
154. *Id.* at 2211.

a more ready solution might perhaps be found within the halls of Congress. The House of Representatives is in the process of conducting hearings on the subject of the need for a new comprehensive federal privacy and consumer protection law.[155] Putting aside for the moment the question of what precise form any bill should take, and perhaps the larger questions swirling in consumer protection circles, a law of this form would be a welcome addition to the legal landscape. Testimony provided this February has already emphasized that individuals are often compelled to engage with the current digital environment in a way that does not suggest the presence of genuine choice.[156] The lack of a sufficiently clear legal answer to the problem suggests that it is time for the people at large to express their will, so as to clearly define consent in this new context.

155. *See Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection and Commerce of the H. Comm. on Energy and Commerce*, 116th Cong. (2019).

156. *See id.* (statement of Nuala O'Connor, President and CEO, Center for Democracy and Technology).

The Automated Tipster: How Implicit Bias Turns Suspicion Algorithms into BBQ Beckys

Christine Kumar*

TABLE OF CONTENTS

* J.D., May 2020, The George Washington University Law School, May 2020. Notes Editor, Federal Communications Law Journal, Vol. 72. B.A. Political Science, Johns Hopkins University, 2016. This Note is dedicated to my parents, Hannah and Suresh Kumar, and my sister, Cynthia Kumar, for their continued support and love and for inspiring me everyday. I would like to thank Dean Renée McDonald Hutchins for her guidance and scholarship on this subject as well as the Federal Communications Journal Vols. 71-72 staff for their work on this Note. I would also like to thank Emily S. Haselton for her work and support while writing this Note. And finally I would like to thank Daniel Wolman, Caitlyn Kretzschmar and Jarrod Carman for their support on this Note and throughout my time at GW.

I. INTRODUCTION

#BBQBecky, one of several satirical hashtags that went viral this summer, refers to Jennifer Schulte, a white woman who called the police on a group of black people barbecuing at an Oakland park after the group refused to stop grilling.[1] The group of black people were using a charcoal grill in a non-charcoal designated area, a rarely enforced rule considered "not a police matter."[2] The video, which captured only twenty minutes of a three-hour phone call Ms. Schulte had with the police department, shows Ms. Schulte on the phone reiterating that this specific area is not designated for charcoal grilling.[3] Despite the hesitations from dispatch and even a recommendation that Ms. Schulte be evaluated for a temporary psychiatric hold, the police eventually arrived and questioned the group of grilling black residents for over an hour.[4] While no arrests were made or citations issued, this successful dispatch of police for implicitly racially motivated reasons, involving no emergency, is just one example of how police are operating on, or are led to operate on, racist biases.[5] In fact, several hashtags, including #BBQBecky, #PermitPatty, and #CornerstoreCaroline, have become part of a national discourse as a response to these videos capturing white people alerting the police to, or threatening to call the police on, people of color doing similarly minor or non-criminal activities, including sleeping in their own dormitory or sitting at a Starbucks.[6] While these hashtags do bring some levity to these overt demonstrations of racism, the videos they are inspired by expose the weaponization of law enforcement against people of color in order to police social norms instead of actual criminal conduct.[7] This kind of policing—unnecessary interactions with lawful black Americans based on racial biases—concerningly results in increased instances of police violence leading to countless murders of innocent, non-threatening black Americans by police

1. Tom Cleary, *Jennifer Schulte, 'BBQ Becky': 5 Fast Facts You Need to Know*, HEAVY.COM (Jun. 23, 2018, 5:54 PM), https://heavy.com/news/2018/05/jennifer-schulte-bbq-becky/.

2. *Id.*

3. *Id.*; *see also* Hilary Hanson, *Listen to Full 911 Audio of 'BBQ Becky' Calling Cops on Black Men Grilling*, HUFFINGTON POST (Sept. 2, 2018, 1:56 PM), https://www.huffingtonpost.com/entry/bbq-becky-911-calls-grill_us_5b8c0f07e4b0162f4724a74c.

4. Hanson, *supra* note 3.

5. *See id.*; Jeffery Robinson, *Let's Address the Ridiculous 911 Calls that People of Color Endure*, THE HILL (June 11, 2018), https://thehill.com/opinion/civil-rights/391639-lets-address-the-ridiculous-911-calls-that-people-of-color-endure.

6. Jessica Guynn, *BBQ Becky, Permit Patty and Why the Internet is Shaming White People Who Police People 'Simply for Being Black*,*'* USA TODAY (July 23, 2018, last updated 12:17 PM), https://www.usatoday.com/story/tech/2018/07/18/bbq-becky-permit-patty-and-why-internet-shaming-white-people-who-police-black-people/793574002/; Gina Martinez, *Woman Dubbed 'Cornerstore Caroline' Faces Backlack After Falsely Accusing a 9-Year-Old Boy of Sexual Assault*, TIME (Oct. 16, 2018), https://time.com/5426067/cornerstore-caroline-backlash-sexual-assault-boy/.

7. Robinson, *supra* note 5.

officers.[8] In fact, this kind of police brutality and subsequent lack of justice, such as the acquittal of Trayvon Martin's killer, has sparked the Black Lives Matter movement.[9]

Under the Fourth Amendment, an officer must be able to demonstrate reasonable articulable suspicion (RAS) in order to legally conduct a stop under *Terry v. Ohio*.[10] Generally, given the risk of consequences for a false report, tips from a reliable source are sufficient to meet the RAS standard in order to conduct a stop, whereas anonymous tips require further corroboration in order to meet the standard.[11] The recent trend in inflammatory 911 calls made by white people against black people doing non-criminal activities demonstrates the need for higher scrutiny from police responding to 911 calls. Most states criminalize those who make false police reports with punishments including misdemeanor or felony charges, and several jurisdictions are even starting to introduce legislation that would criminalize 911 calls against people of color when there is no evidence of wrongdoing.[12]

While greater attention is being paid to these discriminatory calls to the police, both publicly and in terms of legal action, other prejudiced alerts to the police are not always as flagrant as #BBQBecky. With the rise of Big Data and data mining,[13] law enforcement agencies have begun to use computers and software in order to aid in crime prevention.[14] More specifically, "predictive policing," an evolving trend in law enforcement, uses data analyses and criminology theories in order to create models that can anticipate when or where a crime will occur.[15] In theory, these models, which are based on numerical statistics and scientific data, should offer neutral and accurate findings and thus lead to a more efficient and better-informed criminal justice

---

8. I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1254 (2017); Ryan W. Miller, *Black Lives Matter: A Primer on What it Stands for*, USA TODAY (July 11, 2016, 9:53 PM), https://www.usatoday.com/story/news/nation/2016/07/11/black-lives-matter-what-what-stands/86963292/.

9. *Id.*

10. Terry v. Ohio, 392 U.S. 1 (1968).

11. Florida v. J.L., 629 U.S. 266, 270 (2000).

12. *See generally* S.C. CODE ANN. § 16-17-722 (2012); CAL. GOV'T CODE § 53153.5 (2012); MICH. CODE § 750.411a (2012); N.J. CODE § 2C:28-4 (2012); *see also* Morgan Gstalter, *NY State Senator Wants to Criminalize Calling 911 on Law-Abiding Black People*, THE HILL (Aug. 16, 2018, 4:00 PM), https://thehill.com/homenews/state-watch/402211-ny-state-senator-wants-to-criminalize-calling-911-on-law-abiding-black.

13. Steve Lohr, *How Big Data Became So Big*, N.Y. TIMES (Aug. 11, 2012), https://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html?auth=login-smartlock ("Big Data is a shorthand label that typically means applying the tools of artificial intelligence, like machine learning, to vast new troves of data beyond that captured in standard databases. The new data sources include Web-browsing data trails, social network communications, sensor data and surveillance data."); Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 3 (2005) (Data mining is the "computer application of statistical formulas to large bodies of data to identify relationships or patterns," specifically "identifying people who fit a designated computer-generated profile.").

14. Michael L. Rich, *Machines as Crime Fighters*, 30 CRIM. JUST. 10 (2016).

15. Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, 41 N.Y.U. REV. L. & SOC. CHANGE 327, 334-35 (2017).

system.[16] However, the software and tools used by the police, including something known as Automated Suspicion Algorithms (ASAs), have demonstrated that these technologies inherit and further perpetuate implicit biases that could lead to discriminatory police alerts similar to those made by a #BBQBecky or a #PermitPatty.[17] However because these predictive policing technologies are trusted to theoretically eliminate any bias involved with human judgment, they are able to function without any of the scrutiny or risk of punishment that bigoted tipsters are now facing when they wrongfully alert the police.[18]

This Note will address the issue of how the police, in employing Big Data tools like data mining and machine learning, perpetuate discriminatory and harmful policing biases similar to stereotypical 911 callers, but without any of the scrutiny or legal recourse available to remedy these prejudices. It will argue that in order to prevent discrimination in predictive policing, the police should abide by the reasonable articulable suspicion standard as applied to anonymous tips before stopping an individual pegged by a predictive policing tool.[19] More specifically, this Note calls for any tip generated from one of these technologies to require support by further corroboration before being acted upon. Finally, this Note will argue that there should be a civil remedy available, namely under the product liability framework, against these technology developers, so as to deter discriminatory models and offer victims targeted by racial bias the opportunity to address their grievances.

Section II will begin looking at the foundations of implicit bias and how it has infiltrated machine learning technologies such that once it has been inputted into the algorithms, it is nearly impossible to extract, and thus perpetuates racist thinking. Section III will explore two possible solutions to this issue: first, this Note will argue that the government should be held accountable for the employment of these algorithms. Given the nature of machine learning and the constant consumption of information that continually adjusts the algorithm, machine learning technologies should be held to the standard courts use for anonymous tips when police are mobilized and should by default be seen as unreliable unless supported by corroboration.[20] Furthermore, to better ensure transparency in what data is being used to train and guide these algorithms, this Note will argue for data protection legislation similar to specific provisions regarding information and access to personal data passed within the European Union's recent data protection legislation in order to give transparency to individuals whose

16. *See* Lindsey Patterson, *How the Evolution of Big Data Is Influencing Law Enforcement*, TECHNOLOGY.ORG (July 28, 2017), https://www.technology.org/2017/07/28/how-the-evolution-of-big-data-is-influencing-law-enforcement/; Andrew Ferguson, *Is "Big Data" Racist? Why Policing by Data Isn't Necessarily Objective*, ARS TECHNICA (Dec. 29, 2017, 7:23 AM), https://arstechnica.com/tech-policy/2017/12/is-big-data-racist-why-policing-by-data-isnt-necessarily-objective/ [https://perma.cc/XW2A-ZARD].

17. *See* Rich, *supra* note 14, at 13.

18. *See* Barrett, *supra* note 15, at 341-42.

19. *See* Terry v. Ohio, 392 U.S. 1 (1968).

20. *See* Florida v. J.L., 629 U.S. 266 (2000).

personal data is being used by third party software companies in these algorithms. Second, this Note will argue that software developers should be held accountable if their technologies are found to be based on discriminatory and racially biased data or models. This accountability should be imposed through a products liability scheme that focuses on strict liability, as opposed to negligence, in order to impose legal obligations on these software developers and compel them to take affirmative, preventative action when creating these algorithms.

Ultimately, the growing reliance on machine learning technologies by law enforcement agencies requires greater knowledge and review of how these technologies function and better assurances to check if they are being employed in a manner that is neutral and accurate, both mechanically and legally. While the issue of #BBQBecky and others who wrongfully mobilize the police continues to be a problem, technologies that use similarly biased thinking and formulations often go unquestioned or unchallenged, and thus require heavier scrutiny as we enter a more data-driven society. Implicit bias, and the racist behavior it leads to, should be curbed, not further reinforced by technological advancements, in order to prevent unnecessary and racially motivated interactions with the police that generate violence against black Americans.

II. THE WRONGFUL MOBILIZATION OF THE POLICE: HOW IMPLICIT BIAS IN HUMANS AND TECHNOLOGIES CAN INFLUENCE POLICING

Subsection A will first look at implicit bias and how it infiltrates daily interactions between civilians and between civilians and the police. Then, Subsection A will examine issues of "profiling by proxy" as demonstrated by #BBQBecky and others who wrongfully mobilize the police.[21] Subsection B will then discuss the new forms of technology based on Big Data and machine learning that law enforcement is increasingly relying upon for crime detection and prevention, and the similar permeation of the same kind of implicit bias in the data and models used to create those technologies.

Despite inherently involving the bias that leads to the outrage with #BBQBecky and other bigoted tipsters, the results of these technologies go unquestioned without any legal pushback or standard, therefore making their effects potentially even more dangerous in terms of racial discrimination in law enforcement.

21. *See* Lisa Thurau & Bob Stewart, *Avoiding 'Profiling by Proxy*,*'* VERA INSTITUTE OF JUSTICE: THINK JUSTICE BLOG (Mar. 13, 2015), https://www.vera.org/blog/police-perspectives/avoiding-profiling-by-proxy.

A. Implicit Bias in Human and Police Interactions

Racial disparities within the criminal justice system are well known—black and Latino people are disproportionately stopped, prosecuted, and incarcerated as compared to white people who commit the same crimes, despite black and Latino populations making up a smaller percentage of the population.[22] Despite the fact that racial bias in the criminal justice system is both pervasive and well-studied, the racism that permeates interactions between minorities and law enforcement is not necessarily obvious or even cognizable by the person or group perpetrating it. Implicit bias is the internalization of stereotypes and perspectives concerning other races or people that can often unintentionally lead to discriminatory behavior.[23] Even in spite of "avowed or endorsed beliefs or principles," a person can unconsciously "activate" a network of negative stereotypes when confronted with pictures, symbolic representations, or members of a stereotyped group, which in turn can lead to discriminatory behavior.[24] More specifically, studies have shown that when exposed to African-Americans or their perceived "culture," such as seeing a member of that group or listening to a certain type of music or language often attributed to that group, participants have displayed "negative emotional arousal" and "evidence of self-regulatory or executive control activity" in response.[25]

Implicit bias is remarkably prevalent in police interactions with the public. Different from overt racism, which is the conscious activation of harmful stereotypes that manifest in outwardly racist behavior, implicit bias is much more difficult to detect and therefore harder to correct.[26] For example, overt racist police behavior would be a police officer deciding "I'm stopping all black people," while implicit bias would be a police officer deciding "I'm stopping all dangerous people," which in effect would be the stopping of only black people due to the officer's unconscious conflation of black with dangerous.[27] Implicit bias in the police is particularly perilous when police officers tend to use more force against black Americans because of latent stereotypical thinking that a black person needs more force to be subdued as

---

22. *See* Radley Balko, *There's Overwhelming Evidence that the Criminal-Justice System Is Racist. Here's the Proof*, WASH. POST (Sept. 18, 2018), https://www.washingtonpost.com/news/opinions/wp/2018/09/18/theres-overwhelming-evidence-that-the-criminal-justice-system-is-racist-heres-the-proof/?noredirect=on&utm_term=.bb3ceddb9a16#section9.

23. *See* Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 CALIF. L. REV. 945, 951 (2006).

24. *Id.*; *See* Robert J. Smith & Justin D. Levinson, *The Impact of Implicit Racial Bias on the Exercise of Prosecutorial Discretion*, 35 SEATTLE U. L. REV. 795, 798-801 (2012).

25. *Id.*

26. Katherine Lee Goyette, *Implicit Bias & Police Encounters*, 87 J. KAN. B. ASS'N 9, 19 (2018); Megan Quattlebaum, *Let's Get Real: Behavioral Realism, Implicit Bias, and the Reasonable Police Officer*, 14 STAN. J. C.R. & C.L. 1, 7 (2018) ("[R]acial profiling will be defined as 'the use of race or ethnicity, or proxies thereof, by law enforcers as the basis of judgments of criminal suspicion,' except with trustworthy information, relevant to the locality and timeframe, that links a person of a particular race or ethnicity to an identified criminal incident or scheme.").

27. *Id.*

compared to their white counterpart.[28] Accordingly, implicit bias has led to black Americans being one-third more likely to be stopped by the police, three times more likely to be searched by the police, and three times more likely to have been the subject of force as compared to their white counterparts.[29] Implicit bias has also led to a phenomenon of "stereotype threat," where someone concerned about being perceived as part of a negative stereotype subconsciously acts in accordance with that negative association, further affirming and perpetuating negative stereotypes in the mind of a police officer and unintentionally escalating already dangerous situations.[30] For example, a black individual may become more self-regulatory in their actions when interacting with an officer and may subsequently exhibit behavior that a police officer would view as "deceptive" or that may affect the individual's ability to resist pressure in interrogative situations.[31]

Not only does implicit bias guide police interactions, from both the perspectives of the officer and the suspected individual, implicit bias is also part of the mobilization of the police. "Profiling by Proxy" is a phenomenon in which individuals alert the police to false claims of misconduct by people or groups of people against whom these callers are biased or dislike.[32] Some of the more notable cases of profiling by proxy involved direct racial profiling such as those of "Permit Patty," where a women called the police on 8-year-old for not having a permit to sell water on a corner,[33] "Cornerstore Caroline," where a woman called the police to report being "sexually assaulted" by a child because his backpack brushed against her back while he walked behind her,[34] or the white women who called 911 on a black Yale graduate student taking a nap in her dormitory's common room.[35] However, incidents like

28. Dakshana Bascaramurty, *Implicit Bias Linked to Lethal Police Force, Research Suggests*, THE GLOBE AND MAIL (July 2017).

29. Tom James, *Can Cops Unlearn Their Unconscious Biases?*, THE ATLANTIC (Dec. 23, 2017), https://www.theatlantic.com/politics/archive/2017/12/implicit-bias-training-salt-lake/548996/.

30. Cynthia J. Najdowski et al., *Stereotype Threat and Racial Differences in Citizens' Experiences of Police Encounters*, 39 LAW & HUM. BEHAV. 463, 464 (2015).

31. *Id.*

32. Thurau & Stewart, *supra* note 21.

33. Kalhan Rosenblatt, *White Woman Dubbed "Permit Patty' for Calling Police on Black Girl Denies It was Racial*, NBC NEWS (June 25, 2018, 9:30 AM), https://www.nbcnews.com/news/us-news/white-woman-dubbed-permit-patty-calling-police-black-girl-denies-n886226.

34. Ryan Grenoble, *White Woman Apologizes for Falsely Reporting That a Black Boy Groped Her*, HUFFINGTON POST (Oct. 17, 2018, 5:56 PM), https://www.huffingtonpost.com/entry/cornerstone-caroline-black-boy-false-grope_us_5bc785d5e4b055bc947d04ac.

35. Alan Pyke, *A Black Yale Grad Student Took a Nap in her Dorm's Common Room, and a White Woman Called the Cops*, THINK PROGRESS (May 9, 2018, 3:54 PM), https://thinkprogress.org/white-woman-calls-cops-on-black-yale-grad-student-for-crime-of-napping-in-a-common-room-10826f736ce3/.

"BBQ Becky,"[36] and the Starbucks employees in Philadelphia who asked two black men to leave for sitting in the store without purchasing anything,[37] display how implicit bias—or, in these cases, internalized racist and stereotypical views of black people that inspired unwarranted feelings of fear and suspicion—can trigger unnecessary and potentially even more discriminatory or harmful police interactions.[38] Given how dire the current situation is between officers and minorities in the United States, addressing implicit bias at the outset of police interactions—specifically how they are getting information that leads to racially targeting individuals—is crucial in order to begin correcting overall bias in policing.

B. Big Data, Machine Learning and the Police

Implicit and explicit biases, specifically concerning an individual's race, are embedded in all aspects of police interactions—from what mobilizes the police to who is arrested. Increasingly, law enforcement agencies have been looking to technological tools in order to aid in crime detection and prevention, with the hope that relying on technology, as opposed to human judgement and bias, can lead to more efficient, and more accurate, results.[39] The rise of Big Data[40] has led to novel methods of discovering latent information within this mass accumulation of data in order to better inform and guide how businesses, service providers, and the government can function more effectively without constant human supervision or, in some cases, human input.[41] One such method is data mining, which is the computerized application of statistical information to these large aggregations of data in order to find relationships or patterns, or to identify people who meet a certain

36. Christina Zhao, *'BBQ Becky,' White Woman Who Called Cops on Black BBQ, 911 Audio Released: 'I'm Really Scared! Come Quick!'*, NEWSWEEK (Sept. 4, 2018, 5:42 AM), https://www.newsweek.com/bbq-becky-white-woman-who-called-cops-black-bbq-911-audio-released-im-really-1103057.

37. Scott Neuman, *Men Arrested in Philadelphia Starbucks Reach Settlements*, NPR (May 3, 2018, 1:06 AM), https://www.npr.org/sections/thetwo-way/2018/05/03/607973546/men-arrested-in-philadelphia-starbucks-reach-settlements.

38. Robert J. Smith, *Reducing Racially Disparate Policing Outcomes: Is Implicit Bias Training the Answer?*, 37 U. HAW. L. REV. 295, 298 (2015) ("Biases could shape whether an officer decides to stop an individual for questioning in the first place, elects to interrogate briefly or at length, decides to frisk the individual, and concludes the encounter with an arrest versus a warning.").

39. Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, NATIONAL INSTITUTE OF JUSTICE: NIJ JOURNAL (Jan. 2019), https://www.ncjrs.gov/pdffiles1/nij/252038.pdf.

40. Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. 41, 42 (2013) ("Big data analytics depend on small data inputs, including information about people, places, and things collected by sensors, cell phones, click patterns, and the like. These small data inputs are aggregated to produce large datasets which analytic techniques mine for insight.").

41. Savan Patel, *Chapter 0: What is Machine Learning?*, MEDIUM, MACHINE LEARNING 101 (Apr. 29, 2017), https://medium.com/machine-learning-101/chapter-0-what-is-machine-learning-ad136361c618.

profile.[42] These discovered relationships, patterns, or profiles are then collected into "models," which create automatic processes in order to classify and organize a particular interest in a practice called "machine learning."[43] Machine learning, in other words, is artificial intelligence that uses relationships, patterns, or profiles found within historical data sets and applies that information in new and unpredictable data sets without much or any human supervision.[44] For example, law firms have begun using machine learning software for document review in the discovery phase of litigation to evaluate large numbers of documents, flag those that are relevant, and send those that are "questionable" to the attorney, all without needing a paralegal or other human oversight.[45] Remarkably, these algorithms continue to learn based on analyzing new data sets and thus "improve their performance on a task with experience."[46] Therefore, those "questionable" documents sent to the attorney who then determines whether the document is relevant or not will be absorbed by the algorithm to better understand what "relevant" means, or could mean, eventually leading to a lower number of "questionable" documents and even less need for attorney input.

Machine learning technology is beginning to transform law enforcement through "predictive policing," which offers information based on criminological theories applied to police records, camera footage, and other information already in use or available to the police to use for both crime detection and crime prevention.[47] For example, officers in Santa Cruz, California are using an algorithm that gives beat cops "crime forecasts" for that particular day in a particular area, so that those officers can then include that area in their patrol and help suppress or uncover any potential crime.[48] An example of this crime forecast could be something like "there is a 10.36% likelihood of a car theft in a particular downtown garage on a particular day. The times when those car thefts are most likely to occur are also listed." "CrimeScan" is another such piece of predictive policing software that offers geographical location information based on past police data in order to preempt high violence crimes.[49] With the assumption that "violent crime is

---

42. Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 3 (2005).

43. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677-78 (2016).

44. Laura A. Odell et al., *A State Cyber Hub Operations Framework*, INSTITUTE FOR DEFENSE ANALYSES (June 2016), https://apps.dtic.mil/dtic/tr/fulltext/u2/1013836.pdf.

45. Bernard Marr, *How AI and Machine Learning are Transforming Law Firms and the Legal Sector*, FORBES (May 23, 2018, 12:29 AM), https://www.forbes.com/sites/bernardmarr/2018/05/23/how-ai-and-machine-learning-are-transforming-law-firms-and-the-legal-sector/#7fea06e932c3.

46. Rich, *supra* note 14, at 10.

47. Barrett, *supra* note 16, at 334-35.

48. Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 268 (2012).

49. Randy Rieland, *Artificial Intelligence is Now Used to Predict Crime. But Is It Biased?*, SMITHSONIAN MAGAZINE (Mar. 5, 2018), https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/.

like a communicable disease," CrimeScan takes in police records ranging from prior high violence crimes, past 911 calls involving gun possession or shots fired, and temporal information regarding high violence crimes in order to build a type of map where high violence is likely to occur, but stops before attempting to predict who might commit these crimes.[50]

Predictive policing, however, has in fact gone beyond just offering geographical or temporal predictions of when crime could occur and now has begun offering the likelihood that an individual is in the progress of committing a crime.[51] "Automated Suspicious Algorithms" (ASAs) determine the likelihood that an individual is engaging in criminal activity and generate probabilistic guesses about an individual's level of suspicion.[52] Based on the historical data already available to the police—for example, description of a suspect and facts of an earlier arrest for cocaine possession—and based on continual learning through ongoing experiences in executing the algorithm—for example, whether individuals tagged by the ASA for similar crimes were arrested or not—a computer can identify patterns that typically signal when an individual is engaging in hand-to-hand cocaine sales.[53] The computer then alerts the police when this level of suspicion reaches a programmed level of confidence, such as a numerical predictive percentage, which can lead to officers being dispatched to the individual that is allegedly dealing cocaine.[54] The computer, therefore, is determining an individual's level of suspicion, as opposed to a bigoted tipster that inheres latent motivations biased against a certain class of people. This kind of suspicion software is already in use in several police departments. In Chicago, the "Strategic Subject List" (SSL) is one working example of an ASA currently in use whose algorithm generates risk scores and identifies individuals who are at the highest risk of danger, either as the victim or the perpetrator of a crime.[55] Factors to determine this score include the individual's prior arrests, including for violent offenses and narcotics, and the number of times an individual was the victim of a shooting or aggravated battery or assault.[56] However, because the workings of the algorithm have not been disclosed, it is unclear how heavily each factor weighs in how the score is actually generated.[57] Individuals who have a score of 250 or above are then tagged by

---

50. *Id.*; Adam Mann, *How Science Is Helping Stop Crime Before It Occurs*, NBC NEWS (Oct. 6, 2017), https://www.nbcnews.com/mach/science/how-science-helping-stop-crime-it-occurs-ncna805176.

51. Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 876 (2016).

52. *Id.*

53. Rich, *supra* note 14, at 10.

54. *Id.* (". . . there is a 62 percent chance the highlighted individual is currently engaged in hand-to-hand cocaine transactions.").

55. Jeff Asher & Rob Arthur, *Inside the Algorithm that Tries to Predict Gun Violence in Chicago*, N.Y. TIMES (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html.

56. *Id.*

57. Brianna Posadas, *How Strategic is Chicago's "Strategic Subjects List"? Upturn Investigates.*, MEDIUM (June 22, 2017), https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c.

the list and put "on [the Chicago Police Department's] radar," although it is not clear how the police actually use this information.[58] Ironically, when the *New York Times* conducted a study based on the information the Chicago Police Department released to the public, they discovered that violence in Chicago is not necessarily concentrated among those with the highest SSL risk scores and that despite the use of the SSL for years, Chicago is still contributing to a large share of increasing urban murders country-wide.[59] The algorithm has, therefore, had minimal, if any, positive effect on crime prevention and reduction.

In theory, the use of a machine to determine an individual's level of suspicion should offer a more neutral, informed, and reliable outcome than a human who is prone to implicit biases and has the potential for bad motivations. However, despite the fact that these algorithms are based on numerical data from past police records and studies and the lack of human supervision in the machine's perpetual learning, these algorithms are just as likely to inhere implicit biases as their human counterparts but, concerningly, without the scrutiny or legal mechanisms to counter these biases.[60] Machine learning AI is typically viewed as a "black box:" although it can learn and "make predictions and decisions as humans do," it does so "without being able to communicate its reasons for doing so" and in methods that humans may not be able to comprehend.[61] In addition to this general lack of knowledge about what actually motivates an algorithm's decision making, implicit bias can easily permeate machine learning processes (and be further perpetuated by machine learning), specifically when it comes to assessing an individual's level of suspicion.[62]

More specifically, data mining technologies, despite their self-learning capabilities, still involve considerable human input when building these algorithms.[63] Data mining involves two types of processes: interpretable processes, which use a limited number of variables in discovering relationships, patterns, or profiles, and thus require human scrutiny; and non-interpretable processes, which involve so many variables (up to thousands) that the way the result came about is nearly impossible to determine.[64] Furthermore, the human analyst "predefine[s] the parameters of the search" that the machine conducts when discovering relationships, patterns, or profiles, meaning that the way the algorithm fundamentally functions is at the analyst's discretion.[65] In either process, therefore, human determination is intrinsically involved in the creation of these models and therefore any human

58. *Id.*
59. Asher & Arthur, *supra* note 55.
60. *See* Barocas, *supra* note 43, at 680-81, 684, 686; Barrett, *supra* note 13, at 339-41.
61. Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 890, 893 (2018).
62. Barocas, *supra* note 43, at 680-81.
63. Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PENN ST. L. REV. 285, 293 (2011).
64. *Id.*
65. *Id.* at 292-93.

bias can also still seep into results of the algorithms, although the extent of their involvement is unknown.

Moreover, even without the active input of human discretion, the results of the machines are dependent on the quality of data used in how these machines are developed.[66] More specifically, the "models," or the collection set of discovered relationships, are learned based on "training data," the data that is used to teach the machine how to behave.[67] The data that is used to train the model is critical in how the machine interacts with data. More specifically, if the training data is biased, then the machine will be biased and perpetuate that bias. Biased data can happen if the data that is used was decided by or involved prejudice, and as such the machine would just be reproducing the same prejudice in their suspicion predictions.[68] For example, if the data used to train the model is based on old police cases for gang-related violence in Los Angeles, the model would then adopt and perpetuate the same kind of discriminatory bias against black and Latino people used by the LAPD that led to excessive incarceration of those populations.[69] Additionally, some of the data actually used in these kinds of predictive policing software "rely on commercial data brokers and data gleaned from social media" which can lead to "acontextual and inaccurate results," as inappropriate motivations, such as profit, or the implicit biases of those brokers and social media accounts are uncertain.[70]

Bias can also infiltrate ASAs if the data used allows the machine to make discriminatory inferences, also known as "collection bias."[71] If the data is based on a particular sample of the population, like if the model is based solely on data regarding cocaine sales from a predominantly black neighborhood, this will lead to an overrepresentation of black people in this data and so the machine would infer a connection between black people and cocaine sales, leading to higher suspicion rates for black people just because they are black.[72] The population sample used in the training data therefore should in theory be representative of the entire population; however, given that these are only samples, this is unlikely.[73]

Ultimately, the implicit bias that has driven racially disparate policing, in terms of both bigoted tipsters and actual police conduct, is just being recycled into these algorithms as the data being used to "teach" these

66. Barocas, *supra* note 43, at 687; Barrett, *supra* note 16, at 340.
67. Barocas, *supra* note 43, at 680-81.
68. *Id.*
69. Donna Murch, *Crack in Los Angeles: Crisis, Militarization, and Black Response to the Late Twentieth-Century War on Drugs*, J. AM. HIST. 162, 164 (2015) ("Punitive campaigns against drugs and gangs in Los Angeles rationalized a new martial infrastructure . . . [A]s in counter-insurgency strategy, the geographic application of force meant that the particular populations were at high risk not only because of their age and race but also because of their location. Indeed, by 1992 city sheriffs listed nearly half of the African American men under age twenty-five in Los Angeles County as gang members.")
70. Barrett, *supra* note 16, at 339.
71. Barocas, *supra* note 43, at 684.
72. *See id.* at 680-81.
73. *Id.* at 686.

algorithms is not reflective of actual crime information.[74] The failure of this technology used by the police to provide accurate results—as well as entirely rid itself of human bias—is not just an indictment of shoddy artificial intelligence but also has serious consequences in terms of an already problematic record of police abuse in the United States.[75] Media and U.S. Department of Justice reports from Baltimore, Cleveland, Ferguson, Chicago, Los Angeles, New Orleans, Albuquerque, and Portland have revealed that police departments in those cities had used excessive force and abuse, even going so far as to suggest that some police officers treated people, specifically minorities, "as animals or subhuman[s]."[76] Despite these serious deficiencies, state police departments and federal law enforcement agencies continue to move forward, as more trials and demonstrations of this technology continue to be put into effect.[77]

Moreover, the uncertainty surrounding the significance of the impact of implicit bias is further exacerbated given the lack of transparency about these algorithms from the developers.[78] Northpointe, a for profit company that created the most-used algorithm for risk assessment recidivism scores has not disclosed any specific calculations that go into the algorithms.[79] Pro Publica, however, used their methodology and found different results in the scores, as well as significant racial disparities.[80] For example, the Florida Supreme Court is deciding a case in which defendant Willie Lynch was arrested for selling approximately fifty dollars' worth of crack cocaine based solely on low quality photos that were run across an algorithmic facial recognition system.[81] "Face Analysis Comparison Examination System" (FACES), the facial recognition system implicated in this case, awarded Lynch "one star"—with the stars correlating to the likelihood of a match—but the analyst who testified to the results admitted that she was neither aware of the maximum number of stars possible nor how the algorithm actually worked, and the other

74. Rieland, *supra* note 49.

75. German Lopez, *Cities Across the Country Have Been Riddled with Accusations of Police Abuse*, VOX (Nov. 14, 2018, 4:12 PM), https://www.vox.com/identities/2016/8/13/17938200/police-shootings-abuse-brutality-justice-department.

76. *Id.*

77. Rigano, *supra* note 39.

78. Julia Angwin et al., *Machine Bias*, PRO PUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/B6T7-7GQJ]

79. *Id.*

80. *Id.*

81. Somil Trivedi & Nathan Freed Wessler, *Florida is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech*, AMERICAN CIVIL LIBERTIES UNION (Mar. 12, 2019, 5:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people?fbclid=IwAR37ossykYzI5zgUc1BWyKX-cG-xDLhb1LuGndyyVIyxmL6DJLZEWWxrv64 [https://perma.cc/RYC4-MVQ4].

photos FACES had tagged as possible matches were not disclosed.[82] The lack of knowledge involved in how FACES's system operates, plus the influence it had in Lynch's conviction, namely that the government's case was wholly based on the officer's testimony that they recognized Lynch as the man selling the crack cocaine, demonstrates the need for more scrutiny in how these technologies are used and how they are built.[83]

III. LEGAL MECHANISMS THAT CAN PROTECT AGAINST IMPLICIT BIAS IN POLICE-USED MACHINE LEARNING TECHNOLOGIES

In Section III, this Note will look at two possible approaches to confronting implicit bias in ASAs and other machine learning technologies used by law enforcement. Subsection A will propose that the police should treat ASA results as anonymous tips, which must be deemed sufficiently reliable or be further corroborated in order to be used to lawfully justify a police stop under the reasonable articulable suspicion standard. Furthermore, the algorithms themselves should be held to certain international data protection standards, specifically Articles 13 through 15 of the European Union's data protection legislation, in order to ensure adequate transparency and algorithm accountability such that, at the very least, these software companies are named and shamed. Subsection B will offer that, because ASAs are technically products that are purchased by police departments, software developers should be held accountable for any defects, namely disproportionate levels of racial disparities, under tort product liability standards.

A. Holding the Government Accountable: Fourth Amendment Checks on Implicit Bias

Unlike bigoted tipsters, like #BBQBecky and #PermitPatty, who face social pushback and are expected to face the appropriate level of scrutiny under the Fourth Amendment in order to be considered reliable, ASAs and other machine learning algorithms used by the police encounter similar issues of implicit bias but do not receive much pushback, either legally or socially. Therefore, ASAs and other machine learning technologies used by the police should, at the very least, be held to the same standard as calls from BBQ Beckys—anonymous tips that require the evaluation of the tip's reliability or some other corroborating information.

Jurisprudence for stops based on the Fourth Amendment requires that police officers must have a reasonable, articulable suspicion (RAS) that the individual is involved in an imminent or pending criminal activity or that the individual has just committed a felony in order to lawfully stop them without

82. *Id.*; Aaron Mak, *Facing Facts*, SLATE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/XCJ4-6V7W].

83. Trivedi & Wessler, *supra* note 81; Mak, *supra* note 82.

their consent.[84] While the Supreme Court has yet to specifically define what RAS means, the standard required to briefly detain a person in order to question or resolve the officer's suspicion is lower than what is required to establish probable cause.[85] In terms of implicit bias, the Court has deemed any pretextual motivation, including racial animus, irrelevant under the Fourth Amendment as long as the officer is able to provide either probable cause or RAS.[86] Even under the Fourteenth Amendment's Equal Protection Clause, plaintiffs must provide evidence that the officer intentionally discriminated, as it is "not sufficient to show disproportionate impact."[87] An officer's intentions, therefore, are largely immaterial when doing a stop under RAS.

When police work on tips from 911 callers, such as #BBQBecky or #PermitPatty, they similarly have to ensure that these tips are sufficiently reliable in order to establish either probable cause or RAS.[88] In evaluating the reliability of tips, courts evaluate the quantity and quality of the information along with the degree of reliability of the tip.[89] More specifically, the Supreme Court found in *Illinois v. Gates* that courts should evaluate the "veracity, reliability and basis of knowledge" of the tipster under a totality of the circumstances analysis, specifically determining whether the tipster is reliable and how the tipster came upon the information.[90] Under a totality of the circumstances analysis, should one element of this reliability determination be considered weak—i.e. the basis of knowledge is based on hearsay and not personal knowledge—the required level of suspicion is not automatically defeated as long as the veracity of the tipster is established.[91] In establishing the veracity of the tipster, the "absence of an apparent motive to falsify an independent police corroboration of the details provided by the informant" can be considered sufficient.[92]

Tips from anonymous tipsters, as opposed to known tipsters, therefore, generally lack an "indicia of reliability" at the outset to justify a stop under *Terry v. Ohio*, but can become sufficient if the police have other compelling

---

84. *See generally* Terry v. Ohio, 392 U.S. 1 (1968).

85. *Id.* at 27 (finding that there must be something more than an "inchoate and unparticularized suspicion or 'hunch'" and "some minimal level of objective justification.")

86. Whren v. United States, 517 U.S. 806, 814 (1996) (holding that pretextual motivations are irrelevant to a Fourth Amendment search or seizure as long as it meets probable cause standards); Ashcroft v. Al-Kidd, 563 U.S. 731, 740 (2011) (citing Saucier v. Katz, 533 U.S. 194, 201-02, (2001)) (holding that pretextual motivations are irrelevant for lower suspicion stops as long as RAS is met).

87. Wayne C. Beyer, *Police Misconduct: Claims and Defenses under the Fourteenth Amendment Due Process and Equal Protection Clauses*, 30 URBAN LAWYER 65, 113-14 (1998).

88. Alabama v. White, 496 U.S. 325, 330 (1990).

89. *Id.* (noting that the same totality of the circumstances test applied in *Illinois v. Gates* to determine probable cause should be used for establishing RAS, albeit it at a lower standard than probable cause).

90. Illinois v. Gates, 462 U.S. 213, 230 (1983) (holding that the "rigid" two-prong test under *Aguilar* and *Spinelli* in assessing the reliability of tips is no longer the law); United States v. Angulo-Lopez, 791 F.2d 1394, 1396 (9th Cir. 1986).

91. *Angulo-Lopez*, 791 F.2d at 1396.

92. *Id.* at 1397.

corroborative information and can find no underlying motivation.[93] In addition, anonymous tips only offering "innocent" details, such as the particulars about the individual's clothing or appearance, are only helpful in identifying the individual, but do not speak to either the tipster's "knowledge of concealed criminal activity," or to whether there is an illegality that can give rise to RAS.[94] Tipsters like #BBQBecky and #PermitPatty, therefore, are only so helpful in identification of individuals since they only describe the suspicious person as opposed to any legitimate unlawful activity and, as such, may reveal their implicit bias and improper, racially based motivation for calling the police. Thus, in order to establish RAS and lawfully stop the individuals in question, the police must have some other corroborating information about an imminent or impending illegality.

Similarly, ASAs are used primarily to identify individuals who meet certain factors of "suspicion" and should not be considered reliable unless there is some other corroborating information.[95] Therefore, each time an ASA alerts the police once an individual reaches the pre-set level of confidence, the police officer should assess the "veracity, reliability, and basis of knowledge" of the ASA itself.[96] The reliability of the information provided by the ASA, however, involves just as much, if not more, implicit bias than #BBQBecky and #PermitPatty and thus its reliability should be considered weak by default. Furthermore, the ASAs are created by third party, for-profit companies that use unverified employees who may have implicit or explicit biases—financial motivations, a lack of concern for ensuring accuracy, or even simply having different hiring standards than officers—that are then learned by the machine they've created.[97]

As a result, an ASA's reliability is fundamentally in question and can often lead to inaccurate, discriminatory results that could amount to a Fourth Amendment violation. Even so, remedies for violations of the Fourth Amendment are limited—an individual who is charged with a crime is entitled to invoke the "exclusionary rule" in order to suppress any illegally obtained evidence.[98] However, several exceptions to the rule, such as the Independent Source Doctrine,[99] Good Faith (or "*Leon*") Doctrine,[100] and the

93. Terry v. Ohio, 392 U.S. 1 (1968); Adams v. Williams, 407 U.S. 143, 147 (1972) (holding that a tip can carry sufficient "indicia of reliability" to establish RAS but not sufficient to establish probable cause like when information comes from a known informant).

94. Florida v. J.L., 629 U.S. 266, 271-72 (2000).

95. *Adams*, *supra* note 84, at 147.

96. *Illinois v. Gates*, 462 U.S. at 230.

97. Angwin, *supra* note 78.

98. *See, e.g.*, Weeks v. United States, 232 U.S. 383, 397-98 (1914) (holding exclusionary rule applies in federal cases); Mapp v. Ohio, 367 U.S. 643, 655-57 (1961) (extending the "exclusionary rule" to states, implying constitutional underpinnings to the rule).

99. *See, e.g.*, Segura v. United States, 468 U.S. 796, 805 (1984); Murray v. United States, 487 U.S. 533, 537 (1988).

100. *See, e.g.*, United States v. Leon, 468 U.S. 897, 923-24 (1984); Davis v. United States, 564 U.S. 229, 246-47 (2011) (holding that officers' illegal conduct had to be deliberate, reckless, or grossly negligent).

Herring doctrine,[101] make the exclusionary rule nearly ineffective. In addition, those who are not defendants in a criminal action and cases where illegally seized evidence is being introduced are forced to seek alternate remedies that are similarly unsatisfactory.[102] Civil suits under 42 U.S.C. § 1983 and *Bivens* actions both require funding that may exclude indigent defendants and are also bound by officers' qualified immunity, which protects discretionary actions by officers as long as "conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[103] Even the Supreme Court has conceded that "exclusion presents the only effective remedy to deter wrongful police conduct," suggesting that some forms of police misconduct within the ambit of the Fourth Amendment cannot be remedied.[104]

Despite the limitations on rectifying Fourth Amendment violations, police officers should still be vigilant in the face of growing reliance on technology. More specifically, officers should be wary of ASAs and their built in biases, as they would be with a #BBQBecky or #PermitPatty and their more blatant racial prejudices, taking care to scrutinize any results produced by ASAs before automatically dispatching an officer. Corroborative information should be acquired before the police interact with a targeted individual in order to ensure that actual illegal conduct is in question and that the individual has not been targeted for racist reasons.

1. Holding the Government Accountable: Data Protection Legislation

Another way of ensuring that ASAs are reliable tools that avert, rather than perpetuate, implicit bias would be to ensure that the data used within these algorithms and used in training models adheres to certain protections. More specifically, there should be certain safeguards and limits on using personal data, such as factors associated with identification (including addresses and physical features like those used on driver's licenses), when used by third party businesses and by the government. Advocacy organizations like the Electronic Privacy Information Center (EPIC) have been a part of litigation against the government and technology companies like Facebook seeking to obtain records of the type of data being used and how it's being used, and to ensure checks on algorithmic transparency are put

101. Herring v. United States, 555 U.S. 135, 144 (2009) (holding that application of the exclusionary rule should be determined on a case by case basis in order to promote deterrence sufficient to be "worth the price paid by the justice system" and as such should not be automatically applied).

102. *See generally*, Brent E. Newton, *The Supreme Court's Fourth Amendment Scorecard*, 13 STAN. J. C.R. & C.L. 1, 13-14 (2017).

103. Wilkerson v. Goodwin, 774 F.3d 845, 851 (5th Cir. 2014).

104. *See* Elkins v. United States, 364 U.S. 206, 220 (1916).

in place.[105] EPIC has also proposed legislation through its Public Voice coalition titled the "Universal Guidelines for Artificial Intelligence," which would impose obligations on businesses to have a final determination made by a human when using algorithms, and obligations on institutions using artificial intelligence generally to ensure that there is no unfair bias or impermissible discriminatory decision making taking place.[106]

Furthermore, in 2016, the European Union passed the General Data Protection Regulation (GDPR), which, in Chapter 3, gave data subjects—any EU citizen whose personal data is being used—the right to ask what of their personal information is being used and how it is being used.[107] Article 35 of the GDPR also requires a company or organization to employ a "data protection officer" whenever personal data, such as ethnicity, religious beliefs, or genetic data, is used in order to ensure that the company or organization using this data is using it in compliance with GDPR standards.[108] Finally, Article 79 sets a penalty for non-compliance, which can rise up to 4% of a company's global annual revenue based on the violation.[109] Although this Note does not suggest adopting all of the GDPR, the move towards regulation ensuring algorithmic transparency, specifically in allowing citizens to at least inquire about their data, should motivate US legislators. This may already be in motion, as California recently passed their own data privacy law.[110]

The United States on both federal and state levels should take California's example and push further, passing legislation that specifically investigates the algorithms employed in the criminal justice system with the goal of uncovering the breadth and severity of implicit bias within these algorithms and its discriminatory effects in the real world. The United States should impose policies similar to the data access protection provisions within the GDPR specifically allowing data subjects, or in this case those stopped by police officers for seemingly no legitimately lawful reason, access to inspect what personal information is being used by the software developers generating ASAs and how their algorithms then use that data.[111] For the US

---

105. Brief for EPIC as Amici Curiae Supporting Appellee, *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2018) (No. 18-15982) (noting that Facebook's collection of biometric data, namely the facial recognition feature used for photos, is a prohibition of the Illinois Biometric Information Privacy Act which asserts "certain obligations on private entities that collect or possess biometric identifiers."); Brief for EPIC as Amici Curiae Supporting Appellee, *United States v. Miller*, [No. 16-47-DLB-CJS, 2017 WL 2705963 (E.D. KY. 2017) (No. 18-5578) (arguing that the search of Miller's emails, which were only searched upon Google becoming aware that there were flagged images of apparent child pornography being sent through the emails, was an invasion of privacy and a violation of the Fourth Amendment).

106. *Universal Guidelines for Artificial Intelligence*, THE PUBLIC VOICE (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.

107. *See generally* 2016 O.J. (L 119) 39-47.

108. *Id.* at 53; Juliana De Groot, *What is the General Data Protection Regulation? Understanding and Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Jan. 3, 2019).

109. De Groot, *supra* note 108.

110. Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

111. General Data Protection Regulation, 2016 O.J. (L 119) 1-88.

government to even acknowledge that these algorithms may be inherently biased, especially when used to detect suspicion levels or identify certain types of people, may be helpful in combatting these algorithms' discriminatory outputs. Moreover, tasking the government with monitoring and regulating how these algorithms operate (specifically in regards to the misuse of personal data that leads to discriminatory results) makes the government responsible for the prevention of automated implicit bias.

B. Holding Developers Accountable: Product Liability

Ultimately, ASAs and other machine learning technologies used by the police are products sold to them by specialized technology and software development companies.[112] Third-party companies that create ASAs and other machine learning technologies employed by the police should be held accountable by implementing a financial penalty in cases of wrongful use of data, such as biased data collection or use of biased historical records, creating a better incentive to be more vigilant in ensuring that algorithms are not incorporating biases in their initial stages and perpetuating inaccurate racial disparities, or at least in attempting to correct these biases within the models. Therefore, one way of ensuring accountability and decreasing the risk of incidents of implicit bias in action would be to hold the developers legally accountable for recklessly or intentionally created ASAs and the like that effectuate disproportionately discriminatory results. An immediate issue with this solution, however, is the lack of consensus on whether artificial intelligence generally should be regarded as a product or as a service, which affects the theory of tort liability under which AI should be evaluated.

1. AI as a Product: Strict Liability

Contemplating artificial intelligence as a product in tort litigation could prompt strict liability if the product, or computer-based technology, is found to be defective.[113] Strict liability notably does not consider fault, but rather is based purely on causation. Therefore, any safeguards taken by the maker or developer in order to prevent the defect would be irrelevant.[114]

Strict liability is found if a plaintiff can prove that the product was "defective and unreasonably dangerous, that the defect existed when it left the

112. Karen Hao, *Police Across the US are Training Crime-Predicting AIs on Falsified Data*, MIT TECH. REV. (Feb. 13, 2019), https://www.technologyreview.com/s/612957/predictive-policing-algorithms-ai-crime-dirty-data/ (mentioning Palantir and PredPol, third party companies developing predictive policing software).

113. Ryan Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, 86 GEO. WASH. L. REV. 1, 15 (2018).

114. Rylands v. Fletcher, L.R. 3 H.L. 300 (1868) (holding that the owner who brought a reservoir onto his land that was considered "abnormally dangerous" is *prima facie* answerable to any damage arising from it); Greenman v. Yuba Power Products, 377 P.2d 897 (Cal. 1963) (en banc) (holding that manufacturers of defective products are strictly liable).

hands of [the] defendant and the defect caused the harm."[115] A defect, as defined by the Restatement (Second) of Torts, requires a showing that the product was unexpectedly dangerous to the ordinary customer, also known as the "consumer expectation test."[116] In *Camacho v. Honda Motor Co., Ltd.*, the Supreme Court of Colorado evaluated whether the product is unreasonably dangerous under a totality of the circumstances test to determine whether the product should be held to a strict liability standard.[117] Factors for a court to evaluate under this test include: the utility of the product to user and public; the safety of the product (which would inquire into the likelihood that the product will cause injury or probable seriousness of harm); the availability of a substitute product meeting the same need and that is not as unsafe; the user's ability to avoid harm with due care, and other factors.[118] Under the Restatement (Third) of Torts, a strong case for applying strict liability for an abnormally dangerous activity is essentially based on whether there was knowledge of significant risk and whether that risk was still disregarded.[119] The factors to evaluate under this theory include whether: "(1) the activity creates a foreseeable risk of physical harm; (2) the risk is a 'highly significant' risk; (3) the risk remains 'even when reasonable care is exercised by all actors;' and (4) 'the activity is a matter of not common usage.'"[120]

Applying strict liability to ASAs that result in disproportionately racist identifications would be a direct way to combat implicit bias in these algorithms. ASAs and other machine learning technologies that are used to identify individuals inherently carry significant risk and thus require constant vigilance from the outset, instead of requiring some error to be seen as dangerous.[121] If a developer is aware that they are strictly liable for any defect in their algorithm's execution, perhaps ASA developers would be more incentivized to have more oversight and controls in place that ensure implicit bias is detected and corrected before it gets integrated into models and gets lost.[122] However, traditional tort product litigation under strict liability is most accessible to users of a product who suffer personal, physical injury, as opposed to a bystander or third party suffering non-physical harms such as

115. Alvin S. Weinstein et al., *Product Liability: An Interaction of Law and Technology*, 12 DUQ. L. REV. 425, 428-29 (1974); DAVID G. OWEN, PRODUCTS LIABILITY LAW 1 (3d ed. 2014); RESTATEMENT (SECOND) OF TORTS § 402A (1965).

116. Roger Traynor, *The Ways and Meanings of Defective Products and Strict Liability*, 32 TENN. L. REV. 363, 366 (1965); RESTATEMENT (SECOND) OF TORTS § 402A (1965).

117. Camacho v. Honda Motor Co., Ltd., 741 P.2d 1240, 1244 (Colo. 1987).

118. *Id.* at 1247.

119. Elizabeth Fuzaylova, *War Torts, Autonomous Weapon Systems, and Liability: Why a Limited Strict Liability Regime Should be Implemented*, 40 CARDOZO L. REV. 1327, 1360 (2019).

120. *Id.*; RESTATEMENT (THIRD) OF TORTS § 20 (AM. LAW. INST. & UNIF. LAW COMM'N 2010).

121. *See generally* Rich, *supra* note 51.

122. Abbott, *supra* note 113, at 22 ("[S]trict liability creates a stronger incentive for manufacturers to make safer products, and manufacturers may be better positioned than consumers to insure against loss.")

economic or emotional pain.[123] The "harms" that result from racially prejudiced algorithms do not necessarily result in physical harms although the effect—unlawful police stops—is still damaging. Furthermore, the "harms" of the defective product are not inflicted on the user, the police officer, but on third parties who are identified by the defective product and stopped by the police. Therefore, meeting even the basic requirements of strict liability, particularly that the defect caused this harm, may be difficult under traditional tort liability theory.[124]

However, should courts move in a direction that recognizes non-physical harms brought on by reliance on machine learning, ASAs and other machine learning technologies used by the police that adopt and employ implicit bias may meet the necessary factors for determining a defect. First, the utility of machine learning in law enforcement is fairly high—all computer-based technologies that involve automation, such as an ASA, should in theory be safer in executing a design than a human since it eliminates the risk of human error.[125] Former General Motors ("GM") vice chairman, Bob Lutz, was quoted predicting that GM's first autonomous car will have a significantly lower accident rate than cars driven by humans.[126] Specifically, within the law enforcement context, the fairly low ratio of officers to citizens, as well as the enormous prison population, suggests that additional, reliable assistance, such as suspicion detecting cameras and facial recognition, would be beneficial.[127] Despite the considerable potential of these kinds of machine learning technologies, the risk of harm inherent in their use, specifically in regards to implicit bias, outweighs the possible benefits of ASAs and thus strengthens the argument that ASAs that incorporate racial bias are defective. More specifically, the safety of an ASA is questionable, as there is clearly a high likelihood of error in terms of racial bias that can lead to unlawful stops or other more intensive police interactions.[128] Although the concern with unquestioned reliance on ASAs is that an unlawful police stop could lead to violence and even death, this would still require courts to broaden their view of "harm" to include non-physical injuries to ensure that all instances of police misconduct initiated by ASAs are punishable, not just those that lead to violence. Second, the availability of

123. Cathy Bellehumeur, *Recovery for Economic Loss Under a Products Liability Theory: From the Beginning Through the Current Trend*, 70 MARQ. L. REV. 320, 321-22 (1987) ("Most courts do not allow tort recovery for purely economic loss in the absence of any personal injury or property damage. However, the method for categorizing a claim is so varied that a claim not recoverable in tort because it constitutes an economic loss in Idaho may be recoverable in tort in Illinois where it is classified as a claim for property damage.").

124. *See* Alvin S. Weinstein et al., *supra* note 102, at 428-29.

125. Abbott, *supra* note 113, at 18-19.

126. *Id.*

127. *Police Employee Data*, Federal Bureau of Investigation: Criminal Justice Information Services Division (2011), https://ucr.fbi.gov/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/policeemployees_main_final.pdf (in 2011, there were 3.4 full-time law enforcement officers for every 1,000 inhabitants).

128. *See* Renata M. O'Donnell*, Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, 94 N.Y.U. L. REV. 544, 553 (2019).

a substitute product without implicit bias may not currently be possible as the algorithms typically rely on police records, which inherently involve bias.[129] However, police officers are beginning to undergo implicit bias trainings to defeat this bias and so could technically be considered an appropriate substitute to an ASA.[130] Finally, even with due care, an officer may not be able to avoid the harms, or rather the perpetuation of harms, that come with relying solely on suspicion algorithms since the implicit bias may be so embedded that it could be difficult to detect where the bias came from and how it influenced the algorithm's results.[131]

Despite courts thus far failing to apply strict liability to AI on technical grounds,[132] the inherent danger of AI used in the context of police identifications should be sufficient to allow courts to view AI software as unreasonably dangerous even though the harm may not necessarily be obvious or physical. Strict liability was born out of a need to find liability when product failures became increasingly difficult to prove under traditional theories of negligence[133] and as such should be the starting standard for how courts evaluate machine learning technology. On a policy level, imposing strict liability would not only on its face imply that there is significant risk in using this technology—which would in application force police officers to use ASAs only with caution—but would also force developers to reduce the risk from the beginning in order to avoid being held liable. Furthermore, companies, as opposed to users, are much better equipped to find and correct defects in products, as seen with companies, such as Volvo and Google, recognizing their ability to correct and prevent harm, announcing that they will accept full responsibility if their self-driving products cause a collision despite no legal compulsion to do so.[134] Courts should therefore create a similar legal obligation on all software developers selling AI products, especially those who provide AI to government agencies, in order to ensure that these algorithms are being generated in good faith and to acknowledge their particular predisposition to biased input. Applying strict liability would also ensure that those who were unlawfully stopped by the police or were the victim of other constitutional violations have the opportunity for redress and thus the traditional strict liability paradigm should expand to include non-physical, third party harms.

---

129. Barocas, *supra* note 43, at 680-81, 684; *see also* William Isaac & Andi Dixon, *Why Big Data Analysis of Police Activity is Inherently Biased*, PBS (May 10, 2017), https://www.pbs.org/newshour/nation/column-big-data-analysis-police-activity-inherently-biased.

130. James, *supra* note 29.

131. Barocas, *supra* note 43, at 673-74.

132. Chatlos Systems Inc. v. National Cash Register Corp., 479 F. Supp. 738, 740-41 n. 1 (D.N.J. 1979), *rev'd on other grounds*, 635 F.2d 1081 (3d Cir. 1980), *aff'd after remand*, 670 F.2d 1304 (3d Cir. 1981) (holding that strict liability could not be applied to a service).

133. David C. Vladeck, *Machines without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 132 (2014).

134. Ben Taylor, *Who's liable for decisions AI and robotics make?*, BETANEWS (Mar. 21, 2017), https://betanews.com/2017/03/21/artificial-intelligence-robotics-liability/.

Ultimately, the use of the algorithms is more often than not going to result in racially disparate and discriminatory results,[135] so despite difficulties in applying strict liability under its traditional tort framework, on a larger policy level, developers should be held liable for the harms they can cause or for failure to properly identify and attempt to correct the implicit bias.

2. AI as a Service: Negligence

Under the Uniform Commercial Code (UCC), software that is specifically designed for a customer, as opposed to mass-produced and for the public, should be considered a service as opposed to a product.[136] As a service, harms caused by AI could then be evaluated under a traditional negligence standard.[137] The plaintiff would have to prove that the defendant, in this case the software developer, had a duty of care, that they breached that duty by failing to conform to a reasonable standard of behavior, and that that breach caused the injury to the plaintiff—essentially determining who is at fault.[138] Duty would, in theory, not be at issue here since there is privity between the software developer and the police officer. Further, many jurisdictions allow for foreseeable bystanders to recover, so, here, individuals targeted by ASAs could recover as well.[139] However, courts have refused to establish professional standards for technology developers as there is no licensing requirement, and as such "computer malpractice" has found limited acceptance in today's jurisprudence.[140] Furthermore, under a negligence paradigm, there is a broader range of harms that could be litigated, including a "knowledge base [that] is incomplete or inadequate; incorrect or inadequate warnings and documentation; [or] . . . the user . . . supplying faulty input or selecting the incorrect program for the task."[141] However, the burden of proof to demonstrate a breach of that nature rests on the plaintiff, a task which is already difficult for software developers given the intricacies of machine learning technology, and likely even more difficult for the injured individual

135. Barocas, *supra* note 43, at 673-74.

136. Rottner v. AVG Technologies USA, Inc., 934 F. Supp. 2d 222, 230 (D. Mass. 2013); Motorola Mobility, Inc. v. Myriad France SAS, 850 F. Supp. 2d 878 (N.D. Ill. 2012) (holding that computer code is considered a service and liability for defective software should be evaluated under a breach of warranty under the UCC as opposed to product liability).

137. J.K.C. Kingston, *Artificial Intelligence and Legal Liability*, *in Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV* 269-279 (Max Bramer & Miltos Petridis eds., 2016).

138. *Id.*

139. MacPherson v. Buick Motor Co., 217 N.Y. 382, 390 (1916) (holding that privity of contract is no longer necessary to establish duty of care in negligence actions and thus, if it is reasonably foreseeable that a product is dangerous, duty of care goes beyond buyer and seller).

140. Marguerite E. Gerstner, *Liability Issues with Artificial Intelligence Software*, 33 SANTA CLARA L. REV. 239, 258-59 (1993).

141. *Id.* at 248.

who has no access to how the algorithm is developed and what information is being used.[142]

Given how complex and impenetrable the neural networks that drive ASAs and other machine learning technologies are, determining fault is nearly impossible to discern within the AI context.[143] Even prior to analyzing the breach inquiry of a negligence claim, the plaintiff would have to demonstrate that the reasonable standard of behavior of a computer is safer than a human and thus the implicit bias that leads to racialized results would be a failure to conform.[144] Furthermore, as is the case with strict liability, causation is hard to prove since ASAs only suggest certain actions, requiring another agent (the officer) to take the action that causes the harm of unlawful police interactions.[145] However, given that there have been cases where officers have solely relied on these algorithmic results to make their arrests suggests that these algorithms are directly causing potentially unlawful arrests or at least lending themselves to potential Fourth Amendment violations.[146]

At the very least, software developers can be compelled to satisfy a duty to warn about the risk that results of ASAs will contain inherent racial bias, so officers can be aware of this risk when relying on the ASA. However, a warning may not be sufficient to offset any police action based on the results of the ASA. Although negligence is what is traditionally used with services it does not do enough to compel software developers to be vigilant and active in identifying sources of bias in generating algorithms. Furthermore, given that these technologies continue to learn and make decisions without human input, and given that companies are already taking full responsibility for their technologies not functioning,[147] courts adopting a strict liability approach would offer a more straightforward, effective means of assigning liability to software developers. Ultimately, placing liability on the developer who has control over the creation of these algorithms sheds light on how implicit bias can permeate automated technologies and help prepare for a future where these machines operate without any human input at all.

IV. CONCLUSION

Implicit bias is a significant issue in the criminal justice system that requires constant vigilance and checks in order to be effectively combatted. The rise of ASAs and other machine learning technologies used by law enforcement should prevent implicit bias rather than perpetuate it, and so both officers and the software development companies that profit off these algorithms should be held liable for being complicit in the perpetuation of

142. Bathaee, *supra* note 62, at 892-93 (noting the near impossibility of discerning how a machine learning algorithm functions given its advanced learning abilities that even humans may not be able to comprehend).

143. Curtis E.A. Karnow, *Liability for Distributed Artificial Intelligences*, 11 BERKELEY TECH. L.J. 147, 192 (1996).

144. Abbott, *supra* note 125, at 22.

145. *Id.* at 22-26.

146. *See* Trivedi & Wessler, *supra* note 81.

147. Taylor, *supra* note 134.

implicit bias in new technology. It should be standard practice for police departments to treat the results from ASAs as anonymous tips in order to meet the requisite RAS to remain compliant with Fourth Amendment protections against search and seizure. Corroborative information ensuring that the ASA identified an illegality as opposed to a suspicious person based on race is necessary to combat the implicit biases that are entangled within these algorithms similar, to how BBQ Beckys are treated. In addition, software developers need to be transparent about the type of information going into these algorithms and therefore should be compelled to disclose to individuals how and what data is being used under a similar access scheme to the GDPR's Chapter 3.[148] Finally, software developers should be held legally responsible for their software through tort strict liability in order to incentivize developers, the only people who have the opportunity and skill to eliminate these biases, to keep vigilant for implicit biases as well as allow targeted individuals the opportunity to recover from the harms they suffer from being unlawfully targeted by the police. Furthermore, while this Note does not address the privacy issues of using this kind of personal data by third parties, as well as the lack of individualized suspicion involved in the employment of ASAs under a Fourth Amendment analysis, these issues add to the need for machine learning to have more transparency and accountability in their models and results.

As algorithms become increasingly universal but with no additional requirements for adequate transparency or accountability, the racial bias of #BBQBecky that has proven to be pervasive in and perpetuated by machine learning algorithms used by the police continues to become more cemented in the criminal justice system and in society. More jurisdictions should mirror California in being attentive to these technologies, but more specifically in how they are relied on by law enforcement, in order to promote equity in our criminal justice system and to help prevent further violence perpetrated by the police against black Americans.

148. *See generally* 2016 O.J. (L 119) 39-47.

Public Safety, Preemption, and the Dormant Commerce Clause: A Narrow Solution for States Concerned with the 2018 Restoring Internet Freedom Order's Preemption Clause

John Bick*

TABLE OF CONTENTS

* J.D., May 2020, The George Washington Univeristy Law School; B.S.W., Social Work, August 2017, Belmont University. Thank you to Professor Ethan Lucarelli for your guidance and feedback throughout the writing process. I would also like to thank the Federal Communications Law Journal staff for their hard work in bringing this note to publication.

I. INTRODUCTION

As wildfires burned in California during July of 2018, fire department personnel in Santa Clara noticed that their Internet service was much slower than usual.[1] In the ensuing conversations with Verizon sales associates, Verizon confirmed that it was throttling the fire department's unlimited data access during this critical time of need.[2] Despite the obvious threat to public safety, the Verizon sales team subjected the fire department to days of negotiation.[3] Indeed, Verizon was able to extract money before finally agreeing to cease throttling the data.[4] The fire department was not watching Netflix or cat videos during this crisis; they were using the data to coordinate life and property saving operations with multiple first responders across the affected area.[5] Consistent and responsive Internet access was critical to track the location of resources across agencies and locations, as well as to communicate with the public.[6] Instead, the fire department spent days distracted by the Internet service provider's (ISP) pecuniary machinations and the citizens of California ultimately paid the price.[7] This episode is emblematic. It highlights the critical position of ISPs in our national and local public safety apparatus, and clearly shows that these companies are not above exploiting this position for monetary gain even when life is quite literally on the line.[8]

While Verizon publicly apologized for this unfortunate lapse in moral judgment and promised not to do such things in the future, the damage was already done, and many questions remain.[9] Specifically, in light of the FCC's 2018 *Restoring Internet Freedom Order* (*2018 Order*) and its stated policy of "light-touch" regulation, along with its broad claim of preemption, it is not clear what actions, short of litigation, states can take to ensure that their critical public health and safety infrastructure is not hampered by unreliable Internet service.[10] Further, while the episode above dealt specifically with data caps on the fire department acting as an end user, the problem could

---

1. Petition for Review of an Order of the Federal Communications Commission, Declaration of Fire Chief Anthony Bowden at ¶ 9, Mozilla Corp., et al. v. FCC, 18-1051(L) (D.C. Cir. 2018) [hereinafter Fire Chief Anthony Bowden].
2. *Id.* at Ex. A.
3. *Id.*
4. *Id.*
5. *See id.*
6. Fire Chief Anthony Bowden, *supra* note 1, at ¶¶ 4-5.
7. *See id.* at ¶ 9-10.
8. Petition for Review of an Order of the Federal Communications Commission at 23, Mozilla Corp., et al. v. FCC, 18-1051(L) (D.C. Cir. 2018) [hereinafter *Petition*].
9. Hamza Shaban, *Verizon Says It Shouldn't Have Throttled California Fire Fighters during Wildfire Emergency*, WASH. POST (Aug. 22, 2018) https://www.washingtonpost.com/technology/2018/08/22/verizon-says-it-shouldnt-have-throttled-california-firefighters-during-wildfire-emergency/ [https://perma.cc/7XLJ-38EQ] (last visited Nov. 17, 2018).
10. Restoring Internet Freedom Order, *Declaratory Ruling and Order*, FCC 17-166, at para. 1 & para. 195 (2018) [hereinafter *2018 Order*].

become more acute when critical health and safety content is given a lower priority than Facebook's data because the state agency, public hospital, or municipal utility lacks the funds to pay for prioritization.[11] Again, the FCC essentially claims congressional authority, direct or indirect, to preempt the field, but this should not necessarily prevent states from regulating ISPs in a narrowly tailored way to ensure the safety and health of their citizens.[12] In short, what is the scope of the preemption as it exists today (after the *2018 Order*), and what steps can states take to ensure they are able to reliably provide critical services that rely on the Internet backbone?

As the above example indicates, ISPs play a key and unavoidable role in keeping citizens safe.[13] Unfortunately, if left unregulated by both state and federal governments, ISPs are incentivized to put corporate interests ahead of social interests and safety.[14] The FCC's *2018 Order* does not adequately take these safety interests into account.[15] In fact, the *2018 Order* does not explicitly mention public health and safety considerations at all, despite prior judicial determinations that the FCC is mandated to explicitly take public health and safety into account when issuing substantive rules.[16] Instead, the *2018 Order* almost exclusively focuses on consumer protection issues, and subsequent state net neutrality laws have focused on consumer protection as well.[17] However, this focus misses the point. The largest issue with the *2018 Order* is not that consumers will have less access to entertaining or otherwise stimulating content. Rather, it is that the *Order's* proactive preemption claim undermines states' abilities to ensure the reliability and quality of Internet service provided to the states' critical public health and safety infrastructure, and thus puts lives and health at risk.[18]

It is quite possible the FCC's policy of deregulation will lead to a more robust Internet ecosystem in the long run,[19] but in the short term ISPs' blocking, throttling, and prioritization of content will lead to avoidable public harm as first responders, public health and safety authorities, hospitals, and utilities have their incoming and outgoing data throttled or deprioritized.[20] Furthermore, unlike consumer harm, where monetary damages as contemplated by the *2018 Order* may adequately compensate victimized

11. *See* Petition, *supra* note 8, at 23-27.
12. *See 2018 Order*, *supra* note 10, at para. 195.
13. *Id.* at para. 195-98.
14. *See generally* Fire Chief Anthony Bowden, *supra* note 1.
15. *See* Petition, *supra* note 8, at 2.
16. Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006) (explaining the FCC is required by its enabling statutes to consider public safety when regulating industries (such as ISPs) that it has repeatedly deemed important to public safety); *See also* Mozilla Corp., et al. v. FCC 18-1051(L) (D.C. Cir. 2018) (where the FCC conceded at oral argument that it did not explicitly consider public safety in the *2018 Order*).
17. *See generally 2018 Order*; California SB-822; New York Bill A08882.
18. *See* Petition, *supra* note 8, at 23-24.
19. Simone A. Friedlander, *Net Neutrality and the FCC's 2015 Open Internet Order*, 31 BERKELEY TECH. L.J. 905, 909 (2016).
20. *See* Petition, *supra* note 8, at 23-27.

consumers, there is no post hoc compensation that truly compensates for the loss of life or a family's home.[21]

This Note argues that state officials can mitigate this risk to public safety without frustrating the goals of the FCC's *2018 Order* by enacting laws that prohibit the blocking, throttling, or deprioritization of specific entities the state deems critical for public safety. State regulations of the nature just described would likely be able to survive preemption claims stemming from the *2018 Order* because of the proposal's limited scope, the proposed law's critical importance to state safety, and the fact that the *2018 Order* fails to adequately deal with public health and safety.[22]

This Note begins by examining the main substantive changes the FCC's *2018 Order* made to the regulatory framework governing ISPs with a focus on the FCC's claim to preempt contrary state regulation in the area. It concludes that, while the FCC may have authority, pursuant to the *2018 Order*, to preempt state consumer protection laws seeking to re-implement anti-blocking, throttling, and paid prioritization regulations on a broad scale, the *2018 Order* does not expressly preempt narrowly tailored state regulations designed to protect critical state Internet communications infrastructure necessary to ensure public health and safety. It also concludes that carefully crafted state laws will be able to survive any conflict preemption or Dormant Commerce Clause claims.

Section II.A discusses the major changes in the *2018 Order* and ultimately finds that the FCC reduced its ability to regulate ISPs and to preempt state laws in the field when it reclassified ISPs under Title I of the Telecommunications Act.[23] Sections II.A.1-3 explain the legal theories the FCC used to justify its preemption claim. Sections II.B.1-3 explain the current state of congressional and agency preemption case law, with an analysis of agency preemption in the FCC context. Taken together, these sections explain the distinction between congressional and agency preemption and clarify the different legal standards that apply. Section II.C explains the current state of Dormant Commerce Clause case law and discusses how and when to use the competing tests. Section II.D identifies state public health and safety entities covered by the proposed law and explains why state regulation is necessary to protect them. Section III is an analysis of the proposed state law in light of the FCC's preemption claim. It discusses how the changes in the *2018 Order* gave the states more room, in specific circumstances, to regulate ISPs despite the FCC's preemption claim, and concludes that the proposed state law is likely to survive any legal challenges.

---

21. Mozilla Corp., et al. v. FCC 18-1051(L) (D.C. Cir. 2018) (oral argument Feb. 1, 2019).

22. *See* Petition, *supra* note 8, at 4 (quoting Metropolitan Life, Ins. Co. v. Massachusetts, 471 U.S. 724, 756 (1985) ("[States] have traditionally had great latitude under their police powers to legislate as to the protection of lives, limbs, [and] health . . . of their residents.")).

23. Verizon v. FCC, 740 F.3d 623, 650 (D.C Cir. 2014); *see* Petition, *supra* note 8, at 47.

II. BACKGROUND

A. The 2018 Restoring Internet Freedom Order and the Authority to Preempt

The *2018 Order* aims to promote corporate investment in the Internet's physical infrastructure by significantly reducing regulations on Internet service providers.[24] Specifically, it repeals the (1) no blocking, (2) no throttling, and (3) no paid prioritization regulations put in place by the *2015 Open Internet Order*.[25] The rationale is that allowing service providers to monetize more aspects of their service will incentivize more robust investment in the Internet's underlying infrastructure; thus leading to wider coverage, faster speeds, and more consistent Internet connectivity nationwide.[26]

The *2018 Order* also reclassifies ISPs as information services, rather than telecommunication services.[27] The legal significance of this reclassification is that ISPs are now regulated under Title I, rather than Title II, of the 1996 Telecommunications Act; the FCC has much less regulatory authority under Title I of the Act than Title II.[28] This was made clear in *Verizon v. FCC*, where the D.C. Circuit held that the FCC could not impose anti-blocking, throttling, and paid prioritization regulations on entities subject to Title I regulation.[29]

The *2018 Order* goes further than repealing the no blocking, no throttling, and no paid prioritization regulations. The *2018 Order* also attempts to preempt states from enacting legislation that would be inconsistent with *the Order's* regulatory goals.[30] Obviously, a federal agency cannot just preempt state law because it would like to. It needs the requisite legal authority, and the FCC's *2018 Order* relies on three distinct theories in an attempt to gain this authority: (1) the impossibility exception, (2) a policy statement inserted into the Telecommunications Act of 1996, and (3) forbearance.[31]

1. The Impossibility Exception

The "impossibility exception to state jurisdiction" is an agency-specific (as opposed to congressional) preemption theory, which has been accepted by the Supreme Court.[32] It can be thought of as a subset of agency preemption

24. *See 2018 Order*, *supra* note 10, at para. 1.
25. *See id.* at paras. 4, 17. Colloquially these regulations have been referred to as net neutrality, but technically they are regulatory mechanisms designed to implement net neutrality.
26. *See id.* at paras. 1, 5.
27. *Id.* paras. 26-29.
28. *See* Verizon v. FCC, 740 F.3d 623, 650 (D.C Cir. 2014).
29. *Id.*
30. *See 2018 Order*, *supra* note 10, at para. 195.
31. *See id.* at para. 198.
32. *Id.*

specific to the FCC. Under this theory, FCC preemption is valid if "(1) it is impossible or impracticable to regulate the intrastate aspects of a service without affecting interstate communication; (2) the Commission determines that such regulation would interfere with federal regulatory objectives,"[33] [and] "(3) the state regulation in question would negate the FCC's exercise of its lawful authority."[34]

The "impossibility exception" closely resembles conflict preemption, which can occur "when a state action stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[35] The difference here is that the agency itself, rather than Congress or a court, has proactively determined that a state law would frustrate its attempts to implement the policy it has determined best fulfills its congressional mandate.[36] The agency in effect substitutes its own express preemption for the direct congressional intent that is usually necessary.[37] There is an ongoing debate, scholarly and judicial, about how much deference agencies should be given when they purport to explicitly preempt state laws absent explicit statutory authority.[38]

2. The Telecommunications Act of 1996: Policy Statement

The second legal justification the FCC gives for valid preemption is a policy statement in the Telecommunications Act of 1996.[39] The relevant section of the statute provides that it is "the policy of the United States to preserve the vibrant and free market that presently exists for the Internet and other interactive computer services including any other information service, unfettered by Federal or State regulation."[40] The *2018 Order* combines this policy statement with Section 3(51) of the 1996 Act, which provides a definition of telecommunication services, to assert that all federal and state

33. *Id.* at para. 198 (citing Vonage Order, 19 FCC Rcd at 22413-15, 22418-24, paras. 17-19, 23-32; Minn. PUC, 483 F.3d at 578-81).

34. Petition, *supra* note 8, at 45 (citing Public Serv. Comm'n of Maryland v. FCC, 909 F.2d 1510, 1515 (D.C. Cir. 1990).

35. *See* Shane Levesque, *Preemption and the Public Health: How Wyeth v. Levine Stands to Change the Ways in which we Implement Health Policy*, 3 ST. LOUIS U. J. HEALTH L. & POL'Y 307, 320 (2010) (quoting Pacific Gas & Electric v. Energ. Res. Comm., 461 U.S. 190, 204 (1983)).

36. *See* Karen A. Jordan, *Agency Preemption and the Shimer Analysis: Unmasking Strategic Characterization by Agencies and Giving Effect to the Presumption Against Preemption*, 2008 WIS. L. REV. 69, 91 (2008).

37. *See id.*

38. Nina Mendelson, *A Presumption Against Preemption*, 102 NW. U. L. REV. 695, 698-99 (2008).

39. *2018 Order*, *supra* note 10, at para. 203.

40. 47 U.S.C. § 230 (b)(2), (f)(2).

common carriage-type regulation[41] of information services is congressionally prohibited.[42] The FCC claims that through this policy statement and statutory definition, Congress itself meant to prevent and thus preempt states from regulating information services in specific yet somehow unnamed ways.[43] With this claim, the FCC is relying on implied congressional authority. The FCC does not seem to be arguing that the entire field is occupied, as the FCC concedes that the states can still regulate in the field as long as the regulations are not inconsistent with the 2018 Order.[44]

3. Forbearance

The third legal justification given for preemption is not especially relevant to this Note's proposed law. The FCC claims that they have forborne the implementation of common carriage regulation under Title II, and therefore the states cannot implement the specific regulations the FCC has affirmatively declined to impose.[45] However, the FCC has not actually forborne these regulations.[46] Instead, it redefined ISP so that providers would be regulated under Title I of the Act.[47] Under Title I of the Act, the FCC has no statutory authority to impose common carriage regulations.[48] It is not clear how one can affirmatively forebear from using a power one does not possess.[49]

B. The Current Preemption Landscape

Determining whether Congress intended to preempt state law in an area is not always straightforward.[50] It has become even murkier as the scope of federal agencies grows and our society becomes more economically and technologically integrated.[51] This section examines the current state of traditional congressional preemption, as well as claims of agency preemption, absent a direct congressional intent to preempt. This section also examines the Dormant Commerce Clause, as it can become important to the vitality of the proposed state law in certain circumstances.

---

41. Typical common-carriage regulations include a duty to, "furnish . . . communication service upon reasonable request, engage in no unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilitities, or services, and charge just and reasonable rates." Verizon v. FCC, 740 F.3d 623, 630 (D.C Cir. 2014) (quoting 47 U.S.C. §§ 201(a)-(b) and 202(a)) (internal citations omitted).

42. *2018 Order*, *supra* note 10, at para. 203.

43. *Id.*

44. *Id.* at para. 196.

45. *Id.* at para. 204; *See also Verizon*, 740 F.3d at 650 (D.C Cir. 2014) (equating no blocking, no throttling, and no paid prioritization regulations to common carrier regulations).

46. *See* Petition, *supra* note 8, at 46.

47. *2018 Order*, *supra* note 10, at para. 20.

48. *Verizon*, 740 F.3d 623, 650 (D.C Cir. 2014).

49. *See* Petition, *supra* note 8, at 47.

50. Levesque, *supra* note 35, at 315-16.

51. *See generally id.* at 322-26.

1. Traditional Forms of Congressional Preemption

The Supremacy Clause in Article VI of the Constitution states, "[t]he Constitution and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the Supreme Law of the Land."[52] One of the primary goals of the Clause is straightforward—to ensure that constitutional laws important for national uniformity are not thwarted by inconsistent state laws or regulations.[53] The clause prevents states from protecting or promoting local interests, whether they be economic or social in nature, at the expense of national interests.[54] Another goal is to ensure that important national policies are not thwarted by a patchwork of different state laws.[55] Preemption stems directly from this Clause and can be either explicit or implicit.[56]

As the role of federal agencies grew in the twentieth century, courts also recognized a type of preemption stemming from the authority of federal agencies, under the well-established theory that federal regulations carry the same legal weight as congressionally passed statutes.[57] The ability of agencies to proactively preempt state law through regulation has further complicated preemption analysis, as it is not always clear what form of preemption is being asserted, and thus what kind of legal analysis is necessary to examine preemption claims.[58] This phenomenon is apparent in the *2018 Order*, where the FCC asserts both its own authority to preempt state laws in the given circumstances, as well as direct congressional authority.[59]

This section will examine (1) explicit preemption; (2) the two forms of implicit preemption; and (3) agency preemption, with a focus on the *2018 Order*.

Explicit preemption is exactly what it sounds like—Congress writes into a statute that all state legislation in the area is now superseded by the federal law at issue.[60] This means that supplemental, complimentary, or even identical state laws relating to a particular issue are no longer operative because Congress has decided that the consistency and advantages of having one standard federal law in the area furthers important national policy goals.[61] The key here is that Congress is acting pursuant to a constitutionally enumerated power and explicitly stated their preemptive intent in the statute.[62]

---

52. U.S. CONST. art. VI, cl. 2.
53. *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 412 (Wolters Kluwer 5th ed. 2015).
54. *Id.* at 414.
55. *See id.* at 414-15.
56. *Id.* at 414.
57. Fidelity Fed. Savings & Loan Ass'n v. de la Cuesta, 458 U.S. 141, 153 (1982).
58. Jordan, *supra* note 36, at 88.
59. *2018 Order*, *supra* note 10, at paras. 198, 203.
60. CHEMERINSKY, *supra* note 53, at 416.
61. *See id.* at 416. *But see id.* at 417 (explaining "even when an express preemption clause exists, it rarely provides guidance as to the scope of preemption.").
62. *Id.* at 412-13.

Implicit preemption is more abstract and is broken down into two categories: (1) field preemption[63] and (2) conflict preemption.[64] Field preemption is determined by performing a statutory analysis of the relevant federal law and determining if "the scheme of federal regulation is so pervasive as to make a reasonable inference that Congress left no room for the states to supplement it."[65] Conflict preemption also involves a detailed statutory analysis and occurs when it is impossible to conform with both the state and federal law at the same time, or when the state law stands in the way of accomplishing the "full purposes and objectives of Congress."[66] For this Note's purposes, it is important to understand that field preemption can also be implied from regulatory schemes drawn from the rules and regulations promulgated by federal agencies.[67] However, in these cases, as in all implied preemption cases, there is a "presumption against preemption of state police power regulations."[68] The Supreme Court is less likely to find field preemption in cases stemming solely from agency promulgated rules.[69]

Even if a statute expressly preempts all state legislative efforts, there is a question about the scope of the preemption.[70] The point is that in any preemption case, the courts must first determine if there is congressional intent to preempt state regulation in the area, and second, if that intent is clear, what the scope of that preemption is.[71] The analysis can be fact sensitive to the point of seeming purely subjective, but one guideline is that courts are less likely to find preemption in areas traditionally left to the police power of the states.[72] For example, in *Metropolitan Life v. Massachusetts*, the Supreme Court upheld a state law regulating insurance companies in the face of the Employment Retirement Income Security Act's (ERISA) notoriously broad preemption clause, noting that states typically have "great latitude" under their police powers to protect the health and safety of their citizens.[73] It is also important to note that implied preemption analyses, both field and conflict,

---

63. *Id.* at 422.
64. *Id.* at 431.
65. *Id.* at 427.
66. *Id.* at 435.
67. *Id.* at 429.
68. Bates v. Dow Agrosciences LLC, 544 U.S. 431, 449 (2005); Medtronic v. Lohr, 518 U.S. 470, 485 (1996).
69. CHEMERINSKY, *supra* note 53, at 429-30; Rice v. Santa Fe Elevator Co., 331 U.S. 218, 230 (1947).
70. *Compare* Shaw v. Delta Airlines, Inc., 463 U.S. 85 (1983) (holding that a state law that forbade insurance plans from discriminating against pregnant women was preempted by federal law because the law "related to" employee benefit plans) *with* N.Y. Conf. of Blue Cross Blue Shield Plans v. Travelers, 514 U.S. 645 (1995) (holding that a state law charging surcharges on commercial insurance plans was not preempted because the purpose of the act was to have national uniformity of employee benefit plans and the surcharge did not thwart this purpose); CHEMERINSKY, *supra* note 53, at 417.
71. CHEMERINSKY, *supra* note 53, at 421 (explaining express preemption clauses rarely define the scope of federal preemption at issue, and thus courts are left to determine their scope and effect).
72. *Id.* at 414.
73. *Metropolitan Life Ins., Co. v. Massachusetts*, 105 S. Ct. 2380, 2398 (1985); Petition, *supra* note 8, at 4.

do not occur in the abstract. They occur in the face of actual state laws that are being challenged in court.[74] This is distinct from both express and agency preemption which may occur proactively before a state law is actually enacted.[75]

2. Agency Preemption

Beyond the traditional categories of congressional preemption discussed above, the Court has also accepted a form of agency express preemption.[76] That is, when an agency passes a substantive rule, such as the *2018 Order*, courts may accept the agency's determination that any contrary state law will frustrate the federal regulatory scheme promulgated by the agency if that scheme itself is within the agencys' congressional mandate and properly promulgated.[77] The Court has accepted agency rules declaring its regulation preempts the field and agency claims that certain state laws would frustrate the regulatory goal, i.e. a type of proactive conflict preemption.[78]

The distinction between traditional congressional preemption and agency preemption is that in traditional preemption, Congress implicitly or explicitly decides that the relevant federal statute preempts state law, while with agency preemption, Congress did not directly make the preemption decision.[79] Instead, Congress gave the agency the authority to promulgate rules, and then the agency determined that the governing statute could only be put into effect if relevant state laws were preempted.[80]

The key legal significance between congressional preemption and agency preemption is the standard of review and tests courts use to review the respective preemption claims.[81] When courts find that the agency is claiming direct congressional authority to preempt, they engage in the types of analysis discussed in section II.B.1. However, when courts determine that the agency is claiming its own express intent to preempt based on its opinion that preemption is necessary to fulfill its congressional mandate, the court engages in something called Shimer analysis.[82]

Shimer analysis is used more rarely than the traditional analysis because courts generally only recognize express agency preemption when the

---

74. *Alascom, Inc. v. FCC*, 727 F.2d 1212, 1220 (D.C. Cir. 1984); Petition, *supra* note 8, at 4.

75. *See* Jordan, *supra* note 36, at 91-92 ("After notice and comment on the issue, and consideration of arguments on both sides, the FCC announced, we now find that there is a necessity to rationalize, interrelate, and bring into uniformity the myriad standards now being developed by numerous jurisdictions. We, therefore, are preempting the field of technical standards…") (quoting *In the Matter of Part 76*, 49 FCC 2d. at 480) (internal quotation marks removed)); *see also* CHEMERINSKY, *supra* note 53, at 416 (explaining that ERISA preempted futute state laws in the field).

76. *Id.* at 75.

77. City of New York v. FCC, 486 U.S. 51, 63-64 (1988).

78. Jordan, *supra* note 26, at 83.

79. *See id.* at 75.

80. *Id.*

81. *Id.* at 76.

82. *Id.* at 92-93.

agency openly acknowledges, in the relevant rule, that it is relying on its own preemption determination.[83] Agencies more often than not will attempt to veil their preemption behind a claim of direct congressional intent.[84] Usually, courts accept this characterization and proceed to engage in the traditional preemption analysis.[85] However, Shimer analysis is well represented in FCC preemption cases, and the Court in *City of New York v. FCC* explained that the analysis involves two steps: (1) identifying the scope of the agency's legal authority, and (2) determining whether the "decision to preempt represents a reasonable accommodation of conflicting policies committed to the agency's care by statute." [86] If both of these conditions are met the agency preemption will be upheld.

Preemption in the FCC context is made more complicated by the dual state and federal regulation envisioned by Congress in the two governing Acts—the Communications Act of 1934, as amended by The Telecommunications Act of 1996.[87] Neither act contemplates the dominant role the Internet has come to play in society today, and both acts force a distinction between inter and intrastate jurisdictions that does not lend itself well to modern communications technology.[88] That being said, over time it has become clear that if any aspect of the technology at issue has an interstate component the FCC regulation will supplant a contradictory state law.[89]

The Acts specifically regulate telecommunications and broadcast services by name.[90] In order to gain jurisdiction over new technologies that do not fit neatly under one of these categories, the FCC must either determine that the technology meets the statutory requirements to fall into one of the two categories, or it must rely on ancillary jurisdiction provided by Title I of the Act.[91] The *2018 Order* defines ISPs as information services, i.e. not telecommunications or broadcast services, and thus it is regulating pursuant to its Title I authority.[92]

The FCC's ancillary jurisdiction under Title I of the Telecommunications Act is a broad catch-all that allows the FCC to regulate technologies in ways not specifically contemplated in the Act when two conditions are met: (1) the communication technology uses interstate wire or radio facilities and (2) "the subject of the regulation [is] reasonably ancillary to performance of the [FCC's] various responsibilities."[93] When the FCC regulates under this ancillary authority, its powers to impose rules on regulated parties, and indeed to preempt state laws, are more limited than

83. *Id.* at 94.
84. *See id.* at 94.
85. *See id.* at 94-95.
86. *Id.* at 113.
87. *See* Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986).
88. HARVEY L. ZUCKERMAN, ET AL., MODERN COMMUNICATIONS LAW 757 (West Group 1999).
89. *Id.* at 759.
90. *See* Comcast Corp. v. FCC, 600 F.3d 642, 645 (D.C. Cir. 2010).
91. *See* ZUCKERMAN ET AL., *supra* note 88, at 757.
92. *2018 Order*, *supra* note 10, at para. 2.
93. Library Association v. FCC, 406 F.3d 689, 689 (D.C. Cir. 2005) (quoting United States v. Southwestern Cable Co., 392 U.S. 157, 167 (1968).

under one of the enumerated classifications.[94] Further, in *Louisiana Public Service Commission v. FCC*, the Court essentially limited preemption under this ancillary authority to instances where (1) the preemption is necessary to achieve a statutorily acceptable goal,[95] and (2) the inter and intra components cannot be separated.[96]

C. The Dormant Commerce Clause

The Dormant Commerce Clause stems from the Commerce Clause,[97] and it is much more controversial than preemption.[98] Its basic premise is that if the federal government has the power to regulate in a specific field, but has *not* chosen to exercise that power, then state laws can still be held invalid if they discriminate against out of state interests or "if they place an undue burden on interstate commerce."[99]

Depending on the state activity in question, courts apply different levels of review to determine if the state law or regulation violates the Dormant Commerce Clause.[100] If the state law is discriminatory against out of state interests, courts apply strict scrutiny and are much more likely to find a violation.[101] In non-discriminatory Dormant Commerce Clause challenges, courts compare the local interest involved with the burden on interstate commerce.[102]

The first step of Dormant Commerce Clause analysis is to determine if the relevant state law discriminates against out-of-state interests—either on its face or through its effects.[103]

This is a fact-specific inquiry, and two seemingly identical laws can lead to different results.[104] This can be seen by comparing *C & A Carbone, Inc. v. Town of Clarkstown* and *United Haulers Association. v. Oneida-Herkimer Solid Waste Management Authority*.[105] Both of the state laws in question required nonhazardous waste to be sent to specific disposal transfer stations, and both required the haulers to pay a fee.[106] Both laws applied equally to in-state and out-of-state parties.[107] The key difference was that in *C & A Carbone* the transfer station was privately owned, while in *United*

94. Verizon v. FCC, 740 F.3d 623, 632 (D.C. Cir. 2014).
95. Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 373-74 (1986).
96. *See id.* at 371, 374.
97. CHEMERINSKY, *supra* note 53, at 443-44.
98. *Id.* at 445, 447.
99. *Id.* at 443.
100. *See id.* at 455, 461.
101. *Id.* at 468.
102. *Id.* at 461.
103. Pharmaceutical Research and Mfrs. v. Thompson, 259 F. Supp. 2d 39, 43 (D.D.C. 2003).
104. *See generally* CHEMERINSKY, *supra* note 53, at 459.
105. C & A Carbone, Inc. v. Town of Clarkstown, N.Y., 114 S. Ct. 1677 (1994); United Haulers Assn. v. Oneida-Herkimer Solid Waste Mngt. Authority, 127 S. Ct. 1789 (2007).
106. CHEMERINSKY, *supra* note 53, at 458-59.
107. *Id.*

Haulers the transfer station was owned by the state.[108] The Court found this ownership distinction dispositive; it held that the law mandating deposit at the privately owned facility discriminated against out-of-state interest, but that the law mandating delivery to the state-owned facility did not.[109] The Court's point was that the law requiring delivery to a privately owned facility discriminated against out-of-state business interests.[110]

On the other hand, courts apply the *Pike* balancing test when the law at issue (1) only has an "incidental effect" on interstate commerce, (2) regulates in-state and out-of-state interests "even-handedly[,]" and (3) attempts to "effectuate a legitimate state interest."[111] If a court finds a legitimate public interest, it balances the importance of the public interest against the effect on interstate commerce.[112] Courts also consider if the public interest could be served by a less restrictive alternative.[113] The *Pike* test is much more permissive of state interests, and any proposed state law anticipating challenges under the Dormant Commerce Clause should be designed to ensure that courts will apply the *Pike* balancing test rather than strict scrutiny.

There are two defenses to otherwise violative state actions. First, if Congress sanctions the state activity, the court will not find a violation.[114] Second, if the state is acting as a market participant as opposed to a regulator, then the courts will also not find a violation.[115] For example, a state purchasing Internet service may claim that it is acting as a market participant rather than a regulator, and can therefore purchase service based on whatever criteria it chooses, e.g. only from ISPs that do not block, throttle, or engage in paid prioritization. However, states cannot condition their Internet service contracts on the future behavior of the ISP; that is, states cannot insert a contractual term to the effect of "if the ISP engages in blocking, throttling, or paid prioritization in the future, it will be deemed to have violated this contract," because that would be construed as a form of regulation.[116] On the other hand, states could choose to only contract with ISPs who have a history of not engaging in the activity stated above. That being said, the market participant exception only applies to the Dormant Commerce Clause, not preemption.[117] In *Wisconsin v. Gould*, the Supreme Court made clear that if a federal statute preempts state law, attempts to regulate through the spending power, as in the above example, are just regulation by another name.[118]

---

108. *Id.*
109. *See id.*
110. *See id.*
111. Pike v. Bruce Church, 397 U.S. 137, 142 (1970).
112. *Id.*
113. *Id.*
114. CHEMERINSKY, *supra* note 53, at 473.
115. *Id.*
116. South-Central Timber Development, Inc. v. Wunnicke, 467 U.S. 82, 97 (1984).
117. *See* Wisconsin Dept. of Indus. v. Gould, Inc., 475 U.S. 282, 290-91 (1986).
118. *Id.* at 1062.

D. Critical State Health and Safety Entities That Rely Upon the Internet

Multiple state and municipal entities integral to public health and safety rely on un-degraded Internet content delivery and transmission in order to keep the public safe.[119] These entities' missions are put at risk when ISPs are allowed to monetize all aspects of their service without due regard for their role in protecting public safety.[120] This Note's proposed law would seek to protect (1) designated municipal utilities, (2) designated public health and safety agencies, and (3) designated public hospitals.

1. The Power Grid

Utility companies and consumers have come to rely on a consistent, responsive Internet to manage the power grid.[121] The so-called "smart grid" allows consumers, energy wholesalers, and buyers to efficiently and safely manage the energy supply by allowing for instantaneous communication between its requisite parts.[122] The smart grid is critical to the safety of local communities because it allows utility companies to get electricity where it needs to be during emergencies and reduce energy loads during times of congestion.[123] This prevents power surges and allows utility companies to comply with federal reliability regulations.[124] Utility companies are integral to public safety, and therefore net neutrality should be preserved for municipal utility companies.[125]

2. Public Health and Safety Agencies

State and local governments use the Internet to manage emergency communications during times of natural disasters, weather events, active shooters, communicable disease outbreaks, and evacuations, and to distribute and receive general public health information.[126] Rapid response is necessary both to communicate with other agencies and with the public at large.[127] These entities are unlikely to have the budget to pay for the prioritization of their data, as are the agencies and entities that they must continuously communicate with to monitor public health and react efficiently in the face of emergencies.[128] As with other front line first responders, state laws should be

119. *See* Petition, *supra* note 10, at 23-28; FRANCESCA SPIDALIERI, STATE OF THE STATES CYBERSECURITY, PELL CENTER FOR INTERNATIONAL RELATIONS AND PUBLIC POLICY 3 (2015).
120. *See* Petition, *supra* note 10, at 23-28.
121. *See id.* at 24.
122. *Id.*
123. *Id.*
124. *Id.*
125. *See id.* at 24-25.
126. *See id.* at 26.
127. *Id.*
128. *Id.* at 28.

crafted to prevent the FCC's deregulation from frustrating their mandate to keep the public safe.

3. Hospitals

Hospitals are integral to public safety. They currently rely on the Internet to save lives and many are in the process of expanding their telemedicine practices, which would allow them to reach more patients and save more lives.[129] Telemedicine typically involves video conferencing and the transfer of large swaths of data.[130] It is not effective if the Internet is inconsistent or prohibitively expensive.[131] Even in the absence of a telemedicine expansion hospitals currently rely on fast and consistent Internet service to save lives in emergency situations.[132]

III. ANALYSIS

Relying on three separate legal theories, the *2018 Order* attempts to preempt "all state laws inconsistent with [the] Order."[133] In practice, this means that states cannot enact anti-blocking, anti-throttling, or anti-paid prioritization regulations.[134] However, the *2018 Order's* preemption claim is focused on state regulations designed to promote consumer protection.[135] It does not consider state laws designed to ensure consistent access to, and delivery of, the Internet content of critical public health and safety entities.[136] In fact, the *2018 Order* does not explicitly mention public health and safety one time.[137] This Note's proposed state law solely focuses on preventing ISPs from blocking, throttling, or deprioritizing data originating from or being sent to: (1) designated municipal utilities, (2) designated public health and safety agencies, and (3) designated public hospitals. Given the vital role ISPs play in modern public health and safety, the states' massive interest in protecting the health of their citizens, and the fact that the *2018 Order* does not consider how its deregulatory initiative will impact these critical state entities' ability to consistently send and receive vital Internet content, it is likely that narrowly tailored state regulations designed to protect these critical entities fall outside of the scope of the *2018 Order's* express preemption claim.[138] Such a law

129. *Id.* at 27.
130. *Id.*
131. *See id.* at 28.
132. *See id.* at 27.
133. *See 2018 Order*, *supra* note 10, at paras. 194-96.
134. *Id.*
135. *See generally id.*
136. *Id.*
137. *See generally id.* This point was conceded by the FCC during oral argument (Feb. 1, 2019). *See also* Mozilla Corp. v. FCC, No. 18-1051, 2019 WL 4777860 *1, *61 (D.C. Cir. 2019) ("nor does [the FCC] claim that it specifically addressed public safety in its 2018 Order").
138. *Supra* Section II.D.; *Medtronic v. Lohr*, 518 U.S. 470, 485 (1996) ("[W]e used a presumption against the pre-emption of state police power regulations to support a narrow interpretation of such an express command in Cipollone.")(internal quaotaion marks removed).

would also be immune from a conflict preemption challenge because the law is sufficiently narrow, such that it will not frustrate the FCC's regulatory scheme.

The proposed state law would not broadly reintroduce the regulations rolled back by the *2018 Order*. It would simply ensure that limited critical aspects of the state health and safety apparatus are able to receive fast and reliable Internet connection at market rates without worrying that the data is being unnecessarily degraded. In effect, the proposed law would put the designated critical entities on par with those able to pay for prioritization—just as they were before the *2018 Order*.

A. The 2018 Order Does Not Expressly Preempt the Proposed Law Because It Failed to Show It was Necessary to Preempt Such Laws

The FCC greatly reduced its ability to regulate ISPs, and to preempt states from doing so when it reclassified Internet service providers as Title I services.[139] Recall that when the FCC makes an express preemption claim under Title I, it is in effect regulating through its ancillary jurisdiction because the governing statutes do not give the FCC the explicit power to preempt.[140] In *Louisiana Public Service Commission*, the Supreme Court said that, to preempt under its ancillary authority, the FCC must show that preemption is *necessary* to achieve statutorily acceptable goals.[141] The *2018 Order* does not meet this high bar in regard to the proposed state law. The *2018 Order* went to great lengths to show that individual states instituting net neutrality regulations on a state-by-state basis would frustrate the purpose of the federal regulation, but it failed to address how a very limited and necessary statewide regime to protect critical safety entities would frustrate its policy.[142] It failed to take these limited regulations into account despite public comments and concrete evidence that these critical state entities would be greatly affected by the deregulation.[143] This indicates that the proposed law is outside of the scope of the FCC's express preemption claim because the FCC did not address, much less show, that preemption of the contemplated law is necessary to achieve the goals laid out in the *2018 Order*.[144]

B. The FCC's Asserted Legal Authority to Preempt State Laws Does Not Apply to the Proposed Law

The FCC asserted three distinct legal theories to justify their preemption authority: (1) the impossibility exception, (2) the policy

139. *See* Verizon v. FCC, 740 F.3d 623, 632 (D.C. Cir. 2014).
140. *See id.*; *Supra* note 80.
141. *See* ZUCKERMAN ET AL., *supra* note 88, at 764.
142. *See 2018 Order*, *supra* note 10, at paras. 194-96.
143. *See* Petition, *supra* note 8, at 22.
144. *Id.* at para. 196 (explaining that the *2018 Order* will not displace any state laws that do not interfere with federal regulatory objectives).

statement, and (3) forbearance.[145] The first two of these theories are applicable to this Note's proposed law. Each of these justifications is distinct and must be analyzed under different frameworks. The impossibility exception is a form of agency preemption and therefore should be analyzed under Shimer analysis and relevant case law involving the FCC.[146] The policy statement argument is an attempt to claim direct congressional authority to preempt, and forbearance is a theory based on judicial precedent, which was previously considered in Section II.A.3.

1. The Impossibility Exception Does Not Apply to the Proposed State Law

The impossibility exception applies when the FCC determines that an intrastate regulation (1) affects interstate communication, (2) would frustrate federal regulatory objectives, and (3) would negate the FCC's lawful authority.[147] The exception can be seen as a subset of agency preemption and therefore must also satisfy both prongs of Shimer analysis.[148] An FCC assertion that the proposed law is expressly preempted by the *2018 Order* would fail Shimer analysis at step two. It would also fail both the second and third prongs of the impossibility exception itself.

This exception is analyzed under Shimer because the FCC made the express preemption claim "pursuant to its [congressionally] delegated authority" to ensure the development of a robust Internet infrastructure.[149] However, Congress did not explicitly or implicitly revoke the states' ability to regulate in this field.[150] Thus, there is no direct congressional preemption. Instead, Congress gave the FCC authority to regulate, and the FCC decided that, to do so in line with its congressional mandate, it had to expressly preempt certain state laws.[151]

In order to satisfy the second prong of Shimer the agency must show that "[the] decision to preempt represents a reasonable accommodation of conflicting policies committed to the agency's care by statute."[152] In the present case, the FCC failed to address public safety concerns in the *2018 Order*, despite judicial precedent saying that such concerns must be addressed when issuing substantive rules.[153] This failure shows that the FCC did not reasonably consider or accommodate states' public safety concerns before attempting to preempt their authority to regulate in a field traditionally left to their control. This failure removes the proposed law from the scope of the *2018 Order's* express preemption claim.

---

145. *Supra* Section II.A; *see also* 2018 Order, *supra* note 10, at para. 197-204.
146. *Supra* Section II.A.1.
147. *2018 Order*, *supra* note 10, at para. 198; Petition, *supra* note 8, at 46.
148. *Supra* note 81.
149. Jordan, *supra* note 36, at 75.
150. *Mozilla Corp. v. FCC*, No. 18-1051, 2019 WL 4777860 *1, *52-53 (D.C. Cir. 2019).
151. *2018 Order*, *supra* note 10, at para. 198.
152. *See supra* Section II.B.2.
153. *Supra* note 20.

The express preemption claim also fails two of the three elements of the impossibility exception itself—namely the second and third prong. In order to satisfy the second prong of the impossibility exception, the FCC must determine that "the regulation would interfere with federal regulatory objectives."[154] The FCC fails this because it did not discuss how limited regulation designed to protect critical state health and safety services would frustrate federal regulatory objectives.[155] It did not contend that such a limited regime was either technologically or economically infeasible.[156] The FCC simply failed to discuss this despite being on notice that this was an issue of great concern, and despite going into detail on how a patchwork of state consumer protection-oriented and net neutrality-focused laws would frustrate the *2018 Order's* purpose.[157] Much like the fatal Shimer flaw above, this failure indicates that state regulation targeting public health and safety Internet service is outside the scope of the *2018 Order*. The third prong of the impossibility exception requires the FCC to state how the law in question "would negate [its] exercise of its lawful authority."[158] Again, the *2018 Order* fails this prong because it failed to address the issue.

That being said, the fact that the proposed law is outside of the scope of the *2018 Order's* express preemption claim does not necessarily mean it is guaranteed to survive traditional preemption analysis. This is a distinct analysis and the FCC made it clear in the *2018 Order* that it will challenge state laws under these traditional theories as well.[159]

2. The Proposed State Law Does Not Conflict with the Federal Regulatory Scheme and is Not Preempted

The FCC argues that a policy statement in the Telecommunications Act of 1996, combined with the congressional definition of telecommunications services in the same Act, implies that Congress meant to prohibit all common carriage type regulation of information services on a state and federal level, and thus when the FCC redefined ISPs as information services, the states were preempted from enacting such regulation.[160]

On its face, this pronouncement is tenuous, as the Act leaves regulation of purely intrastate services up to the states, who are free to introduce common carrier regulation as they see fit on purely intrastate services.[161] However, given the interstate nature of the Internet, it is true that a federal prohibition

154. *2018 Order*, *supra* note 10, at para. 198.

155. *Supra* note 124.

156. *Id.*

157. Petition, *supra* note 8, at 22; *see also* Public Service Com'n of Maryland v. FCC, 909 F.2d 1509, 1515 (D.C. Cir. 1990).

158. *Public Service Com'n of Maryland*, 909 F.2d at 1515.

159. *Supra* Section II.A. (explaining that the FCC is asserting three distinct legal theories to preempt state regulations).

160. *See supra* Section II.A.2.

161. *See* Petition for Emergency Relief and Declaratory Ruling Filed by Bell South Corp., 7 FCC Rcd 1619, 1620 (1992) (upheld by the Court of Appeals for the 11th Cir.).

against the regulation of information services as common carriers could affect state laws.[162] This would depend on a reviewing court's determination of whether or not Congress implicitly preempted state laws in the area. That being said, just because the federal government lacks the statutory authority to regulate in a certain way does not mean that states also lack that authority.[163]

Even if the D.C. Circuit finds this purported authority valid, it would not affect the outcome of this Note's proposed state law. A reviewing court would likely proceed under an implied conflict preemption analysis because implied field preemption only happens when Congress has created or authorized the creation of a federal regulatory scheme that is so pervasive as to have occupied the entire field.[164] Further, Section 253(b) of the Communications Act endorses state regulation in areas such as "public safety and welfare," and Section 601(c) of the Telecommunications Act explicitly states that "[t]his Act shall not be construed to modify, impair, or supersede . . . State or local law unless expressly so provided in such Act or amendments."[165] In the instant case, Congress has left aspects of the regulation to the states, and the *2018 Order* acknowledges that the states do in fact play a role in the regulation.[166] These facts indicate that implied conflict preemption analysis is likely to be used.

In conflict analysis, a state law will be preempted if (1) it is impossible or impracticable to comply with both federal and state laws at the same time, or (2) the state law frustrates the purposes of the federal regulatory scheme.[167] It is worth noting that under the current theory being analyzed a reviewing court would not engage in Shimer analysis because the FCC directly pointed to and interpreted a specific statutory delegation of authority to preempt the state law. As said above, Shimer is only used when an agency claims it must preempt to effectuate a congressional command. In the instant case, the court will engage in traditional conflict analysis.[168]

The first part of the analysis is not applicable to the proposed law because there is no express law that an ISP must follow. They are free to follow the repealed net neutrality regulations or not. The *2018 Order* makes clear that the Federal Trade Commission or Department of Justice can bring consumer protection claims against ISPs who promise in advertising or terms of service to follow net neutrality principles but do not.[169] Therefore, there is no conflict here. However, there is still the second element of the test.

In order to evaluate the second element, the court must look at the congressional intent of the governing acts and determine if the specific state law frustrates those purposes to such an extent that preemption is

---

162. *2018 Order*, *supra* note 10, at para. 194.
163. *See* Petition, *supra* note 8, at 46-47.
164. CHEMERINSKY, *supra* note 53, at 413.
165. 47 U.S.C. § 253(b); 47 U.S.C § 152; Petition, *supra* note 8, at 51-52.
166. *2018 Order*, *supra* note 10, at para. 196.
167. CHEMERINSKY, *supra* note 53, at 413.
168. Jordan, *supra* note 36, at 81.
169. *See 2018 Order*, *supra* note 10, at para. 2.

warranted.[170] Taking the FCC at its word, the purposes of the specific governing statute is to preserve "a vibrant free market unfettered by . . . regulation."[171] However, the *2018 Order* also imposes network management transparency rules on ISPs.[172] Therefore, the Telecommunications Act, and indeed the *2018 Order* itself, evidently anticipate that some type of regulation is necessary.[173]

The *2018 Order* itself only specifically seeks to preempt state laws that would broadly reintroduce the repealed net neutrality regulations.[174] Under the proposed state law, ISPs would still be able to offer prioritized service to non-critical edge providers, as well as block and throttle general content as they see fit. In this way, the law actually helps the FCC fulfill its mission of serving the public interest and the stated policy goal of supporting a vibrant Internet ecosystem because the ISPs will be able to make more money, which they can use to develop their networks without putting public safety at risk. Therefore, the proposed law does not frustrate the FCC's interpretation of congressional intent and a reviewing court would have no reason to find that the law conflicts with the federal regulatory scheme to such an extent that preemption is warranted.

C. State Regulations Can Be Designed to Avoid Violating the Dormant Commerce Clause

If the proposed state law survives a direct preemption challenge, it seems likely that it would also survive a challenge under the Dormant Commerce Clause, given that that kind of preemption is far less controversial within constitutional doctrine, and the fact that, to survive preemption, the law would have needed to show that it did not conflict with the federal regulations in place.[175] Still, they are two distinct challenges to the law's validity, and both should be analyzed. The Dormant Commerce Clause could become particularly relevant if the D.C. Circuit strikes down the FCC preemption clause.

Recall that the Dormant Commerce Clause is triggered when a state law poses an undue burden on interstate commerce, and Congress has the ability to legislate in the area but has not yet done so.[176] It is very important for the law not to discriminate, even unintentionally, against out of state business interests.

The distinction between *C & A Carbone, Inc. v. Town of Clarkstown* and *United Haulers Assn. v. Oneida-Herkimer Solid Waste Management Authority*,[177] discussed in Section II.C, is very important for the proposed law protecting critical state infrastructure because states, when crafting the law,

170. Levesque, *supra* note 35, at 317-18.
171. *2018 Order*, *supra* note 10, at para. 203 (quoting 47 U.S.C. § 230(b)(2), (f)(2)).
172. *Id.* at para. 209.
173. *Id.* at para. 3.
174. *Id.* at para. 195.
175. *See* CHEMERINSKY, *supra* note 53, at 445.
176. *Id.* at 443.
177. *Supra* note 108.

may be tempted to fold in any entity that they can make a colorable argument is critical to the state's health and safety. However, if the law includes privately owned businesses, such as hospitals and utility companies, then a court could easily find that the law has a discriminatory impact on interstate commerce. For example, it is easy to imagine that a private hospital or utility that is given a choice between two states—one that has laws mandating higher quality Internet service and another without a comparable law—will likely choose the state that has the protective law. It is also easy to imagine consumers preferring hospitals in states that prohibit ISPs from degrading critical data. If the court finds that there is a discriminatory impact, it would subject the law to strict scrutiny and the law is virtually guaranteed to be struck down.[178] On the other hand, if the state limits the proposed law to state or municipally owned entities, the court is more likely to apply the *Pike* balancing test, which is much more permissive of the state interest.[179]

The *Pike* test discussed in Section II.C is also a very fact sensitive balancing test, but the public interest served by critical communications infrastructure, especially that used by first responders, is likely to weigh heavy on a reviewing court.[180] The ISP challenging the statute would need to provide very persuasive evidence to outweigh the state's public interest. It could do this in three ways. First, it could attempt to show that the burden of blocking, throttling, and prioritization do not actually negatively affect the public interest at stake. This is a tall order considering the wildfire example already discussed. Second, the ISP may argue that the law burdens interstate commerce because it forces ISPs to shift costs to other non-regulated states and sectors. Third, the ISP could argue that the technology necessary to differentiate between critical public safety entities and non-entities either does not exist or is prohibitively expensive.[181]

The subjective nature of the test allows for biases and other considerations to creep into the court's analysis.[182] In the absence of a concrete claim by a litigant and specific facts, determining whether or not a statute will be upheld is especially difficult.[183] However, the state can make a solid argument that public health and safety are threatened by the absence of any substantive regulation of ISPs. The Supreme Court has been deferential to legitimate public safety concerns, even when those regulations incidentally propose seemingly substantial burdens on interstate commerce.[184] Thus, the key for states is to craft legislation so that it will be subject to the *Pike* test rather than strict scrutiny.

178. CHEMERINSKY, *supra* note 53, at 468.

179. *Supra* note 98.

180. *See* Metropolitan Life Ins., Co. v. Massachusetts, 105 S. Ct. 2380, 2398 (1985).

181. *See* Petition, *supra* note 8, at 23.

182. CHEMERINSKY, *supra* note 53, at 462.

183. Alascom, Inc. v. FCC, 727 F.2d 1212, 1220 (D.C. Cir. 1984) (discussing conflict preemption, but also applies to Dormant Commerce Clause).

184. CHEMERINSKY, *supra* note 53, at 431.

IV. CONCLUSION

Net neutrality is a divisive issue; there are good policy points and big money on both sides of the debate.[185] Net neutrality has mostly been discussed in a consumer protection context, but as the Internet came to dominate public life, it has become more than a way to entertain ourselves and connect with friends. The Internet is more than a way to efficiently run businesses. Indeed, it has become critical to public health and safety.[186] Removing all open Internet protections without any prohibitions against degrading critical public health and safety entities' data puts lives at risk and hampers the ability of states to efficiently respond to emergency situations.[187] It is important for safety that some form of regulatory protection is allowed to stay in place.[188] The FCC failed to take this into account when promulgating the *2018 Restoring Internet Freedom Order*,[189] and states can likely fashion regulations around any federal preemption or Dormant Commerce Clause claims.

Both preemption and the Dormant Commerce Clause are highly fact-specific and the analysis of proposed laws cannot receive the same level of scrutiny as they would in an actual case or controversy. This fact cuts against the FCC's presumptive claim to preempt "all state legislation inconsistent with [its] Order."[190] The waters surrounding agency preemption are muddier than most, and it can be hard to determine just what kind of preemption is being claimed.[191] The categories tend to bleed into each other. There is an ongoing legal debate about what kind of deference agency preemption claims should be given, and thus far the Supreme Court has failed to give any definitive guidance.[192]

Scholars arguing for little to no deference claim that agencies, especially independent agencies, are unaccountable to the voters and have an incentive to gather power for themselves.[193] People in favor of deferential treatment for agency preemption point to agency expertise and point out that agencies are indirectly accountable to voters.[194] The debate around agency preemption is made more complicated by the enormous discretion most statutes give to executive agencies.[195] It is quite easy for agencies to craft vast regulatory schemes within the confines of their governing statutes and then claim that any state law in the field would frustrate their purposes. Thus far

185. Anupam Chander, et al., *The Myth of Net Neutrality*, 2 GEO. L. TECH. REV. 400, 401 (2018).
186. *See* Petition, *supra* note 8, at 24; SPIDALIERI, *supra* note 116, at 3.
187. Petition, *supra* note 8, at 22-28.
188. *Id.*
189. *See* Petition, *supra* note 8, at 22.
190. *2018 Order*, *supra* note 10, at paras. 194-95.
191. Jordan, *supra* note 36, at 94.
192. Levesque, *supra* note 35, at 327-28.
193. *Id.*
194. *Id.*
195. *See id.* at 326.

courts have been somewhat deferential to these claims but, given the growth of the administrative state, perhaps courts should apply less deference.[196]

The state legislation that this Note proposes manages to stay out of the main thrust of the net neutrality policy debate by focusing on a relatively small amount of entities necessary to protect public health and safety. It respects the FCC's policy decision that "light touch regulation" will better serve the nation's communications infrastructure in the long run, but it also takes into account the states' need to ensure the safety of their citizens. As such, courts should uphold the proposed state legislation under both preemption and the Dormant Commerce Clause.

196. *Id.*