Federal Communications Law Journal

THE TECH JOURNAL

VOLUME 74

Editor-in-Chief

Merrill Weber

Senior Projects Editor
Pauline Wizig

Senior Articles Editor
Veronica Lark

Senior Publications Editor
Brittany Gault

Senior Managing Editor
Chloe Vizzone

Senior Production Editor
Bethel Etta

Senior Notes Editor
Jadyn Marks

Managing Editors
Anne Grae Martin
Harut Minasian

Articles Editor
Ellen Boettcher
John Killingbeck

Notes Editors
Julia Heasley
Natasha Nerenberg
Andrew M. Seneviratne

Production Editor
Alexa Pappas

Associates

Jaylla Brown
Michael DeJesus
Tyler Dillon
William Elman
James Elustondo
Kimia Favagehi
Daniel Fishelman
Chris Hon
Gabriella Joseph
Kyle J. Kessler
Young Kyoung Kim
Cashel Koski
Ellen Liew
Chengming Liu
Yirong Mao
Megane Messier
Francisco Maldonado
Andreu
Emily Rodriguez
Michael Scott

Members

Dallin Albright
Andrew Bearkland
John Bogert
Robin Briendel
Julia Dacy
Garrett Dowell
Delaney Dunn
John Evans
Nicolas Florio
Thompson Hangen
Alan Harrison
Julia Herring
Glen Hisani
Sydney Huppert
Kelly Hutchinson
Courtland Ingraham
Jonathan Johnson
Aleeza Kanner
Abraham Kim
Alyssa Kurke
Micah Leval
Anthony Licata
Adam Lindemulder
Briyana Louis
Max Matheu
Gavin McClure
Jacob Naim
Samantha Nardone
Leah Moonyoung Park
Aditi Patil
Vaibhavi Patria
Juan Pazmiño
Jamie Reiner
Rebecca Roberts
Catherine Tsang
Avery Turzanski
Patrick Walters
Julia Wells
Briana Whitmore

Faculty Advisors

PROFESSOR ARTURO CARRILLO
PROFESSOR DAWN NUNZIATO

Adjunct Faculty Advisors

MICHAEL BEDER
SARAH MORRIS
ETHAN LUCARELLI
MEREDITH ROSE

Published by The George Washington University Law School
and the Federal Communications Bar Association

EDITOR'S NOTE

FCLJ is excited to present the third and final Issue of Volume 74 of the *Federal Communications Law Journal.* This Issue features a practitioner Article, three student Notes, and the *Journal's* Annual Review of notable communications law. Issue Three covers several topics relating to consumer privacy, technological advancements, social media regulation, and more. Our authors present a myriad of ideas and arguments that demonstrate the need for federal regulators and legislative bodies to take action in the rapidly expanding field of communications and technology law.

This issue begins with an Article written by Scott Jordan. Jordan, a computer science professor at the University of California, Irvine, discusses consumer privacy—primarily, he addresses user notice and choice requirements as incorporated in Europe's General Data Privacy Protection Regulation and the California Consumer Privacy Act. Jordan critiques aspects of each law, suggesting that neither are sufficient for consumers' protection. Instead, Jordan proposes his own statutory text to resolve the current inadequacies in consumer privacy regulations.

This Issue also features three student Notes. The first Note, written by Jaylla Brown, posits that the use of biometric facial recognition—a technology police use to identify potential suspects with varying accuracy—should be disclosed to defendants under the rule in *Brady v. Maryland.* Brown argues that facial recognition system misidentifications disparately impact women and people of color, and that disclosing its use under *Brady's* due process requirements is imperative to formulating a misidentification defense.

The second Note, written by Veronica Lark, focuses on the Fourth Amendment's protection of consumer privacy as applied to blockchain transactions. Lark urges that the third-party doctrine, which states that consumers have no expectation of privacy in third-party entities, should not be applied to blockchain transactions. The *Journal's* third and final Note of Volume 74 is authored by Jadyn Marks. Marks addresses the ever-relevant topic of social media regulation, focusing her analysis on Facebook, Twitter, and Parler's internal policies for regulating political advertising, misinformation, and disinformation. Marks argues in favor of federal legislation that would permit the Federal Trade Commission to regulate these entities, citing section 230 and public policy as justifications for her proposition.

Finally, this Issue features our Annual Review of notable court decisions pertinent to our field. This year's review contains six case briefs summarizing the relevant issues and analysis presented in each case. I sincerely appreciate each *Journal* member who authored these case briefs and their contribution to communication law scholarship.

On behalf of the outgoing members of Volume 74, I would like to thank The George Washington University Law School, our faculty advisors, and the Federal Communications Bar Association for their support over the past year. Our publication has sincerely benefitted from your guidance and assistance. On my own behalf, I would like to thank the Volume 74 Editorial Board, Associates, Members, and authors who made this Volume possible. We have been honored to provide quality scholarship to the communications field and beyond, and are confident the Volume 75 Editorial Board will continue the *Journal's* excellence.

The *Journal* is committed to providing its readership with scholarly analysis and thought leadership on topics relevant to communications and information technology law and related policy issues. The *Journal* thus welcomes any submissions for publication, which may be directed to fcljarticles@law.gwu.edu for consideration. Any further questions or comments may be directed to fclj@law.gwu.edu. This Annual Review Issue and our archives are available at http://www.fclj.org.

Merrill Weber
Editor-in-Chief

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

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

Federal Communications Bar Association

The 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’s why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

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

FCBA Officers and Executive Committee Members
2021-2022

Megan Anne Stull, *President*
Barry J. Ohlson, *President-Elect*
Diane Griffin Holland, *Treasurer*
Krista L. Witanowski, *Assistant Treasurer*
Anna Gomez, *Secretary*
Kathleen A. Kirby, *Assistant Secretary*
Dennis P. Corbett, *Delegate to the ABA*
Cynthia B. Miller, *Chapter Representative*
Daniel Waggoner, *Chapter Representative*
Elizabeth Cuttner, *Young Lawyers Representative*

Paula H. Boyd
Matthew S. DelNero
Darah S. Franklin
Patrick R. Halley
Mia Guizzetti Hayes
Grace Koh
Natalie G. Roisman
Johanna R. Thomas
Stephanie S. Weiner
Sanford S. Williams

FCBA Staff

Kerry K. Loughney, *Executive Director*
Janeen T. Wynn, *Senior Manager, Programs and Special Projects*
Wendy Jo Parish, *Bookkeeper*
Elizabeth G. Hagerty, *Membership Services Administrator/Receptionist*

FCBA Editorial Advisory Board

Lawrence J. Spiwak Jeffrey S. Lanning

The George Washington University Law School

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

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

The *Federal Communications Law Journal* is published by The George Washington University Law School and the 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 fclj@law.gwu.edu.

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

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

Copyright: Copyright © 2022 Federal Communications Bar Association. Except as otherwise provided, the author of each article in this issue has granted permission for copies of the article to be made for classroom use, provided that 1) copies are distributed at or below cost, 2) the author and the *Journal* are identified, 3) proper notice of copyright is attached to each copy, and 4) the *Journal* is notified of the use.

Production: The citations in the *Journal* conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia L. Rev. Ass'n et al. eds., 21st ed., 2021). 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 74 FED. COMM. L.J. ___ (2022).

The views expressed in the articles and notes printed herein are not to be regarded as those of the *Journal*, the editors, faculty advisors, The George Washington University Law School, or the Federal Communications Bar Association.

FEDERAL COMMUNICATIONS
LAW JOURNAL

THE TECH JOURNAL

GW LAW VOLUME 74 ISSUE 3 fcba THE TECH BAR

APRIL 2022

ARTICLE

NOTES

heightened need for access to this evidence for defendants susceptible to misidentification.

This paper explains how facial recognition technology disproportionately misidentifies people based on race and gender and why any evidence indicating this occurrence satisfies the elements of the Brady rule. Until the racial disparities of facial recognition technology are solved, or restrictions are placed on how police use this technology, the Brady rule could provide opportunity for a fair trial when the only defense is misidentification by technology designed and used to disproportionately identify Black and brown people.

This paper draws a distinction between blockchains and cryptocurrency exchanges, and it shows how this distinction should alter the third-party doctrine analysis under the Fourth Amendment. By nature, blockchain is not a third-party entity—it is distinct from third-party cryptocurrency exchanges. However, courts have applied the third-party doctrine in cases implicating cryptocurrency exchanges, even when the malicious behavior occurred off of the exchange, on the decentralized blockchain, making this distinction a moot point. *Carpenter* proposes a framework concerning emerging technology that could easily be applied to the distinction between blockchain and exchanges. Other scholars in the privacy space have distinguished the problem of equating secrecy with privacy—a problem that is upheaved by blockchain's transparency and lack of third-party ownership—but there is also a need to distinguish blockchains from exchanges which use Know-Your-Customer protocols. With this in mind, requiring that law enforcement acquire a search warrant to pursue Coinbase customers seems to be the best way to resolve the issue. Consumers should have a reasonable expectation of privacy in their blockchain transactions because personally identifiable information is not shared with the blockchain, it is only shared with a cryptocurrency exchange. Consumers should not be subject to a general warrant simply for having a Coinbase account.

The tumultuous 2020 election brought to light several prevalent social and political issues, including the spread of misinformation and disinformation on social media. At present, social media sites are virtually unregulated in this area due to protections from section 230 of the Communications Decency Act of 1996. Due to Big Tech's minimal competition, social media companies can make virtually any rules they like and remain competitive as social media sites. Furthermore, social media companies whose business models thrive on engagement and hits are disincentivized to remove or flag disinformation when it increases engagement and thus increases profits. Inaccurate information about procedural aspects of elections, including locations of polling places, registration and voter eligibility, and the status of ongoing elections lead to voter disenfranchisement and have concerning implications for American

COMMUNICATIONS LAW: ANNUAL REVIEW

A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law

Scott Jordan[*]

TABLE OF CONTENTS

[*] Scott Jordan is a Professor of Computer Science at the University of California, Irvine. He served as the Chief Technologist of the Federal Communications Commission during 2014-2016. This material is based upon work supported by the National Science Foundation under Grant No. 1956393.

I. INTRODUCTION

The United States Congress has been devoting substantial attention to crafting a comprehensive consumer privacy law in the last few years. Any bill that attracts a majority vote is almost certain to include specific requirements for notices (e.g., elements of privacy policies) and for user choices (e.g., opt-out and/or opt-in). The formulation of these notice and choice provisions is the focus of this article.

Some researchers and stakeholders have criticized the notice and choice approach to consumer privacy regulation, pointing out the difficulty that consumers have reading privacy notices and the powerful position that businesses have in constructing choice mechanisms. Some researchers and stakeholders suggest imposing duties of care, loyalty, and confidentiality. However, whether or not such duties are incorporated into a future U.S. comprehensive consumer privacy law, it is exceedingly likely that notice and choice will remain a critical part of any such law.

In addition to notice and choice provisions, a comprehensive consumer privacy law may include requirements relating to a lawful basis other than user consent; data minimization; duties of care, loyalty, and confidentiality; readability of privacy policies; consumer rights to access, correct, and delete their personal information; methods for consumers to exercise these rights; methods for exercising choice; data portability; financial incentives; profiling; automated decision-making; research purposes; data security; data breaches; and enforcement. These issues are important but are outside the scope of this article.

The two common starting points for a comprehensive consumer privacy law are the 2016 European General Data Protection Regulation (GDPR)[1] and the 2018 California Consumer Privacy Act (CCPA).[2] In the GDPR and in the CCPA, notice requirements and user choices play a central role. However, the GDPR and the CCPA often do not agree on the specific requirements for notice and for user choice.[3] Thus, the GDPR and the CCPA often present two different policy options for notice and for choice.

However, policy options should not be limited to those offered by the GDPR and the CCPA. The notice requirements in these two options have proven to be insufficient to provide consumers the information necessary to make informed choices about their use of services and applications. Privacy policies often use non-standardized definitions of personal information that do not align with those in the GDPR or the CCPA or even with each other, leaving consumers confused about what constitutes personal information. Privacy policies often include assertions about the anonymity of personal information that exceed both the technical abilities and legal definitions of

[1] Commission Regulation 2016/679, 2016 O.J. (L 119/1) [hereinafter GDPR].

[2] CAL. CIV. CODE § 1798 (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[3] *See generally* Scott Jordan, *Strengths and Weaknesses of Notice and Consent Requirements Under the GDPR, the CCPA/CPRA, and the FCC Broadband Privacy Order*, CARDOZO ARTS & ENT. L.J., (2021), https://papers.ssrn.com/abstract=3894553.

anonymization and of de-identification. Privacy policies often lack specificity over what personal information is collected and how, leaving consumers uncertain about the related privacy risks. Additionally, privacy policies often lack transparency about which personal information is required to provide functionality of the service or app, and which personal information is used for non-functional purposes such as advertising, frustrating consumers' attempts to balance functionality and privacy. Privacy policies often fail to disclose sufficient information about sharing of personal information, impeding consumers' ability to understand the degree of identifiability of their shared information, to determine the associated privacy risks, or to follow the dissemination of their personal information through the data ecosystem. A comprehensive consumer privacy law should remedy these shortcomings of the GDPR and the CCPA.

Turning to the opt-in and opt-out choices currently offered to consumers, there are also failings that need to be addressed. When privacy policies give choices to consumers, the choices are often limited. Privacy policies often give consumers little choice over what personal information is collected. Privacy policies generally do not provide consumers choices about the use of their personal information that provide a tradeoff between functionality of the service or application and the consumer's privacy. Privacy policies also often fail to give consumers much control over which of their personal information is shared, with whom, and for what purposes. Ultimately, privacy policies generally give consumers little control over the dissemination of their personal information through the data ecosystem. The choice requirements mandated by the GDPR (often described as opt-in) and by the CCPA (often described as opt-out) present two different policy options. However, there are policy options that apply opt-in and opt-out requirements to different types of personal information, that may be superior to either the GDPR's or the CCPA's approaches, and that may remedy these shortcomings.

The academic literature includes several articles that analyze the GDPR and/or the CCPA. Hoofnagle, van der Sloot, and Borgesios provide an overview of the GDPR's roots and goals.[4] They explain the history of European data protection and privacy laws prior to the GDPR,[5] the GDPR's scope,[6] Fair Information Practices,[7] the legal basis for processing personal data,[8] special requirements for sensitive personal data,[9] data transfers,[10] and enforcement.[11] They also broadly discuss the responsibilities of businesses and processors[12] and the rights of consumers.[13] However, this piece does not give detailed analyses of notice and consent requirements.

[4] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What it is and What it Means*, 28 INFO. & COMMC'NS TECHNOLOGY L. 65 (2019).

[5] *Id.* at 69-72.

[6] *Id.* at 72-76.

[7] *Id.* at 76-78.

[8] *Id.* at 79-82.

[9] *Id.* at 82-83.

[10] *Id.* at 83-85.

[11] *Id.* at 92-97.

[12] *Id.* at 85-88.

[13] *Id.* at 88-92.

Hintze provides a summary of the GDPR's notice requirements, along with advice on how a business may comply with them.[14] He briefly discusses the types of organizations subject to the GDPR,[15] and then discusses in detail the required elements of privacy notices. His article is broader than the focus of this article, including discussion of not only notices regarding the processing of personal data, but also notices regarding the identity of the controller;[16] the legal basis for processing personal data;[17] user rights to access, correct, and delete personal data;[18] the user right to data portability;[19] the user right to complain;[20] data transfers;[21] and data retention.[22] Pardau provides a summary of the unamended original version of the CCPA.[23] He briefly summarizes the CCPA's notice and consent requirements.[24] He also summarizes other provisions in the CCPA, including its scope[25] and user rights to access and delete personal information.[26]

There are a few academic articles that compare various aspects of the GDPR and the CCPA. Buresh compares the European and American principles and definitions of privacy and discusses some of the relevant case law.[27] He then compares user rights under the GDPR and the unamended original version of the CCPA. Blanke focuses on the protection under the GDPR and the CCPA of personal information that consists of inferences drawn from other personal information.[28] However, neither article goes into much detail on the similarities and differences in the notice and consent requirements of the GDPR and the CCPA.[29] Jordan compares the notice and consent requirements of the GDPR, the unamended original version of the CCPA, and the recently amended version of the CCPA, including definitions of personal information; notices regarding use, collection, and sharing; and choice frameworks.[30]

The academic literature also includes many articles that criticize the GDPR and/or the CCPA, and that propose alternatives to notice and choice

[14] Mike Hintze, *Privacy Statements Under the GDPR*, 42 SEATTLE UNIV. L. REV. 1129-30 (2019).

[15] *Id.* at 1131.

[16] *Id.* at 1132-34.

[17] *Id.* at 1138-39.

[18] *Id.* at 1140-42

[19] *Id.* at 1142.

[20] *Id.* at 1144.

[21] *Id.* at 1144-47.

[22] *Id.* at 1147-48.

[23] Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECHNOLOGY L. & POL'Y 68, 91-100 (2018).

[24] *Id.* at 96-99.

[25] *Id.* at 92-93.

[26] *Id.* at 94-96.

[27] Donald L. Buresh, *A Comparison Between the European and the American Approaches to Privacy*, 6 INDONESIAN J. INT'L & COMPAR. L. 257 (2019).

[28] Jordan M. Blanke, *Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act*, 1 GLOB. PRIV. L. REV. 81 (2020).

[29] In addition, this article disagrees with some of the comparisons drawn in Buresh, *supra* note 27.

[30] *See generally* Jordan, *supra* note 3.

frameworks. Van Eijk *et al.* propose supplementing notice and choice with rules on unfair commercial practices.[31] Rothchild suggests supplementing notice and choice with rules grounded in the doctrines of unfairness and unconscionability.[32] Barrett proposes applying a fiduciary requirement to data collectors.[33] Hartzog and Richards propose a combination of rules regarding the corporate form: duties of discretion, honesty, protection, and loyalty; data minimization, deletion, and obscurity; and mitigating externalities.[34]

However, few academic articles propose specific requirements for notices of collection, use, and sharing. Hintze briefly argues that privacy policies should include increased detail, e.g., more granular detail about collection of personal information, and separate disclosures *for each category* of personal information collected of the purpose for collecting that category of personal information.[35] In contrast, Pardau briefly argues that a business' privacy policy should not be required to disclose the detailed list of disclosures about collection, use, and sharing required by the CCPA, but should only be required to disclose "the nature of its business as it relates to the collection of personal information."[36]

Similarly, there are no academic articles that propose alternative choice frameworks to those in the GDPR and in the CCPA.

The void in the academic literature has been filled by proposals from advocacy groups. Following is a brief summary of the notice and choice provisions in three frameworks that likely span the spectrum.

Privacy for America, an advocacy group composed of advertiser trade associations, proposed statutory text for a comprehensive consumer privacy law.[37] Privacy for America proposes fairly standard definitions of personal information[38] and de-identified information,[39] and a narrow definition of sensitive information that omits web browsing history.[40] With respect to collection and use of personal information, required disclosures are minimal, only including the categories of personal information collected and used.[41] With respect to sharing, required disclosures are heightened, including the categories of third parties and, for each such category, the categories of

[31] Nico van Eijk et al., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, 3 EUROPEAN DATA PROT. L. REV. 325, 334-37 (2017).

[32] John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEVELAND STATE L. REV. 559, 637 (2018).

[33] *See generally* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE UNIV. L. REV. 1057 (2019).

[34] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1745-1760 (2020).

[35] Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1083-1084 (2017).

[36] Pardau, *supra* note 23, at 112.

[37] PRIVACY FOR AMERICA, PRINCIPLES FOR PRIVACY LEGISLATION 13-39 (2019), https://www.privacyforamerica.com/wp-content/uploads/2020/01/Principles-for-Privacy-Legislation.pdf.

[38] *Id.* at 16.

[39] *Id.* at 14-15.

[40] *Id.* at 22-24.

[41] *Id.* at 20.

personal information shared and categories of uses.[42] Privacy for America proposes that opt-in consent be required for collection, use, or sharing of sensitive personal information.[43] It proposes no opt-in or opt-out requirements for its broad definition of non-sensitive personal information, other than an opt-out requirement from a narrow subset of data personalization.[44]

The Information Technology & Innovation Foundation (ITIF), an advocacy group funded in large part by the tech and communications industries,[45] proposes elements that it recommends be included in a comprehensive consumer privacy law.[46] ITIF argues for (but does not propose) a narrow definition of personally identifiable information that omits some types of linkable personal information.[47] It argues for (but does not propose) a broad definition of de-identified data that includes not only anonymized and aggregated data but also pseudonymized data.[48] ITIF recommends a narrow definition of sensitive personal data that omits much of web browsing history,[49] and a definition of critical services.[50] It gives few recommendations about notice,[51] but proposes that there should be no required disclosure of the use of personal information.[52] ITIF proposes a novel framework for choice. It proposes that opt-in consent be required for the collection of sensitive personal data for critical services, and that consumers be given an opt-out choice from the collection of non-sensitive personal data for critical services and from the collection of sensitive personal data for non-critical services.[53] It proposes that there should be no opt-in or opt-out requirements for the collection of its broad definition of non-personal data for non-critical services.[54] Finally, although ITIF argues that a law should provide incentives for data sharing, it does not propose any specific provisions regarding sharing.[55]

The Mozilla Foundation, an advocacy group funded primarily by royalties from Firefox web browser search partnerships, proposes a blueprint for a comprehensive consumer privacy law.[56] Mozilla proposes a broad

[42] *Id.* at 20.

[43] *Id.* at 22-24.

[44] *Id.* at 31, 32.

[45] ITIF's funders include Amazon, Apple, AT&T, Charter Communications, Comcast, CTIA, Facebook, Google, Microsoft, NCTA, T-Mobile, U.S. Telecom, and Verizon, among others. *Our Supporters*, INFO. TECHNOLOGY & INNOVATION FOUND., https://itif.org/our-supporters [https://perma.cc/7DKG-9BW3].

[46] ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA (2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america [https://perma.cc/SEF9-Y8C7].

[47] *Id.* at 16.

[48] *Id.* at 18.

[49] *Id.* at 16.

[50] *Id.*

[51] *Id.* at 27.

[52] *Id.* at 49.

[53] *Id.* at 23.

[54] *Id.*

[55] *Id.* at 39.

[56] MOZILLA, U.S. CONSUMER PRIVACY BILL BLUEPRINT (2019), https://blog.mozilla.org/netpolicy/files/2019/04/Mozilla-U.S.-Consumer-Privacy-Bill-Blueprint-4.4.19-2.pdf [https://perma.cc/4JH2-4RUE].

definition of covered data that includes information that can be reasonably connected to either a person or a device,[57] and argues for (but does not propose) a broad definition of sensitive data.[58] Mozilla makes detailed and expansive recommendations about notice. It proposes that privacy policies should disclose the personal data collected and the sources; the use of personal data, including inferences and decisions based on that data; the categories of personal data shared, with whom, and for what purposes.[59] Mozilla also proposes a novel framework for choice. It proposes that opt-in consent be required for the linking of personal information collected and shared by multiple entities.[60] It proposes that consumers be given an opt-out choice from specific granular uses of their personal information,[61] particularly including marketing.[62] Mozilla does not propose specific consumer choice requirements for collection or sharing, other than for the linking of personal information.

Two of the most discussed bills in the last session of Congress were the Consumer Online Privacy Rights Act (COPRA)[63] sponsored by Sen. Cantwell, and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA)[64] sponsored by Sen. Wicker.

The COPRA bill includes a definition of *covered data* which includes information that is reasonably linkable to either an individual or a device,[65] a definition of *de-identified data* which includes information that is not reasonably linkable to either an individual or device,[66] and a broad definition of *sensitive covered data* that includes online activities.[67] It requires that privacy policies disclose a moderate amount of detail, including the categories of covered data collected and used and the purposes for collecting and using each category, and a list of third parties with which covered data is shared and the purposes for which it is shared with each.[68] The COPRA bill requires that opt-in consent be obtained for the use or sharing of sensitive data for non-functional purposes,[69] and that consumers be given an opt-out choice from sharing of non-sensitive data for non-functional purposes.[70]

The SAFE DATA bill includes a similar definition of *de-identified data* as does the COPRA bill,[71] but a narrower definition of *covered data* which similarly includes information that is reasonably linkable to an individual, but

[57] *Id.* at 2.

[58] *Id.*

[59] *Id.* at 9.

[60] *Id.* at 5.

[61] *Id.* at 8.

[62] *Id.* at 9.

[63] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) [hereinafter COPRA].

[64] SAFE DATA Act, S. 4626, 116th Cong. (2020) [hereinafter SAFE DATA].

[65] COPRA, *supra* note 63, at § 2(8).

[66] *Id.* § 2(10).

[67] *Id.* § 2(20).

[68] *Id.* § 102(b)(2-3).

[69] *Id.* §§ 105(c)(1-2), 110(c-d).

[70] *Id.* §§ 105(b)(1), 110(c-d).

[71] SAFE DATA, *supra* note 64, at § 2(10)(E).

only includes information that is reasonably linkable to a device if the device is itself reasonably linkable to an individual, and a narrower definition of *sensitive covered data* that omits many online activities.[72] It requires similar disclosures in privacy policies as does the COPRA bill about the collection and use of covered data,[73] but with respect to sharing it requires less detailed disclosures that only identify the categories of recipients rather than a list of recipients.[74] As with the COPRA bill, it requires that opt-in consent be obtained for the use or sharing of sensitive data for non-functional purposes, but the scope of sensitive data is narrower.[75] It also requires that consumers be given an opt-out choice from collection, use, and sharing of non-sensitive data for non-functional purposes.[76]

The remainder of this article is devoted to identifying failures of the GDPR and the CCPA and to developing alternatives. In Part II, this article reviews the choice frameworks under the GDPR and the CCPA, finding that although both differentiate on the basis of whether personal information is sensitive and on whether it is used solely for functional purposes, neither utilizes both opt-in and opt-out choices. This lack of utilization of both options results in a diffuse application of choice that does not properly differentiate between various degrees of identifiability.

In Part III, the analysis delineates between different types of personal information on the basis of whether the personal information is trackable and/or identifiable. Looking first to the computer science literature to understand the abilities of various types of privacy-preserving algorithms and the spectrum of identifiability that they enable, it is evident that the GDPR's and the CCPA's definitions of personal information are too broad to differentiate between meaningful differences in identifiability within them, and thereby too broad to effectively encourage privacy-preserving treatment. Thus, it would make sense to categorize personal information into three types: reasonably identifiable, pseudonymous, and non-trackable.

Presented in Part IV are examples of collection, use, and sharing of these three types of personal information. The article differentiates between uses of personal information that enable functionality of a service or app versus those that do not. These examples illustrate the need for notices that disclose these differences and the need for choice mechanisms that afford consumers different choices for different types of personal information.

In Part V, a new choice framework is constructed, taking into account both opt-in and opt-out choices, as well as collection, use, and sharing required as part of the terms of a service. Unlike the GDPR (which doesn't use opt-out) and the CCPA (which only uses opt-in for minors and financial incentives), the proposed framework utilizes the full spectrum of user choice options in order to incentive the full spectrum of privacy-preserving techniques. The article differentiates between functional and non-functional

[72] *Id.* § 2(30).
[73] *Id.* § 102(b)(2-3).
[74] *Id.* § 102(b)(4).
[75] *Id.* §§ 104(a), 108(a).
[76] *Id.* §§ 104(d), 108(a).

use, between non-sensitive and sensitive personal information, and between use and sharing.

Illustrated in Part VI is the effect of this user choice framework on different types of advertising. It shows how the proposed choice framework incentives the use of contextual ads over audience segment ads, and the use of audience segment ads over behavioral ads, and how it disincentivizes tracking.

In Part VII, specific requirements are crafted for disclosures of collection, use, and sharing in privacy policies. These requirements include more detailed disclosures than those required in the GDPR or the CCPA, so that consumers may understand the degree of identifiability of their personal information collected and used, the flow of their personal information through the data ecosystem, and the associated privacy risks.

Finally, Part VIII develops statutory text that implements the proposed choice framework. There are proposed definitions for each of the types of personal information, the goal being to illustrate problems in current privacy policies, and create definitions to address these problems, drawing from the GDPR and the CCPA when helpful. Additionally, the article offers potential legal controls that should accompany each type of personal information.

The proposed statutory text is restated in the Appendix.

II. FAILURES OF THE GDPR AND THE CCPA TO USE BOTH OPT-IN AND OPT-OUT CHOICES

Consent is a primary driver for both the GDPR and the CCPA. However, they approach the issue of consent very differently, and, consequently, afford consumers substantially different choices.

Both the GDPR and the CCPA differentiate on the basis of whether the information is sensitive.[77] This article considers the definition of *sensitive information* in Part VIII. Both the GDPR and the CCPA also differentiate on the basis of whether the information is necessary to offer functionality of the service or application.[78] This article considers the definition of *functional use* in Part VIII.

When *non-sensitive personal information* is only used to provide functionality of the service or application, both the GDPR and the CCPA allow a business to mandate its collection and use in the terms and conditions of the service.[79]

However, when a business wishes to use *sensitive personal information* to provide functionality, the GDPR and the CCPA disagree. The CCPA allows a business to mandate the collection and use of personal information for functional purposes in the terms and conditions of the service.[80] In

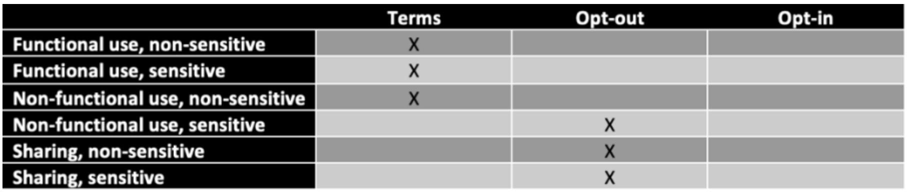
[77] Jordan, *supra* note 3, at 33-35.

[78] *Id.* at 28.

[79] GDPR, *supra* note 1, at art. 6(1)(b); Jordan, *supra* note 3, at 28.

[80] Jordan, *supra* note 3, at 28.

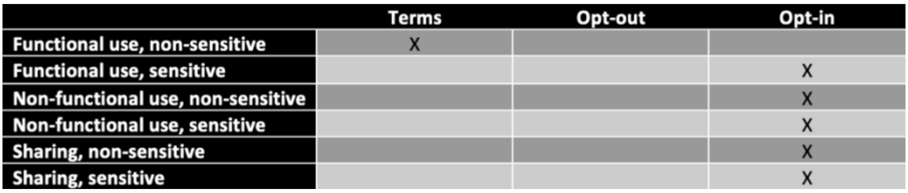
contrast, the GDPR requires that the business obtain opt-in consent from the consumer, absent another legal basis for the collection and use.[81]



	Terms	Opt-out	Opt-in
Functional use, non-sensitive	X		
Functional use, sensitive	X		
Non-functional use, non-sensitive	X		
Non-functional use, sensitive		X	
Sharing, non-sensitive		X	
Sharing, sensitive		X	

Table 1. User choice under the CCPA.

When *non-sensitive personal information* is used for a purpose other than to provide functionality of the service or application, the GDPR and the CCPA again disagree. The CCPA allows a business to mandate the collection and use of personal information for non-functional purposes in the terms and conditions of the service.[82] In contrast, the GDPR requires that the business obtain opt-in consent from the consumer, absent another legal basis for the collection and use.[83]



	Terms	Opt-out	Opt-in
Functional use, non-sensitive	X		
Functional use, sensitive			X
Non-functional use, non-sensitive			X
Non-functional use, sensitive			X
Sharing, non-sensitive			X
Sharing, sensitive			X

Table 2. User choice under the GDPR.

When a business wishes to use *sensitive personal information* for a purpose other than to provide functionality of the service or application, the GDPR and the CCPA again disagree. The CCPA requires that the consumer be given an opt-out choice,[84] while the GDPR requires opt-in consent absent another legal basis.[85]

Finally, when a business wishes to share either personal information with another business, the GDPR and the CCPA again disagree. The CCPA again requires an opt-out choice,[86] while the GDPR again requires opt-in consent absent another legal basis.[87]

The resulting differences in choice between the GDPR and the CCPA are wide. While the GDPR and the CCPA both allow a business to mandate in the terms and conditions of a service the collection and use of personal information for functional purposes, they do not agree on anything else related to choice.

[81] GDPR, *supra* note 1, at art. 9(2)(a).

[82] Jordan, *supra* note 3, at 28.

[83] GDPR, *supra* note1, at art. 6(1)(a).

[84] CAL. CIV. CODE § 1798.121(a) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[85] GDPR, *supra* note 1, at art. 9(2)(a).

[86] CAL. CIV. CODE §§ 1798.120(a), 1798.121(b).

[87] GDPR, *supra* note 1, at arts. 6(1)(a), 9(2)(a).

Furthermore, neither the GDPR nor the CCPA utilize all three options: mandating use through terms and conditions, requiring an opt-out choice, and requiring opt-in consent. The CCPA utilizes terms and opt-out, but not opt-in. The GDPR utilizes terms and opt-in, but not opt-out. This underutilization of all three options brings up the question of whether doing so could result in a more effective choice framework.

III. FAILURES OF THE GDPR AND THE CCPA TO ADDRESS THE SPECTRUM OF IDENTIFIABILITY

A. Limited Definitions in the GDPR and in the CCPA

Both the GDPR and the CCPA apply their choice frameworks to information related to an identifiable person, but not to information that is related to an unidentifiable person. The GDPR defines *personal data* (its version of personal information) as "any information relating to an identified or identifiable natural person."[88]

Under the GDPR, *personal data* does not include *anonymous information*, which it defines as "information which does not relate to an identified or identifiable natural person."[89]

Personal data is subject to the GDPR's choice framework, and *anonymous information* is not.

The CCPA defines *personal information* as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[90]

However, the CCPA also recognizes that there may be information that can be linked to a particular consumer or household, but for which the process of linking may be prohibitive due to the difficulty in finding other information with which it can be linked. In 2012, the Federal Trade Commission issued a report containing recommendations for businesses and policymakers.[91] It proposed that information be considered *de-identified information* if it is not reasonably linkable to a particular consumer or device.[92] In a similar vein, the CCPA defines *de-identified information* as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer . . . ."[93]

Under the CCPA, *personal information* does not include *de-identified information*. *Personal information* is subject to the CCPA's choice framework, and *de-identified information* is not.

[88] *Id.* at art. 4(1).

[89] *Id.* at recital 26.

[90] CAL. CIV. CODE § 1798.140(v)(1).

[91] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012) [hereinafter *FTC Report*].

[92] *Id.* at 21.

[93] CAL. CIV. CODE § 1798.140(m).

Both the GDPR and the CCPA thus classify any information relating to a person into one of two mutually exclusive sets (for the GDPR, *personal data* or *anonymous information*; for the CCPA, *personal information* or *de-identified information*) based on whether the person is identifiable.

Unfortunately, while this partition of information into only two sets is simple, it does not reflect the spectrum of identifiability of personal information. Within the category of information that the GDPR classifies as *personal data* and that the CCPA classifies as *personal information*, research has repeatedly shown that there are substantial differences in the degree of identifiability.[94] These differences should be reflected in a choice framework.

B. Lack of Recognition of the Benefits of Pseudonymous Information

In *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification* Jules Polonetsky presents a spectrum of identifiability of information.[95] To differentiate degrees of identifiability, the article uses the concepts of a *direct identifier* and of an *indirect identifier*.[96] While there is no need to define these terms in a consumer privacy law, the concepts are useful. Simon Garfinkel, in a report by the National Institute of Standards and Technology, defines a *direct identifier* as "data that directly identifies a single individual."[97] Polonetsky somewhat similarly defines a *direct identifier* as "data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain."[98] Garfinkel then defines an *indirect identifier* as "information that can be used to identify an individual through association with other information."[99]

The most identifiable form of information is that relating to an identified person or household.[100] It contains direct identifiers such as a person's name, personal telephone number, personal email address, driver's license number, or social security number. Polonetsky calls such information *explicitly personal data*,[101] but this article will use the term *reasonably identifiable information*. This type of information is classified as personal information under both the GDPR and the CCPA.[102]

The second most identifiable form of information is information relating to a person or household that is identifiable but has not yet been

[94] *See generally* Scott Jordan, *Aligning Legal Definitions of Personal Information with the Computer Science of Identifiability*, RES. CONF. ON COMMUN., INFO., AND INTERNET POL'Y (Sept. 2021), https://ssrn.com/abstract=3893833.

[95] Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SANTA CLARA L. REV. 593 (2016).

[96] *Id.*

[97] SIMSON L. GARFINKEL, NAT'L INST. OF STANDARDS & TECHNOLOGY, DE-IDENTIFICATION OF PERSONAL INFORMATION 1, 40 (2015).

[98] Polonetsky et al., *supra* note 95, at 605.

[99] GARFINKEL, *supra* note 97, at 41.

[100] Polonetsky et al., *supra* note 95, at 609.

[101] *Id.*

[102] Jordan, *supra* note 3, at 9-12.

identified, and that is tracked over time.[103] It does not contain direct identifiers, and thus the person or household cannot be identified using a direct identifier.[104] However, this type of information contains indirect identifiers, such as a device identifier or advertising identifier, that can be used to identify the person or household by combining the information with other information containing the same indirect identifiers.[105] The indirect identifiers can also be used to track the person or household over time.[106] Polonetsky calls such information *potentially identifiable*,[107] but this article will use the more common term *pseudonymous information*. This type of information is classified as personal information under both the GDPR and the CCPA, absent legal controls to prevent reidentification.[108]

Neither the GDPR nor the CCPA differentiates between *reasonably identifiable information* and *pseudonymous information* in their choice frameworks.[109] The GDPR requires opt-in consent for the sharing of both types of information.[110] The CCPA requires an opt-out choice from the sharing of either type of information.[111] As a consequence, neither the GDPR nor the CCPA incentivize the use of pseudonyms in their choice frameworks.

C. Lack of Recognition of the Benefits of Non-Trackable Information

A form of information that is less identifiable than *pseudonymous information* is information relating to a person or household that is identifiable but has not yet been identified, and that is *not* tracked over time.[112] It does not contain direct identifiers.[113] It may contain indirect identifiers, but these indirect identifiers cannot be persistent.[114] An example of a non-persistent identifier is a randomized identifier that is only used in a single interaction with a consumer.[115] Apple is beginning to use such one-time identifiers in some of its applications. Polonetsky calls such information *pseudonymous*,[116] but this article will use the term *non-trackable information*. This type of information is classified as personal information under both the GDPR and the CCPA, absent legal controls to prevent reidentification.[117]

[103] Polonetsky et al., *supra* note 95, at 609-13.
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] Jordan, *supra* note 3, at 9-12.
[109] *Id.*
[110] *Id.* at 31-32.
[111] *Id.*
[112] Jordan, *supra* note 94, at 14-17.
[113] *Id.*
[114] *Id.*
[115] Polonetsky et al., *supra* note 95, at 608.
[116] *Id.* at 615-17.
[117] Jordan, *supra* note 3, at 9-12.

Neither the GDPR nor the CCPA differentiate between *pseudonymous information* and *non-trackable information* in their choice frameworks.[118] The GDPR requires opt-in consent for the sharing of both types of information.[119] The CCPA requires an opt-out choice from the sharing of either type of information.[120] As a consequence, neither the GDPR nor the CCPA incentivize the use of one-time identifiers in their choice frameworks. However, the use of such one-time identifiers could eliminate tracking.

D. Differences in Consumer Views of Reasonably Identifiable Information, Pseudonymous Information, and Non-Trackable Information

The consumer views of reasonably identifiable information, pseudonymous information, and non-trackable information are quite different.

An example of reasonably identifiable information is a person's name paired with personal information about the person.[121] The information can be used for behavioral advertising, since the personal information may provide valuable information about the person's interests. An ad broker can collect reasonably identifiable information and create a profile of the person, resulting in tracking. Furthermore, this profile is associated with the person's name.

An example of pseudonymous information is a device or advertising identifier paired with personal information about the person using the device. As with reasonably identifiable information, the information can be used for behavioral advertising and tracking. However, the profile is associated with the device or advertising identifier, not with the person's name, providing that device or advertising identifier is not associated with a person or household. As a result, the person seeing the advertisements may properly perceive that they are pseudonymous.

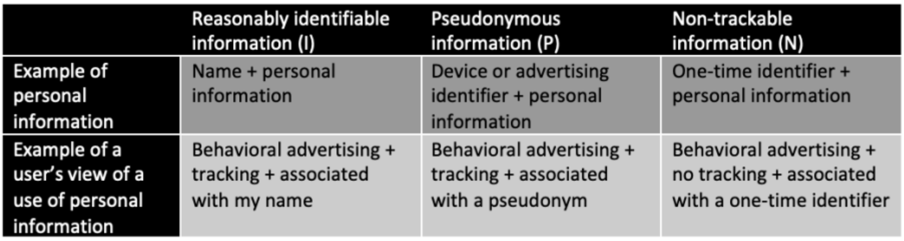
An example of non-trackable information is a one-time identifier paired with personal information. As with the other types of information, it can be used for behavioral advertising. However, it cannot be used for tracking. As a result, the person seeing the advertisements may properly perceive that they are pseudonymous and not tracked.

[118] *Id.*

[119] *Id.* at 14-16.

[120] *Id.*

[121] *Id.* at 6-8.



	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Example of personal information	Name + personal information	Device or advertising identifier + personal information	One-time identifier + personal information
Example of a user's view of a use of personal information	Behavioral advertising + tracking + associated with my name	Behavioral advertising + tracking + associated with a pseudonym	Behavioral advertising + no tracking + associated with a one-time identifier

Table 3. Examples of the Three Most Identifiable Types of Personal Information

These three types are summarized in Table 3. Although neither the GDPR nor the CCPA choice frameworks differentiate between these three types of personal information, consumers are likely to view their use very differently.

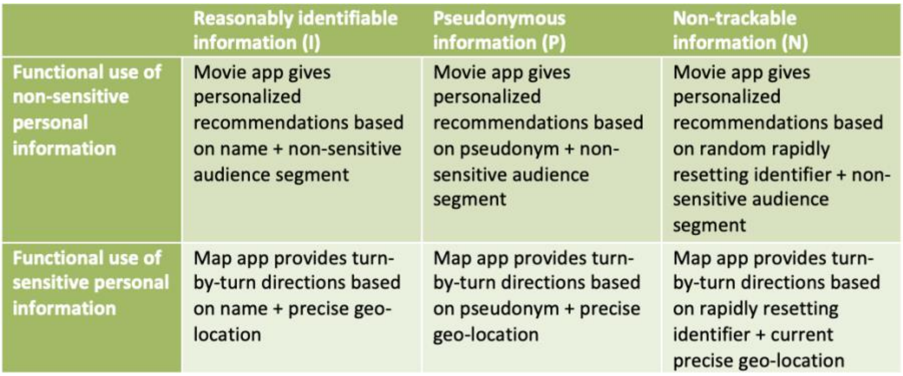
IV. EXAMPLES OF COLLECTION, USE, AND SHARING OF DIFFERENT TYPES OF PERSONAL INFORMATION

Part V will formulate a framework for choices that consumers should be given in a consumer privacy law. To inform the development of this framework, this section gives examples of collection, use, and sharing of the types of personal information discussed in Part III.

Both the GDPR and the CCPA make some attempts to distinguish between uses of personal information that are related to the functionality of the service or app versus uses that are not related. Before examining their approaches to this distinction, this article provides some examples of uses of various types of personal information.

A. Functional Use

Some uses of personal information enable functions or features of a service or app. Table 4 presents some examples.



	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Functional use of non-sensitive personal information	Movie app gives personalized recommendations based on name + non-sensitive audience segment	Movie app gives personalized recommendations based on pseudonym + non-sensitive audience segment	Movie app gives personalized recommendations based on random rapidly resetting identifier + non-sensitive audience segment
Functional use of sensitive personal information	Map app provides turn-by-turn directions based on name + precise geo-location	Map app provides turn-by-turn directions based on pseudonym + precise geo-location	Map app provides turn-by-turn directions based on rapidly resetting identifier + current precise geo-location

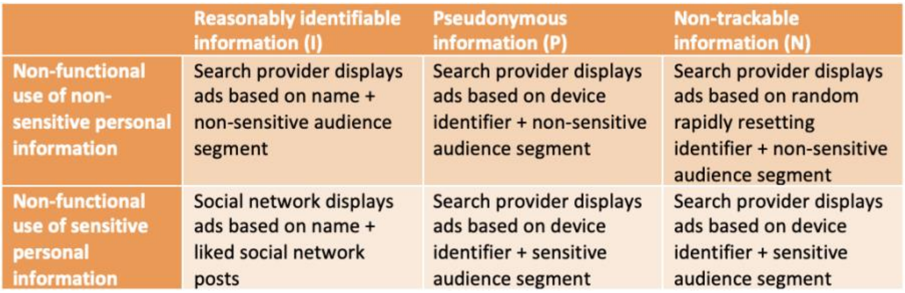
Table 4. Examples of Functional Uses of Various Types of Personal Information

Consider a movie app that provides personalized recommendations. In order to determine recommendations, suppose the app observes the title of a movie that a user has watched, uses the observation to place the user into non-sensitive audience segments (e.g., likes historical dramas), and then immediately discards each movie title. If the app pairs the non-sensitive audience segments with the user's name, then the combination of the user's name and non-sensitive audience segments constitutes non-sensitive reasonably identifiable information. Alternatively, if the app assigns the user a pseudonym, the app pairs the non-sensitive audience segments with the pseudonym, then the combination of the pseudonym and non-sensitive audience segments constitutes non-sensitive pseudonymous information. Finally, if the app assigns the user a random rapidly identifier, then the combination of the random rapidly resetting identifier and non-sensitive audience segment constitutes non-sensitive non-trackable information.

Next, consider a map app that provides turn-by-turn directions. In order to determine directions, suppose the app collects the precise geo-location of the user. If the app pairs the precise geo-location with the user's name, then the combination constitutes sensitive reasonably identifiable information. Alternatively, if the app assigns the user a pseudonym, then the combination of the pseudonym and precise geo-location constitutes sensitive pseudonymous information. Finally, if the app assigns the user a random rapidly resetting identifier and collects only the current geo-location of the user (but not the location history), then the combination of the random rapidly resetting identifier and current precise geo-location constitutes sensitive non-trackable information.

B. Non-Functional Use

Some uses of private person information do not enable functions or features of a service or app, but are used to subsidize the service or app. Table 5 presents some examples.



	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Non-functional use of non-sensitive personal information	Search provider displays ads based on name + non-sensitive audience segment	Search provider displays ads based on device identifier + non-sensitive audience segment	Search provider displays ads based on random rapidly resetting identifier + non-sensitive audience segment
Non-functional use of sensitive personal information	Social network displays ads based on name + liked social network posts	Search provider displays ads based on device identifier + sensitive audience segment	Search provider displays ads based on device identifier + sensitive audience segment

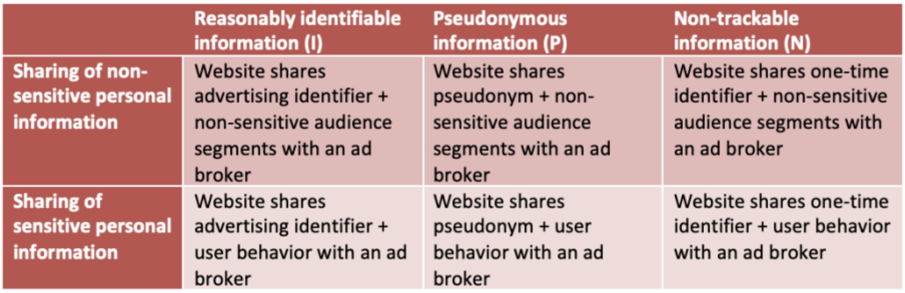
Table 5. Examples of Non-Functional Uses of Various Types of Personal Information

Consider a search provider that displays personalized ads aside search results. In order to determine which ads to display, suppose the search provider uses the search terms to place the user into non-sensitive audience segments (e.g., interested in tennis), and then immediately discards the search terms. If the search provider pairs the non-sensitive audience segments with the user's name, then the combination of the user's name and non-sensitive audience segments constitutes *non-sensitive reasonably identifiable* *information*. Alternatively, if the search provider pairs the non-sensitive audience segments with a device identifier, then the combination of the device identifier and non-sensitive audience segments constitutes *non-sensitive pseudonymous information*. Finally, if the search provider assigns the user a random rapidly identifier, then the combination of the random rapidly resetting identifier and non-sensitive audience segment constitutes *non-sensitive non-trackable information*. However, none of these uses are functional; the functional use is limited to displaying the search results, not the ads.

Similarly, consider a social network provider that displays personalized ads aside social network activity. In order to determine which ads to display, suppose the social network provider stores and analyzes a list of social network posts that the user has liked. Because this information constitutes app usage history, it is properly classified as *sensitive personal information*. If the social network provider pairs the list of social network posts that the user has liked with the user's name, then the combination constitutes *sensitive reasonably identifiable information*. This use is non-functional; the functional use is limited to displaying the social network posts, not the ads.

C. Sharing

In addition to using personal information, service or app providers may also share personal information. Table 6 presents some examples.



	Reasonably identifiable information (I)	Pseudonymous information (P)	Non-trackable information (N)
Sharing of non-sensitive personal information	Website shares advertising identifier + non-sensitive audience segments with an ad broker	Website shares pseudonym + non-sensitive audience segments with an ad broker	Website shares one-time identifier + non-sensitive audience segments with an ad broker
Sharing of sensitive personal information	Website shares advertising identifier + user behavior with an ad broker	Website shares pseudonym + user behavior with an ad broker	Website shares one-time identifier + user behavior with an ad broker

Table 6. Examples of Sharing of Various Types of Personal Information

Consider a website that wishes to display ads on one of its webpages. In order to determine which ads to display, suppose the website collects information about user interests, and places the user into non-sensitive audience segments. If the search provider discloses to an ad broker the non-sensitive audience segments paired with a user's advertising identifier, and does not limit how the ad broker uses this information, then the combination of the advertising identifier and non-sensitive audience segments constitutes *non-sensitive reasonably identifiable information*. The information is reasonably identifiable because the user corresponding to the advertising identifier is reasonably identifiable due to the lack of limitations on the ad broker's use of the information.

However, if the website discloses to an ad broker the same information pursuant to a written contract that prohibits the ad broker from identifying the person to whom the information relates, then the information constitutes *pseudonymous information*.

Finally, consider the case in which the website discloses to an ad broker the non-sensitive audience segments paired with a one-time identifier, pursuant to a contract that ensures that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the one-time identifier relates. Then the combination of the one-time identifier and non-sensitive audience segment constitutes *non-trackable information*.

V. PROPOSED CHOICE FRAMEWORK

There are two problems with the policy choices made in the GDPR and the CCPA. First, neither use both opt-in consent and opt-out choice.[122] The GDPR allows functional use of non-sensitive personal data to be mandated as part of the terms and conditions of service, but then jumps all the way up to opt-in consent for all other uses and for sharing.[123] The CCPA requires that users be given an opt-out choice from non-functional use of sensitive personal information and from all sharing, but never requires opt-in consent, even for sharing of sensitive personal information.[124] A superior public policy can be achieved by using opt-out choice for some types of processing and opt-in consent for others.

Second, neither the GDPR nor the CCPA differentiate between *non-trackable information*, *pseudonymous information*, and *reasonably identifiable information*.[125] By failing to differentiate, neither the GDPR nor the CCPA provide much incentive for a business to use less identifiable forms of personal information.

If *pseudonymous information* were differentiated from *reasonably identifiable information*, then there would be an incentive to pair personal information with pseudonyms rather than with names, and hence prevent the person or household relating to the personal information from being identified.

Similarly, if *non-trackable information* were differentiated from *pseudonymous information*, then there may be an incentive to pair personal information with one-time identifiers, and hence prevent tracking. Instead, both the GDPR and the CCPA attempt to reduce profiling in other ways. Both require specific disclosure relating to profiling. However, these disclosures don't translate into the availability of different user choices.

Use of the full range of options would also enable policy to match the full range of user perceptions of the risk associated with different uses of personal information. Sensitive personal information should be accorded higher protections that non-sensitive personal information. More identifiable forms of personal information should be accorded higher protections that less

[122] *See supra* Part II.
[123] *See supra* Part II.
[124] *See supra* Part II.
[125] *See supra* Part III.

identifiable forms. In addition, consumers associate a higher risk when their personal information is widely shared among the data ecosystem than when it is held only by the entity with which the consumer is interacting.

This section develops a choice framework. Statutory text to implement this framework is presented in Part VIII.

A. Functional Use

Functional use is a good starting point. Both the GDPR and the CCPA agree that functional use of non-sensitive personal information can be mandated in the terms and conditions of a service. This makes sense. There is a natural tradeoff here. A user must agree to the use of personal information that is technically required to provide the functionality of the service or app. The tradeoff is direct: use of information in exchange for functionality.

However, while the CCPA applies this same logic to functional use of sensitive personal information, the GDPR requires opt-in consent.[126] This makes little sense. If the sensitive personal information is technically required to provide the functionality, the choice remains the same; either agree to use of the personal information or don't use the function. All that requiring opt-in consent does is move the prompt to make the decision from the time at which the service or app is used to the time at which the functionality is used. A business should be allowed to mandate the functional use of both sensitive and non-sensitive personal information in the terms and conditions of a service.

B. Non-Functional Use

Next consider non-functional use (but not sharing) of non-sensitive personal information. Since the use is not functional, it is likely that the purpose of the use is to subsidize the service or app. The CCPA allows non-functional use to be mandated, while the GDPR requires opt-in consent.[127] This is exactly where there should be a distinction based on the level of identifiability. If a consumer privacy law requires that a user be given an opt-out choice for the non-functional use of *reasonably identifiable information*, but not for less identifiable forms, then businesses will be incentivized to prevent the person or household relating to the personal information from being identified.

Next to consider is non-functional use (but not sharing) of sensitive personal information. The CCPA requires that a user be given an opt-out choice, while the GDPR requires opt-in consent.[128] If a consumer privacy law requires opt-in consent for the non-functional use of *sensitive reasonably identifiable information*, but only that users be given an opt-out choice for the non-functional use of *sensitive pseudonymous information*, then businesses will be strongly incentivized to prevent the identification of the person or

[126] Jordan, *supra* note 3, at 33-35.

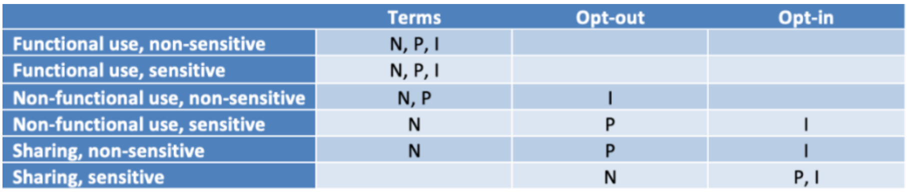
[127] *Id.* at 30-32.

[128] *Id.* at 33-35.

household to whom sensitive personal information is related. In addition, if a consumer privacy law requires that users be given an opt-out choice for the non-functional use of *sensitive pseudonymous information*, but not for *sensitive non-trackable information*, then businesses will be incentivized to not track people using sensitive personal information.

C. Sharing

Finally, consider the sharing of personal information. The CCPA requires that users be given an opt-out choice, while the GDPR requires opt-in consent.[129] Neither differentiates between non-sensitive and sensitive personal information.[130] Again, there is a superior option in which opt-in consent is required for more identifiable forms of personal information and for more sensitive information. Specifically, opt-in consent should be required for the sharing of both non-sensitive and sensitive *reasonably identifiable information*, and for the sharing of *sensitive pseudonymous information*. In addition, users should be given an opt-out choice from the sharing of all other forms of *reasonably linkable information*.



	Terms	Opt-out	Opt-in
Functional use, non-sensitive	N, P, I		
Functional use, sensitive	N, P, I		
Non-functional use, non-sensitive	N, P	I	
Non-functional use, sensitive	N	P	I
Sharing, non-sensitive	N	P	I
Sharing, sensitive		N	P, I

Table 7. Proposed User Choice in a Market with Effective Competition

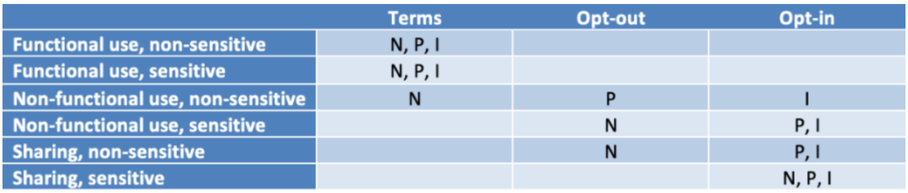
The resulting choice framework is summarized in Table 7, where N denotes non-trackable information, P denotes pseudonymous information, and I denotes reasonably identifiable information. Comparing this framework to the GDPR and the CCPA frameworks in Tables 1 and 2, the full range of options are now used. More identifiable forms of personal information are accorded greater protection, thus incentivizing good privacy practices. Non-functional use faces stronger forms of user consent than functional uses and sharing faces yet stronger forms of user consent. Use and sharing of sensitive personal information often requires a stronger form of user consent than does use and sharing of non-sensitive personal information. Finally, in the cases in which GDPR and the CCPA disagree, this proposal often chooses an intermediate option.

There is one last policy issue that should be addressed here. There are some uses of personal information that merit higher thresholds than those proposed in Table 7. First, personal information that takes the form of communications has traditionally been afforded higher privacy protections. Section 705 of the Communications Act prohibits a communications provider from divulging the "existence, contents, substance, purport, effort, or meaning" of communications, except for functional purposes or with

[129] *Id.* at 31-32.
[130] *Id.* at 33-35.

consent.[131] Second, in situations in which consumers have few choices for a provider of a particular service, competition between businesses based on their privacy policies is less likely. For example, in many geographical regions in the United States, there is only a single Internet Service Provider that offers broadband service with speeds that are acceptable to many consumers. In this case, the choice framework should reflect the lack of impact of competition upon privacy.

In either of these situations, while it still makes sense to allow such a business to mandate functional use in the terms and conditions of a service, when a business wishes to use personal information for non-functional purposes, or wishes to share personal information, the choice framework should further incentive the use of less identifiable forms of information. This can be accomplished by moving each type of personal information up one notch, e.g., from mandated to opt-out or from opt-out to opt-in. The resulting choice framework for communications providers or in a market without effective competition is illustrated in Table 8.



	Terms	Opt-out	Opt-in
Functional use, non-sensitive	N, P, I		
Functional use, sensitive	N, P, I		
Non-functional use, non-sensitive	N	P	I
Non-functional use, sensitive		N	P, I
Sharing, non-sensitive		N	P, I
Sharing, sensitive			N, P, I

Table 8. Proposed User Choice in a Market Without Effective Competition and for Communications Services

VI. EMPOWERING CONSUMERS WHO DESIRE PRIVACY-PRESERVING ADVERTISING

This section investigates how advertising can be implemented using different types of personal information. The goal is to understand if and how differentiating between different types of personal information may affect consumers.

This section of the article gives examples of advertising based on reasonably identifiable information, pseudonymous information, and non-trackable information. In each example, the following entities are considered:

- An ad venue, an entity which offers a venue in which ads appear, e.g., a website with ads on its webpages.
- An advertiser, an entity which offers ads to be published in ad venues, e.g., a business advertising a product.
- An ad broker, an entity which determines the ad venues on which a particular ad will appear, e.g., a business that contracts with both ad venues and advertisers and that determines the placement of each ad.

The examples do not address other businesses that are part of the ecosystem. They presume that the advertiser and the ad broker have a contract

[131] 47 U.S.C. § 605(a).

under which the advertiser pays the ad broker to place an ad, and that the ad broker and the ad venue have a contract under which the ad broker pays the ad venue to have the ad appear. The examples presume that none of the entities have market power.

They also distinguish between the acts of "placing" and "publishing" an ad. *Placing* an ad is the function of determining the ad venues on which an ad appears; the examples assume this is done by the ad broker. *Publishing* an ad is the technological function of causing the ad to appear; the examples assume this may be done by any of the parties.

Both the GDPR and the CCPA distinguish between entities that make decisions about the collection, use, and sharing of personal information versus entities that are hired to implement specific tasks involving the collection and use of personal information.[132] The GDPR calls the former *controllers* and the latter *processors*.[133] The CCPA calls the former *businesses* and the latter *service providers* or *contractors*.[134] This article uses the term *controller* to describe the entity that makes decisions about collection, use, and sharing. When a controller shares personal information with a third party, this article calls that third party a *contractor* if and only if there is a contract between the controller and the third party under which the third party uses that personal information only for the purposes specified by the controller. These terms are defined, and the contractual terms are discussed in Part VIII.

For each advertising example, the types of personal information collected and used by each party, and the types disclosed or shared between parties, are considered. How the information may be classified is discussed. Whether each entity might be a controller or a contractor is also considered. Finally, the impact of the proposed user choice framework is discussed.

This section starts with a privacy-invasive example that is commonplace today, and then works through a sequence of increasingly less privacy-invasive examples.

A. *Using Reasonably Identifiable Information for Behavioral Ads Published by an Ad Broker*

First, this article considers the use of reasonably identifiable information to place behavioral ads. In this example, the advertiser chooses to advertise based on the behavior of people in the desired audience. *Behavioral advertising* can describe this form.

Imagine that SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who are interested in luxury automobiles based on detailed profiles of these people. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that have detailed profiles of their website visitors.

[132] Jordan, *supra* note 3, at 15-16.

[133] *Id.*

[134] *Id.*

When a person visits CarReviews.com, the website collects the person's email address and advertising identifier, and looks up a profile that was previously compiled based on the person's activity on the website. CarReviews.com shares the person's IP address, advertising identifier, and profile with AbcAdBroker.com, which shares this information with advertisers, and auctions off the ad. SmithLuxuryCars.com wins the auction, and AbcAdBroker.com tells CarReviews.com to redirect the website visitor to SmithLuxuryCars.com to obtain the ad. The ad is thus seen only be people whose profiles demonstrate that they are interested in luxury automobiles.

The collection, use, and sharing of personal information is shown in Figure 1. The combination of the person's IP address, email address, advertising identifier, and profile is *reasonably identifiable information*. The information shared with the ad broker and the advertiser remain *reasonably identifiable information*, presuming that the contracts between the ad venue, ad broker, and advertiser do not prohibit the ad broker or the advertiser from using the IP address and advertising identifier to identify the person. Furthermore, since the profile contains web browsing history, the information is *sensitive*.

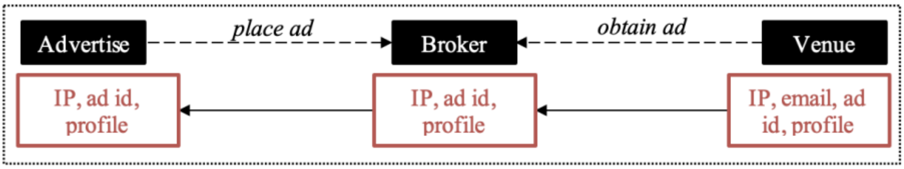


Figure 1. Behavioral Ads

The ad venue is a controller, since it determines the purposes and means of its collection and use of personal information. The ad broker and advertiser are also controllers, since neither is limited to using the information shared with it solely for the purposes of placing the ad.

The ad venue is using and sharing sensitive reasonably identifiable information. Under the proposed user choice framework, it would need to first obtain opt-in consent from the website visitor for this non-functional use and for sharing. If it does so, it would presumably pass this consent on to the ad broker for it to use and share this information, which would presumably pass this consent on to the advertiser to use this information.

This type of advertising is common, but privacy-invasive since it uses the most identifiable form of information. The proposed user choice framework thus places a high threshold on behavioral advertising. Because the information is both sensitive and reasonably identifiable, opt-in consent is required.

B. *Using Pseudonymous Information for Audience Segment Ads with Tracking*

Next, consider the use of pseudonymous information to place audience segment ads. In this example, the advertiser chooses to advertise to people who fall into specified audience segments based on prior tracking of these people.

For example, SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who fall into a luxury automobile audience segment, based on prior tracking. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that can determine if its website visitors fall into the luxury automobile audience segment.

When a person visits CarReviews.com, the website collects the person's advertising identifier, and looks up a profile that was previously compiled based on the person's activity on the website. However, instead of sharing the person's profile with AbcAdBroker.com, CarReviews.com selects audience segments based on the profile, and only shares the person's IP address, advertising identifier, and audience segments. AbcAdBroker.com awards the ad to SmithLuxuryCars.com, who is the advertiser willing to pay the most to place an ad to a person in the luxury automobile audience segment. AbcAdBroker.com tells CarReviews.com to redirect the website visitor to AbcAdBroker.com to obtain the ad. AbcAdBroker.com generates summary statistics about its ad placements for SmithLuxuryCars.com, but it does not share information about the individual people who saw the ad.

The collection, use, and sharing of personal information is shown in Figure 2. Since a consumer may be reasonably identified using the consumer's IP address, the combination of the person's IP address, advertising identifier, and profile is *reasonably identifiable information* if there are no legal controls preventing this identification. However, if the legal controls proposed in Part VIII are in place, then the personal information is *sensitive pseudonymous information*, and all entities using and sharing this information would commit to maintaining in a pseudonymous form. In addition, when the ad venue converts the profile information into audience segments, the information is transformed from *sensitive* to *non-sensitive* (shown as a dashed rectangle in the figure), and thus the combination of the person's IP address, advertising identifier, and audience segments shared with the ad broker are *non-sensitive pseudonymous information*, if the contract between the ad broker and the ad venue commits the ad broker to implement the corresponding legal controls (including not re-identifying the person) and to maintain the information in *non-sensitive* form. The advertiser only receives summary statistics, which qualify as *anonymous information*.

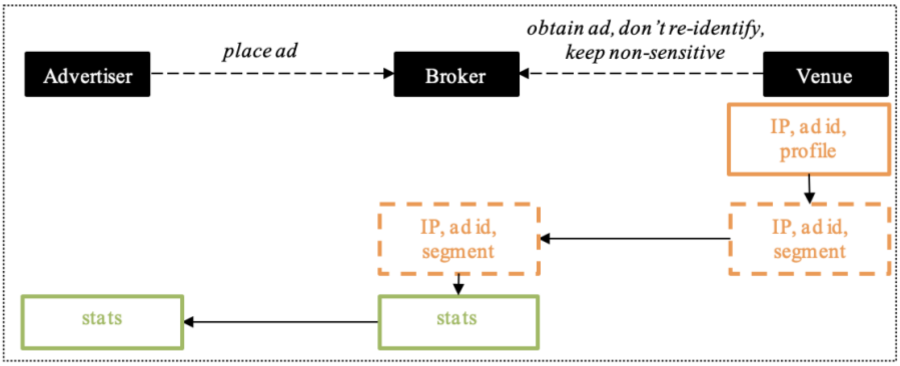


Figure 2. Audience Segment Ads with Tracking

As in the previous example, all three entities are *controllers*. The ad venue is using *sensitive pseudonymous information*. Under the proposed user choice framework, it would need to give the website visitor the ability to opt-out of this non-functional use. The ad venue is also sharing *non-sensitive pseudonymous information* with the ad broker, and it must separately give the website visitor the ability to opt-out of this sharing. The ad broker's non-functional use of *non-sensitive pseudonymous information* does not require an opt-out choice, but the website visitor can prohibit that use by simply opting out from the ad venue's sharing of that information. Finally, the advertiser only collects *anonymous information*, which is exempt from choice requirements.

The proposed user choice framework thus places a moderate threshold on audience segment ads with tracking. Because the information used by the ad venue is sensitive but pseudonymous, an opt-out choice is required for this use. Because the information shared by the ad venue is also pseudonymous but non-sensitive, an opt-out choice is also required for this sharing. The threshold is lower than on behavioral ads, which required opt-in consent. This lower threshold incentivizes the use of pseudonymous information instead of readily identifiable information, allowing consumers to remain pseudonymous.

C. Audience Segment Ads Without Tracking

The advertiser chooses to advertise to people who fall into specified audience segments, based solely on the current interaction with these people.

For example, SmithLuxuryCars.com wishes to advertise to people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads that will be seen only by people who fall into a luxury automobile audience segment, based solely on the current interaction with these people. AbcAdBroker.com contracts with websites (including CarReviews.com) that are often visited by people who are interested in luxury automobiles and that can determine if its website visitors fall into the luxury automobile audience segment based on the current website visit.

When a person visits CarReviews.com, the website collects the person's advertising identifier, and determines audience segments, based on the current website visit only. It generates a one-time identifier, and shares that one-time identifier and audience segments with AbcAdBroker.com, who awards the ad to SmithLuxuryCars.com, the advertiser willing to pay the most to place an ad to a person in the luxury automobile audience segment. AbcAdBroker.com tells CarReviews.com to publish SmithLuxuryCars.com's ad. AbcAdBroker.com generates summary statistics about its ad placements for SmithLuxuryCars.com, but it does not share information about the individual people who saw the ad.

The collection, use, and sharing of personal information is shown in Figure 3. The combination of the person's IP address, advertising identifier, and profile is sensitive pseudonymous information, if the ad venue implements the corresponding legal controls discussed in Part VIII (including not re-identifying the person). However, when the ad venue converts the profile information into audience segments and pairs it with a one-time identifier instead of an IP address, the information is transformed from sensitive to non-sensitive and from trackable to non-trackable. Thus, the combination of the one-time identifier and audience segments shared with the ad broker are non-sensitive non-trackable information, if the contract between the ad broker and the ad venue commits the ad broker to implement the corresponding legal controls (including maintaining the information in non-trackable form). The advertiser only receives summary statistics, which qualify as anonymous information.

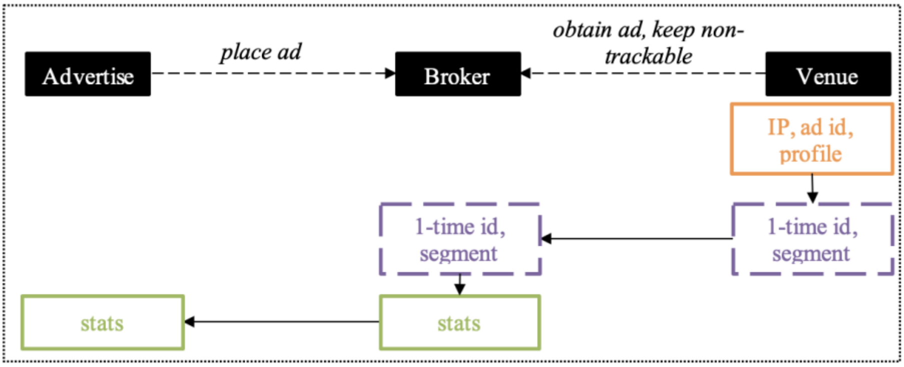


Figure 3. Audience Segment Ads Without Tracking

As in the previous examples, all three entities are controllers. As in the example with tracking, the ad venue is using sensitive pseudonymous information, and this it would need to give the website visitor the ability to opt-out of this non-functional use. However, the ad venue is only sharing non-sensitive non-trackable information with the ad broker, and under the proposed user choice framework it does not need to give the website visitor a separate opt-out choice from this sharing.

There is an alternative advertising model that results in similar consequences, but which allows the ad broker to publish the ad. Suppose the ad broker commits to acting as a contractor for the ad venue, by processing the shared information solely for the purposes of obtaining ads for the venue. Then the ad venue may share IP addresses with the ad broker instead of one-time identifiers, and the ad venue can publish the ad instead of asking the ad venue to do so. In this situation, because the ad broker is acting as a contractor, the ad venue similarly needs to give the website visitor the ability to opt-out of this non-functional use.

The proposed user choice framework thus places a low threshold on audience segment ads without tracking. Because the information used by the ad venue is sensitive but pseudonymous, an opt-out choice is required for this use. However, because the information shared by the ad venue is both non-sensitive and non-trackable, no additional choice is required for this sharing. The threshold is lower than on ads with audience segment ads with tracking, which required an opt-out choice from both use and sharing. This lower threshold incentivizes the use of one-time identifiers and thereby reduces tracking.

D. Contextual Ads

An advertiser advertises basely solely on characteristics of the ad venue. This article uses the term contextual advertising to describe this form.

For example, SmithLuxuryCars.com wishes to advertise on websites that are frequently viewed by people who are interested in luxury automobiles. SmithLuxuryCars.com purchases a service from AbcAdBroker.com to place ads on such websites. AbcAdBroker.com contracts with websites (including CarReviews.com) that provide summary statistics to show that they are often visited by people who are interested in luxury automobiles.

When people visit CarReviews.com, the website keeps track of the types of automobiles they are interested in, but it does not store any identifiers of its website visitors. In addition, it generalizes this information. Based on the generalized information, CarReviews.com generates summary statistics, including the percentage of its website visitors who are interested in luxury automobiles. It shares these statistics with AbcAdBroker.com, which auctions ads based on these statistics, and SmithLuxuryCars.com wins the auction. AbcAdBroker.com tells CarReviews.com to publish SmithLuxuryCars.com's ad.

The collection, use, and sharing of personal information is shown in Figure 4. The generalized information used by the ad venue may qualify as non-sensitive de-identified information if the ad venue implements the corresponding legal controls (including maintaining the information in de-identified form). The ad broker and the advertiser only receive summary statistics, which qualify as anonymous information.

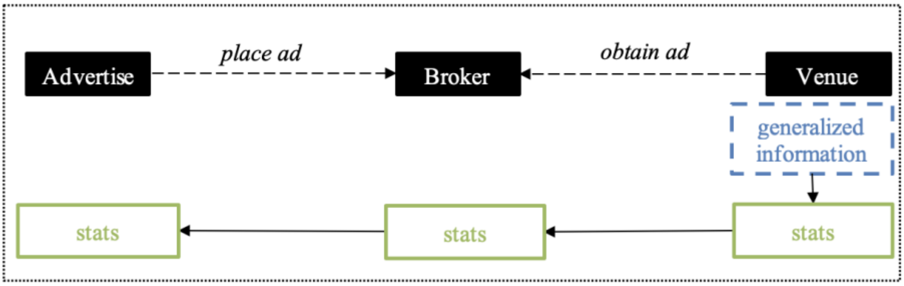


Figure 4. Contextual Ads

As in the previous examples, all three entities are *controllers*. However, the ad venue only uses *non-sensitive de-identified information*, and thus under the proposed user choice framework can require this use in its terms and conditions.

The proposed user choice framework thus places no threshold on contextual advertising. The threshold is lower than on ads with audience segment ads without tracking, which required an opt-out choice. This lower threshold incentivizes contextual advertising over audience segment ads.

VII. Proposed Notice Requirements

In this section, transparency regarding collection, use, and sharing of personal information is considered. One of the goals of transparency is to allow consumers and privacy experts to understand collection, use, and sharing. Another goal of transparency is to empower consumers to make choices.

A. Types of Notice

The GDPR and the CCPA both require transparency, but they require different types of notices at different points in time.[135]

The GDPR requires notices from controllers, but not from processors, about processing of personal data, which includes collection, use, and sharing.[136] The content of required notices is considered in the following subsections. When a controller obtains personal data directly from the individual whom the personal data concerns, the GDPR requires that the notice be given "at the time when personal data are obtained."[137] If the personal data was not obtained directly from the individual whom the personal data concerns, but instead from an intermediary, then the GDPR requires a controller to provide notice to the person "within a reasonable period after obtaining the personal data, but at the latest within one month."[138] When personal data is shared, the GDPR requires that the corresponding

[135] Jordan, *supra* note 3, at 16-25.

[136] *Id.*

[137] GDPR, *supra* note 1, at art. 13(1).

[138] *Id.* at art. 14(3)(a).

notice be given "when the personal data are first disclosed to the recipient."[139] The GDPR doesn't specify whether these notices must be public (e.g., in a publicly accessible privacy policy) and/or must be given directly to the person concerned, other than to say that the notices must be in an "easily accessible form." [140] The GDPR requires that notices from controllers include information about processing by the controller's processors.[141]

The CCPA similarly requires notices from businesses, but not from service providers or contractors, about collection, use, and sharing of personal information.[142] Unlike the GDPR, the CCPA does not distinguish between businesses that collect personal information directly from the individual whom the information concerns and those that collect personal information from an intermediary, and the CCPA does not have a separate requirement for notice to be provided at the point of sharing of personal information.[143] However, unlike the GDPR, the CCPA specifies that notices must be provided both in "its online privacy policy … or its internet website"[144] and "at or before the point of collection."[145] Similar to the GDPR, the CCPA requires that notices from businesses include information about collection, use, and sharing by the business's service providers and contractors.[146]

In addition to notices about collection, use, and sharing of personal information, both the GDPR and the CCPA require notices about user rights of access, correction, deletion, and consent.[147] However, these additional notices are outside the scope of this article.

B. Contents of Notices About Collection and Use

Most privacy policies today give separate disconnected disclosures about a business's collection of personal information, its use of personal information, and its sharing of personal information. However, collection and use are tightly connected, and notices about collection and use should be combined so that consumers may understand how each category of personal information is used. In contrast, sharing is conceptually distinct, and notices about sharing should be distinct. This approach also supports the choice framework proposed in Part V, which similarly treats use and sharing differently. Notices about collection and use are discussed in this subsection and notice about sharing is discussed in the following subsection.

[139] *Id.* at art. 14(3)(c).

[140] *Id.* at art. 13(1). Also *see id.* at recital 58, which envisions that notice may be "addressed to the public or to the data subject."

[141] *Id.* at art. 28(3)(e).

[142] Jordan, *supra* note 3, at 16-25.

[143] *Id.*

[144] CAL. CIV. CODE §1798.130(a)(5) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[145] *Id.* § 1798.100(a).

[146] *Id.* § 1798.130(a)(3)(A).

[147] GDPR, *supra* note 1, at arts. 13(2)(b), 14(2)(c); CAL. CIV. CODE § 1798.130(a)(5)(A).

1. Categories of Personal Information

The CCPA requires that privacy policies include "the categories of personal information it *has collected* about consumers in the preceding twelve months,"[148] and that notices provided at or before the point of collection include "[t]he categories of personal information *to be collected*."[149] The CCPA also specifically requires that the categories of personal information include "the categories of sensitive personal information."[150] The GDPR has a similar requirement that notices include "the categories of personal data" the controller has collected.[151]

Notice of the categories of personal information collected is beneficial, but the disclosed categories are sometimes too broad to provide information sufficient for consumers to understand what personal information is collected. For example, while some privacy policies disclose that they collect the IP address and/or the IMEI of the device that a consumer is using,[152] other privacy policies merely disclose that they collect unspecified "device identifiers."[153] Similarly, while some privacy policies disclose that they collect the Apple and Android advertising identifiers,[154] other privacy policies merely disclose that they collect unspecified "[a]dvertising [identifiers]."[155]

Regarding the level of detail or granularity of these categories, the CCPA requires that they use "the specific terms set forth" in the definitions of personal information and sensitive personal information.[156] The CCPA regulations require that they be described "in a manner that provides consumers a meaningful understanding of the information being collected."[157] This is a good start, but the information should not only provide a meaningful understanding, it should also be sufficient for consumers to act upon the information.

[148] CAL. CIV. CODE § 1798.130(a)(5)(B)(i) (emphasis added).

[149] *Id.* § 1798.100(a)(1) (emphasis added).

[150] *Id.* § 1798.100(a)(2).

[151] GDPR, *supra* note 1, at art. 14(1)(d). The GPDR is explicit about this requirement for personal data that is not obtained directly from the individual whom the personal data concerns. Inexplicably, it is unclear whether the GDPR has a similar notice requirement when personal data is obtained directly from the individual; note the omission of such a requirement in GDPR, art. 13, as compared to its inclusion in art. 14(1)(d).

[152] *See, e.g.*, *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US (last updated July 1, 2021) (under "Unique identifiers") [https://perma.cc/L4AT-TSVF].

[153] *See, e.g.*, *AT&T Privacy Policy*, AT&T, https://about.att.com/csr/home/privacy/full_privacy_policy.html (last updated Nov. 1, 2021) (under "The information we collect") [https://perma.cc/ZC34-JQJ8].

[154] *See, e.g.*, *Privacy Policy*, THE WEATHER CO., https://weather.com/en-US/twc/privacy-policy (last updated Oct. 21, 2021) (under "Use of Advertising Identifiers") [https://perma.cc/R9UN-ZJM9].

[155] *See, e.g.*, *Privacy Policy*, KAYAK, https://kayak.com/privacy (last updated July 1, 2021) (under "What are Cookies?") [https://perma.cc/SSM7-W36A].

[156] CAL. CIV. CODE § 1798.130(c) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[157] California Consumer Privacy Act Regulations, CAL. CODE REGS. tit. 11, §§ 999.300, .305(b)(1), .308(c)(1)(d) (2020) [hereinafter CCPA Regulations].

An important policy question is which type of personal information should be subject to disclosures about collection, use, and sharing. The GDPR requires disclosure about all personal data, which includes de-identified information but not anonymous information. [158] The CCPA requires disclosure about all personal information, which excludes both de-identified information and anonymous information.[159] However, neither de-identified information nor anonymous information should be subject to the proposed choice framework, as neither presents significant privacy risks. However, it is important to understand the collection, use, and sharing of both types of personal information in order to ensure that the personal information satisfies the characteristics required to be classified as de-identified information or anonymous information. Thus, notices about collection, use, and sharing should be applied not only to reasonably linkable information but to all personal information. A consumer privacy law should thus require:

> A controller shall maintain a publicly accessible privacy policy. The privacy policy shall disclose accurate information regarding the controller's collection, use, and sharing of personal information sufficient for consumers to make informed choices regarding the use of the controller's services.[160]

Notice of the categories of personal information collected is also insufficient to provide consumers with the information necessary to understand the degree of identifiability of the personal information collected and used. As will be discussed in Part VIII, privacy policies often assert that personal information is non-personal, that linkable information is anonymous, that reasonably linkable information is de-identified, that information including a resettable identifier is not trackable, that information including a device identifier is not identifiable, and that only information including a direct identifier is identifiable. More generally, consumers are rarely provided with notices that accurately explain whether personal information that is collected is anonymous, de-identified, trackable, or reasonably identifiable.

Clear definitions of each type of personal information can help. However, the corresponding information about the classification of each category of personal information collected and used should also be included in notices about collection and use. A consumer privacy law should thus require:

[158] Jordan, *supra* note 3, at 13.

[159] *Id.*

[160] This language is modeled on the FCC's net neutrality transparency rule; *see* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, at para. 9 (2015).

> The privacy policy shall disclose the categories of personal information collected and used, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

2. Method and/or Source of the Collection of Personal Information

The method and/or source of personal information is also important, both to understand the information collected and to track personal information through the ecosystem.

Unfortunately, neither the GDPR nor the CCPA require a business that collects personal information directly from a consumer disclose the *methods* by which it collects this personal information.[161] This lack of disclosure about methods of collection is often used by businesses to obscure details about what personal information is collected. For example, a business may simply disclose that it collects information about which websites a consumer visits but fail to disclose whether it collects this information by examining packet headers or by collecting DNS queries.[162] The latter information about the method used could have informed a consumer about whether adopting a different DNS provider would change the collection of personal information.

In contrast to their lack of requirements about disclosure of *methods*, both the GDPR and the CCPA do include some requirements about disclosure of *sources*. Under the GDPR, if a controller collects personal data from an intermediary, then the controller must disclose "from which source the personal data originate, and if applicable, whether it came from publicly accessible sources."[163] In contrast, the CCPA only requires that disclose, in its privacy policy, "[t]he categories of sources from which the personal information is collected."[164]

Notice of only the categories of sources does not permit a consumer to identify and act upon the entity that originally collected and shared the consumer's personal information. There is no reason for lack of disclosure of sources that outweighs a consumer's right to follow the flow of their personal information through the ecosystem and to act upon this information.

It is unclear whether the GDPR requires a controller to disclose, *for each category* of personal data collected, the source of that category of personal data. Separate disconnected disclosures of categories and of sources are insufficient. For example, consider a business that discloses that it collects both your address and your browsing history, and that separately discloses

[161] Jordan, *supra* note 3, at 18.

[162] *See, e.g.*, AT&T, *supra* note 153 (under "Web browsing and app information").

[163] GDPR, *supra* note 1, at art. 14(2)(d). However, if multiple sources have been used, the GDPR allows for the disclosure only of general information; see GDPR, recital 61.

[164] CAL. CIV. CODE § 1798.110(c)(2) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

that it collects personal information both directly from you and from your Internet Service Provider (ISP). These separate disclosures fail to indicate whether the business collects your browsing history from your ISP. A consumer privacy law should thus require:

> The privacy policy shall disclose, for each category of personal information collected: (a) the method of collection (if the personal information is collected by or on behalf of the controller) and (b) the sources of collection (if the personal information is shared with the controller by another entity).

3. Use of Personal Information

The GDPR requires that notices include "the purposes of the processing for which the personal data are intended."[165] The CCPA similarly requires a business to disclose "the purposes for which the categories of personal information are collected or used."[166]

However, it is unclear whether the GDPR or the CCPA requires a business to separately disclose, *for each category* of personal information collected, the purpose for collecting that category of personal information. Separate disconnected disclosures of categories and of purposes are insufficient. For example, consider a business that discloses that it collects the IP addresses of the websites you visit,[167] and that separately discloses that it collects personal information both to route your Internet traffic to the intended destination and for advertising.[168] These separate disclosures fail to indicate whether the business uses the IP addresses of the websites that you visited for advertising (i.e., behavioral advertising).[169]

A consumer must be able to understand the purpose for the collection of each category of personal information in order to meaningfully exercise the consumer's right to consent. A consumer privacy law should thus require:

[165] GDPR, *supra* note 1, at arts. 13(1)(c), 14(1)(c).

[166] CAL. CIV. CODE §§ 1798.100(a)(1), .110(c)(3).

[167] *See, e.g.*, *Our Privacy Policy Explained*, XFINITY, https://www.xfinity.com/privacy/policy (last updated Oct. 12, 2021) (under "The Personal Information We Collect and How We Collect It") (Comcast collects "Domain Name Server … searches and network traffic activity") [https://perma.cc/2ASV-UYJS].

[168] *See, e.g.*, *id.* (under "Collection and Use of Personal Information," then under "Learn more about your rights if you are a California resident and how to exercise them") (Comcast uses "[i]nferences drawn from other personal information" consisting of a "[p]rofile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" to "provide marketing and advertising").

[169] *See, e.g.*, *id.* (under "How and When We Use Information, Including for Marketing and Advertising") (Comcast asserts that "[w]here you go in the Internet is your business, not ours" and that Comcast has "never used [DNS] data for any sort of marketing or advertising").

> The privacy policy shall disclose, for each category of personal information collected or used, the purposes for which the category of personal information is collected or used.

In the proposed choice framework in Part V, user choice should be based in part on whether the personal information is collected for functional or for non-functional use.[170] In particular, non-functional use of reasonably identifiable information or of sensitive pseudonymous information should not be mandated in terms and conditions of a service. In order to exercise this choice, a consumer must be able to understand whether the use of a category of personal information will result in added functionality of the service or whether it will only result in non-functional uses such as advertising. A consumer privacy law should thus require:

> The privacy policy shall disclose, for each category of personal information collected or used and each such purpose, whether the use constitutes functional use, and if so, the functionality enabled by the collection and use of that category of personal information.

C. *Contents of Notices About Sharing*

Finally, this section turns to notices about sharing.

1. Categories of Personal Information Shared

The CCPA requires a business to disclose in its privacy policy a "list of the categories of personal information it has sold or shared about consumers in the preceding 12 months."[171] It also requires a business to disclose in its privacy policy a "list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months."[172] Surprisingly, it is unclear whether the GDPR has a similar requirement that a controller disclose the categories of personal data disclosed to third parties.

Regarding the level of detail or granularity of these categories, as with disclosure of collection and use, the CCPA requires that they "use the specific terms set forth" in the definitions of personal information and sensitive personal information.[173] However, disclosure of categories of personal information is insufficient to provide consumers with the information necessary to understand the degree of identifiability of the personal information shared. For example, some businesses appear to share the

[170] A statutory definition of *functional use* was proposed in Part V.B.

[171] CAL. CIV. CODE § 1798.130(a)(5)(C)(i) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[172] *Id.* § 1798.130(a)(5)(C)(ii).

[173] *Id.* § 1798.130(c).

combination of an advertising identifier and audience segments,[174] which might be classified as *pseudonymous information* if there are the corresponding legal controls in place. In contrast, other businesses appear to share the combination of an IP address and fine-grained user interests,[175] which are likely to be classified as *reasonably identifiable information*. For this reason, disclosure of the categories of personal information should be accompanied by the classification of each category:

> The privacy policy shall disclose the categories of personal information shared, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

2. Recipients of Personal Information

The GDPR requires controllers to disclose "the recipients or categories of recipients" to whom the personal data have been or will be disclosed. Somewhat similarly, the CCPA requires that privacy policies include the "categories of third parties to whom the business discloses consumers' personal information."[176] There are two issues here worth consideration: the granularity of the disclosure and the scope of the recipients that must be disclosed.

Regarding granularity, CCPA regulations define *categories of third parties* as "types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party," and give as examples "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."[177] However, CCPA regulations also interpret the CCPA as also requiring the disclosure in privacy policies of the "third parties to whom [each category of personal information] was . . . sold."[178]

It is well known that personal information is widely shared amongst a large number of businesses that comprise an advertising and tracking ecosystem. One of the most fundamental issues in privacy regulation is how

[174] *See, e.g.*, *Privacy Policy*, PINTEREST, https://policy.pinterest.com/en/privacy-policy (last updated July 1, 2021) (under "What we do with the info we collect") ("if you show an interest in camping tents on Pinterest, we may show you ads for other outdoor products") [https://perma.cc/K95L-W3QQ].

[175] *See, e.g.*, *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Jan. 4, 2022) (under "Apps, websites, and third-party integrations on or using our Products") ("when you … use a Facebook Comment or Share button on a website, … the website … can receive a comment or link that you share from the website on Facebook") [https://perma.cc/S8SZ-7UNE].

[176] CAL. CIV. CODE § 1798.130(a)(5)(B)(iv).

[177] CCPA Regulations, *supra* note 157, at § 999.301(e).

[178] *Id.* § 999.308(c)(1)(g)(1-2).

to address this widespread sharing. If a consumer wishes to track the path of their personal information through the advertising and tracking ecosystem, it would be useful to know both the recipients of their personal information from a particular business and also the source of their personal information from a downstream business. There is no reason for lack of disclosure of a list of recipients that outweighs a consumer's right to follow the flow of their personal information through the ecosystem and to act upon this information.

The second issue is the scope of the recipients that must be disclosed. The GDPR defines a *recipient* as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not."[179] It thus requires disclosure of sharing of personal data with processors. In contrast, the CCPA only requires disclosure of sharing of personal information with third parties, which excludes service providers and contractors.

There is a fundamental choice to be made here. One option is to require disclosure when sharing personal information with contractors; to not hold controllers responsible for disclosure of collection, use, and sharing by its contractors; and to require contractors to disclose their collection, use, and sharing of personal information. However, this option is burdensome on consumers, who must examine the privacy policies of both the controller and all of its contractors to understand what personal information is collected, how it is used, and with whom it is shared. A superior option is to hold controllers responsible for disclosure of collection, use, and sharing by its contractors. In this case, disclosure of sharing of personal information with contractors need not be required, and contractors need not be required to disclose their collection, use, and sharing of personal information. A consumer privacy law should thus require:

> The privacy policy shall disclose the third parties with which the controller shares personal information.

Notices about sharing of personal information are of limited use unless a consumer also understands why a business is sharing their personal information. The CCPA requires a business to disclose in its privacy policy "the business or commercial purpose for . . . selling personal information."[180] Similarly, the GDPR requires a controller to disclose "the purposes of the processing for which the personal data are intended," and it defines *processing* to include disclosure to third parties.

However, the usefulness of these mandated notices is determined in part by the amount of detail. For example, consider a business that discloses that it shares both your address and your browsing history, and that separately discloses that it shares personal information both for advertising and to improve insurance rate-setting. These separate disclosures fail to indicate whether the business shares your browsing history for advertising (i.e., behavioral advertising) or for insurance rate-setting (e.g., risk estimation).

[179] GDPR, *supra* note 1, at art. 4(9).

[180] CCPA Regulations, *supra* note 157, at § 999.308(c)(1)(f).

These two possibilities have very different consequences. For this reason, privacy policies should disclose the purpose for sharing each category of personal information.

The terms, if any, on which personal information is shared is also important. The definitions of several types of personal information (*de-identified information*, *non-trackable information*, and *pseudonymous information*) proposed in Part VIII include commitments to contractually obligate any third parties to whom the controller discloses the information to implement a set of legal controls that ensure that the information does not become more identifiable. These contractual obligations should be disclosed in a privacy policy whenever a controller shares personal information. A consumer privacy law should thus require:

> For each such third party, the privacy policy shall disclose the categories of personal information shared with that third party, the purposes for which the controller shares each category of personal information with that third party, and any contractual limits on the third party's use and further sharing of that personal information.

Finally, on the Internet it is common that as part of a consumer's interaction with a first party, the first party not only shares the IP address of the consumer with a third party but also enables the third party to directly collect further information from the consumer. In this case, a consumer has a right to know that, in addition to the first party sharing the consumer's information, that the first party is also enabling third parties to collect further information. A consumer privacy law should thus require:

> If a controller enables any third parties to collect additional personal information, the controller's privacy policy shall disclose the third parties so enabled and any contractual limits on such collection.

VIII. STATUTORY TEXT

Part VII presented proposed statutory text regarding notice. In this section, statutory text is developed to implement the choice framework proposed in Part V, as well as the supporting definitions.

A. Defining Personal Information and Reasonably Linkable Information

Notice and choice requirements typically apply only to information that is both personal and private. Privacy laws often call this type of information *personally identifiable information*, *personal information*, or *personal data*.

Many privacy policies lack any definition whatsoever of personally identifiable information. For example, Microsoft uses the term personal data, but does not define it.[181] Pinterest uses the term personal information, but does not define it.[182] Twitter interchangeably uses the terms personal information and personal data, but does not define either of them.[183] By omitting a definition of personally identifiable information, the scope of such privacy policies is unknown, and consumers may be left wondering what personally identifiable information is collected that the privacy policy fails to disclose.

The GDPR defines *personal data* as "any information relating to an identified or identifiable natural person."[184]

The CCPA defines *personal information* as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[185]

In these definitions, both the GDPR and the CCPA combine the concept of personal information (e.g., information relating to a person) with the concept of identifiability (e.g., an identified or identifiable person). However, by combining these two concepts into a single definition, both the GDPR and the CCPA fail to address information that is personal but whose degree of identifiability falls short of relating to an "identifiable natural person."

Because of this conflation of personal and identifiable, the CCPA then goes back and separately defines other types of information—including *publicly available* information, *aggregate consumer information*, and *de-identified information*—and proceeds to exclude each of these from personal information.[186] In addition, the CCPA defines *pseudonymization*, but fails to address the relationship of pseudonymized information to personal information or to de-identified information.[187]

The GDPR exhibits similar problems, but to a worse degree. The GDPR uses the terms *aggregate data* and *anonymous information*, both of which it excludes from personal data.[188] In contrast to the CCPA, which excludes publicly available information from personal information, the GDPR uses (but not define) the term *public sector information*, which it appears to include in personal data.[189] Finally, the GDPR defines the term *pseudonymisation,* and treats pseudonymized data as a subset of personal data, but it fails to apply any different notice and choice requirements to pseudonymized data than to other personal data.[190]

Because of these problems, the next three subsections separately address personal information (i.e., information relating to a person), private

[181] *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Dec. 2021) [https://perma.cc/3XYR-LQM8].

[182] PINTEREST, *supra* note 174.

[183] *Twitter Privacy Policy*, TWITTER, https://www.twitter.com/en/privacy (last updated Aug. 19, 2021) [https://perma.cc/B29R-CWT4].

[184] GDPR, *supra* note 1, at art. 4(1).

[185] CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[186] *Id.* § 1798.140(v).

[187] *Id.* § 1798.140(aa).

[188] GDPR, *supra* note 1, at recitals 26, 162.

[189] *Id.* recital 154.

[190] *Id.* recital 26.

information (i.e., information that is not public), and identifiable information (i.e., information relating to an identifiable person).

1. Is the Information Personal?

A consumer privacy bill is concerned with the privacy of people, not the privacy of organizations or businesses.

The GDPR limits personal data to "information relating to . . . [a] natural person."[191] The EU clarifies that a "natural person" means an individual, not a business, institution, or other entity.[192] The EU further clarifies that "relating to" means "information about a person" and that it includes not only "information pertaining to the private life of a person" but also "professional activities, as well as information about his or her public life."[193] As examples, the GDPR lists a "natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[194]

The CCPA's list of terms used in its definition of personal information similarly includes "information that . . . relates to [or] describes . . . a particular consumer."[195] It is unclear whether the CCPA's addition of the word "describes" broadens its definition, since it is unclear whether there is any information that "describes," but does not "relate to," a particular consumer.

A consumer privacy law should define personal information and should require that privacy policies adhere to this definition. Today, privacy policies often deny that much information relating to a person is actually personal. For example, Apple uses the term non-personal information to refer to "data in a form that does not, on its own, permit direct association with any specific individual."[196] Examples of non-personal information Apple collects and uses include occupation, location, and search queries.[197] However, the information is certainly personal, given that occupation, location, and search queries relate to a person.

Personal information should include, at a minimum, information which relates to an individual. However, there remains an important policy decision: should personal information also include information which relates to a household? Some identifiers used by services and apps to associate information identify a group of persons rather than a single person. Often, the group of persons constitutes a household. For example, a home postal address

[191] *Id.* at art. 4(1).

[192] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 83-86 (2018) [hereinafter EU HANDBOOK].

[193] *Id.* at 83, 86.

[194] GDPR, *supra* note 1, at art. 4(4).

[195] CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[196] *Privacy Policy*, APPLE, https://web.archive.org/web/20200101005603/https:/www.apple.com/legal/privacy/en-ww/ (last updated Dec. 31, 2019) (under "Collection and Use of Non-Personal Information").

[197] *Id.* (under "Collection and Use of Non-Personal Information").

or home telephone number may be associated with a household rather than with a single person.

However, privacy policies are often unclear about whether they consider information relating to a household to be included in the scope of personal information. Indeed, providers of services and apps often argue that they are not. For example, the California Chamber of Commerce, representing a wide variety of businesses, argued that information associated with households should be excluded from the CCPA's scope of personal information.[198]

The ambiguity of whether information relating to household is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a privacy law the role of information associated with a group of people such as a household, and the rights of individuals within such a group.

The GDPR seems to include information relating to households in its scope of personal data, since it states that the regulation "applies to controllers or processors which provide the means for processing personal data for such personal or household activities."[199] However, this should have been made clear.

The CCPA is more explicit. In its definition of personal information, it includes information that relates to either a consumer or a household.[200] A household is defined as a group of consumers who reside at the same address and share a common device or service. The CCPA exempts businesses from certain specified obligations insofar as they concern household data, but it is unclear whether these exemptions include notice and choice obligations.[201]

A consumer privacy law should be explicit that information relating to a household qualifies as personal information. First, information relating to a household is clearly information relating to one or more natural persons in the household. Second, a household identifier has traditionally been treated as identification of a natural person, even if it is not sufficient to pin down which person within the household. For example, a home postal address and a home phone number are both always considered to be personal identifiers. For this reason, personal information should include information which relates to either an individual or a household.[202]

[198] Letter from Tim Day & Harold Kim, Senior Vice President, Chamber Technology Engagement Ctr. & Chief Operating Officer, U.S. Chamber Inst. for Legal Reform, California Chamber of Com., to California Attorney Gen. Xavier Becerra, 4 (Mar. 8, 2019) (on file with California Chamber of Com.), https://www.uschamber.com/assets/documents/ca_ag_privacy_comments.pdf [https://perma.cc/G9JX-CJNR].

[199] GDPR, *supra* note 1, at recital 18.

[200] CAL. CIV. CODE § 1798.140(v)(1).

[201] *Id.* § 1798.145(p).

[202] However, there are peculiarities with other user rights, such as the right to inspect, when they concern household information.

2. Is the Information Private?

A consumer privacy bill should be concerned with the use of private information, not with the use of publicly available information.

The CCPA excludes from the scope of personal information any information that is publicly available. It defines *publicly available* information to include information in government records, information about a consumer that a consumer him or herself made publicly available, information about a consumer that the consumer disclosed to a third party "if the consumer has not restricted the information to a specific audience," and information about a consumer that was made publicly available by "widely distributed media."[203]

The GDPR does not provide any similar exclusion from personal data for any type of publicly available information. It recognizes the existence of *public sector information*, which it does not define, but which appears by reference to consist of personal data that is held by a State, regional or local authority, by a body governed by public law, or by associations of such bodies.[204] Thus, unlike the CCPA, such public sector information remains a subset of personal data. The GDPR places the same notice requirements on public sector information as on other personal data, but it exempts public sector information from GDPR's choice requirements if public access to this information is provided for by EU or State law.[205]

The GDPR and the CCPA thus disagree on their approach to publicly available information. An intermediate approach would be in the public interest. As provided in the CCPA, information that a consumer has made publicly available should not be subject to notice and choice requirements, since the consumer has already decided to waive control over this information. However, CCPA's exemption goes beyond this. It also classifies information that a consumer has disclosed to a third party as *publicly available* if the consumer failed to restrict the third party's sharing of that information to a specific audience. This creates a chicken-and-egg situation. A consumer may wish to restrict sharing of personal information, but might not be accorded such a choice unless given this right by a privacy law. For this reason, the definition of *publicly available information* should not include such information.

In addition, even with respect to information in government records that are publicly available, the GDPR applies notice requirements, while the CCPA does not. While a consumer may benefit from transparency about a business's use of such publicly available information, applying notice requirements to information that is already publicly available goes beyond the mandate of a consumer privacy law that should be focused on private information.

Personal information should thus be defined as:

[203] CAL. CIV. CODE § 1798.140(v)(2).

[204] GDPR, *supra* note 1, at recital 154.

[205] *Id.* at art. 86.

> The term "personal information" means any information relating to a natural person or to a household, excluding publicly available information.
> The term "publicly available information" means information relating to a natural person or to a household (a) in publicly available government records, (b) that the person or household to whom the personal information is related has made publicly available, or (c) that was made publicly available by widely distributed media.

Personal information is thus personal and private.

3. Is the Information Reasonably Linkable?

Having defined *personal information* as information that is both personal and private, this section now turns to the issue of whether it is identifiable information (i.e., information relating to an identifiable person).

There are several methods by which a person may be identifiable. The most obvious method is the use of person's name. The GDPR specifies that a natural person may be identified "by reference to an identifier such as a name . . . ."[206] The CCPA similarly specifies that a particular consumer may be identified using "a real name."[207] Other identifiers can also be used to reasonably establish a person's identity. For example, the CCPA specifies that a particular consumer may be identified using "a real name, . . . postal address, . . . email address, . . . social security number, driver's license number, [and a] passport number."[208] Thus, under both the GDPR and the CCPA, it is clear that a natural person may be identifiable through, at a minimum, a person's name, personal telephone number, personal email address, and government issued individual identifiers (e.g., driver's license number, social security number, or passport number).

Many privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person. For example, Apple defines personal information as "data that can be used to identify or contact a single person." [209] Cox defines personally identifiable information as "subscriber name, service and mailing addresses, telephone numbers, social security number, driver's license number, email address, billing and payment records (including credit card and bank account numbers used to pay for our services), subscriber credit information, or other information that potentially could be used to identify, contact, or locate you."[210] Chase uses the term

[206] *Id.* at art. 4(1).

[207] CAL. CIV. CODE § 1798.140(v)(1).

[208] *Id.*

[209] APPLE, *supra* note 196 (under "Collection and Use of Non-Personal Information").

[210] *Your Privacy Rights as a Cox Customer and Related Information*, COX https://www.cox.com/aboutus/policies/annual-privacy-notice.html (last updated Jan. 1, 2022) (under "Your Information") [https://perma.cc/QM8X-NS4F].

personal information to describe contact information but excludes "usage and other information."[211]

However, often it is not the identifier itself that is personal. It is the information *associated* with an identifier that is personal. For example, a person may have a public telephone number listing, and hence that person's name and telephone number are public. However, a person's name and telephone number are often associated with information about that person's Internet browsing history, and it is the browsing history that is personal. By omitting information associated with an identifier from the scope of personally identifiable information, consumers may be left wondering what personally identifiable information is collected that the privacy policy fails to disclose.

Other privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person and to information that the provider of that service or app links to that identifier. For example, Google defines personal information as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account."[212]

However, limiting the scope of reasonably linkable information to an identifier that itself identifies a person and to information that the provider of that service or app links to that identifier is severely underinclusive in two separate ways. Identifiers are often used that uniquely identify a person, but not by name, telephone number, or email address. For example, Google and Facebook assign their own identifiers to each person they profile. Such identifiers are then associated with personal information such as browsing history or social network posts. Cox considers contact information to be personally identifiable information, but considers "general location, demographics, . . . usage, . . . and preferences" to be non-personally identifiable information unless it is directly linked to personally identifiable information.[213] Such definitions open up the possibility that these providers consider browsing history, social network posts, or usage information to be *excluded* from the scope of personally identifiable information, if not paired with an identifier that itself identifies a person, and thus not subject to disclosure requirements.

Although such privacy policies often then proceed to list categories of information that the service or app collects that do not fall into the severely limited scope of personally identifiable information as the provider defines it, the exclusion of information related to a person undermines the credibility that the privacy policy's disclosures are comprehensive.

In contrast, some privacy policies use definitions of personally identifiable information that either match or borrow language from those in

[211] *Online Privacy Policy*, JPMORGAN CHASE & CO., https://www.chase.com/digital/resources/privacy-security/privacy/online-privacy-policy (last updated Dec. 10, 2020) (under "Information we collect") [https://perma.cc/5M6S-7NLF].

[212] GOOGLE, *supra* note 152 (under "We want you to understand the types of information we collect as you use our services" in the pop-up window for "personal information").

[213] COX, *supra* note 210 (under "Your Information").

the GDPR or the CCPA. AT&T uses the CCPA's definition of *personal information.*[214] Comcast defines personal information as "any information that is linked or reasonably linkable to you or your household,"[215] which includes part of (but not the full) CCPA definition. Comcast states that personal information "can include information that does not personally identify you—such as device numbers, IP addresses, and account numbers" and "may also include information that does personally identify you, such as your name, address, and telephone number."[216]

Finally, some privacy policies use different terms and definitions depending on the privacy law that applies in the person's location. In its nationwide privacy policy, Facebook avoids use of the term personal information, but characterizes "information that personally identifies you" as "information such as your name or email address that by itself can be used to contact you or identifies who you are."[217] In contrast, in its California privacy policy, Facebook uses the term personal information, and adopts a definition similar to (but not exactly the same as) the CCPA's definition.[218]

Both the GDPR and the CCPA also recognize that personal information may be used to establish a person's identity, even if the information lacks an identifier that itself establishes that identity. The GDPR specifies that a natural person may be identified "by reference to . . . location data . . . or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[219] The EU clarifies that "it is possible to categorise [a] person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her."[220] Thus, data records that contain no personal identifiers still relate to an identifiable natural person, if the information in those records is "reasonably likely to be used," potentially in combination with other available information, "to identify the natural person" to whom the information relates.[221]

The CCPA takes a similar approach to the use of personal information to establish identity, albeit with different language. The CCPA's definition of *personal information* implies that a particular consumer may be identified using information that "is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer."[222] The phrase "could reasonably be linked, directly or indirectly, with" is similar to that used often used by the Federal Trade Commission.

[214] AT&T, *supra* note 153 (under "When this Policy applies").

[215] XFINITY, *supra* note 167 (under "Introduction" in the popup window for *personal information*).

[216] *Id.* (under "The Personal Information We Collect and How We Collect It").

[217] FACEBOOK, *supra* note 175 (under "Advertisers").

[218] Facebook, *California Privacy Notice*, https://www.facebook.com/legal/policy/ccpa (last updated July 1, 2021), [https://perma.cc/9RP2-CZRY].

[219] GDPR, *supra* note 1, at art. 4(1).

[220] EU HANDBOOK, *supra* note 192, at 89 (quoting an opinion issued by the Article 29 Data Protection Working Party).

[221] GDPR, *supra* note 1, at recital 26.

[222] CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

The concept of reasonable linkability is more familiar in the United States, and thus serves as a good starting point. However, the CCPA does not define the term.

Garfinkel defines *linkable information* as "information about or related to an individual for which there is a possibility of logical association with other information about the individual."[223] Adding a reasonableness test and leveraging the definition of *personal information* results in:

> The term "reasonably linkable information" means personal information for which there is a reasonable possibility of logical association with other information relating to the person or household to whom the personal information relates.

Reasonably linkable information is thus personal, private, and reasonably identifiable.

B. Defining Reasonably Identifiable Information, Pseudonymous Information, and Non-Trackable Information

The choice framework proposed in Part V differentiates between the use and sharing of three different types of reasonably linkable information. This subsection crafts definitions of each.

1. Is the Information Trackable?

The most privacy preserving form of reasonably linkable information is *non-trackable information*. Tracking is made possible by associating pieces of personal information with each other, even if they are not associated with a person by name.

Part III.B discussed information relating to a person or household that is identifiable but has not yet been identified, and that is *not* tracked over time. Such personal information typically involves the use of non-persistent identifiers such as randomized one-time identifiers. Polonetsky states that, in such personal information, direct identifiers have been removed or transformed so that they cannot link back to any individual, but indirect identifiers may remain intact if they have "no life outside of the specific context in which it was used."[224]

Consumer privacy laws increasingly are concerned with whether personal information can be used to track a person and create a profile, even if the person's name is not associated with the profile. The CCPA defines *profiling* as "any form of automated processing of personal information . . . to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences,

[223] GARFINKEL, *supra* note 97, at 42.

[224] Polonetsky, et al., *supra* note 95, at 615.

interests, reliability, behavior, location, or movements."[225] The CCPA distinguishes between profiling versus "[s]hort-term, transient use" of personal information.[226] For example, if a consumer opts-out of sharing of personal information, the CCPA prohibits a business from profiling that consumer, but allows the business to use the consumer's personal information for non-personalized advertising shown as part of the consumer's current interaction with the business.[227] The GDPR also extensively discusses profiling. It requires that privacy notices specifically include disclosure of profiling,[228] and it gives consumers a right to opt-out of profiling used for direct marketing purposes.[229]

However, neither the GDPR nor the CCPA defines trackable information as an explicit subset of personal information. Instead, they consider profiling as a particular use of personal information. As a result, while they include specific provisions related to profiling, neither require disclosure of whether personal information is stored and use in a trackable form, and neither incorporate tracking directly into their choice framework.

A spirited debate has occurred about whether personal information is trackable when non-persistent identifiers are used. Many identifiers used by service and apps to associate information relating to a person are resettable. Common examples of resettable identifiers include dynamic IP addresses, advertising identifiers that can be reset using mobile device settings, and cookies that can be cleared using browser settings.

Most privacy policies are unclear about whether they consider resettable identifiers and information associated with them to be included in the scope of personally identifiable information. Indeed, providers of services and apps often argue that they are not. Apple argued that information "identified by non-personally identifiable identifiers such as those that are random, resettable, or rotating" should *not* be included in the scope of *personal information* under the CCPA.[230] One common argument made by those opposed to classifying a household's IP address as a personal identifier is that IP addresses are often assigned to a household for only a limited period of time. The Network Advertising Initiative thus argued that resettable identifiers "do not in fact relate to any one unique consumer," and hence it

[225] CAL. CIV. CODE § 1798.140(z). The GDPR has an identical definition, except that it uses the term *personal data* instead of *personal information*; *see* GDPR, *supra* note 1, at art. 4(4).

[226] *Id.* § 1798.140(e)(4).

[227] *Id.* §§ 1798.135(f), .140(e)(4).

[228] GDPR, *supra* note 1, at arts. 13(2)(f), 14(2)(g).

[229] *Id.* at art. 21(2).

[230] E-mail from Katie Kennedy, Priv. & Info. Sec. Counsel, Apple, Inc. to California Dep't of Just. Priv. Reguls. at 4, (Mar. 8, 2019, 3:10 PM) (on file with California Office of the Attorney Gen.), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf.

proposed that probabilistic identifiers and information associated with them be *excluded* from the scope of *personal information*.[231]

The ambiguity of whether information relating to a person by reference to a resettable identifier is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a consumer privacy law that resettable identifiers are a common method of tracking a person. The CCPA treats a resettable identifier, and the information associated with it, as *personal information* if it "can be used to recognize a consumer [or] a family . . . over time . . . ."[232] The CCPA further explicitly states that an IP address qualifies as *personal information* if it could be reasonably linked with a particular consumer or household.[233] The GDPR takes a slightly different tack, classifying a resettable identifier, and the information associated with it, as a *personal data* if and only if it can be reasonably used to identify an individual or household.[234] EU guidance states than an IP address is *personal data* if there is additional information reasonably available that identifies the person to whom the IP address has been assigned.[235]

Dynamic IP addresses are usually assigned by an Internet Service Provider to a house's modem for at least a day at a time, and they are usually renewed at the end of the IP address lease, so that a dynamic IP address is usually associated with a household for weeks or months at a time. Advertising identifiers and cookies are usually very persistent. In most situations, they are only cleared when a user explicitly does so.[236]

Many consumers have a higher sensitivity when their personal information is tracked over time than when it is used only in the current interaction with a business. However, whereas both the CCPA and the GDPR consider profiling to be a particular use of personal information, it is a cleaner approach to define a particular category of personal information that allows tracking to take place. The advantage of this approach is that *trackable information* takes it rightful place on the spectrum of identifiability, rather than being called out as a particular use of personal information. This helps guide an assignment of notice and consent obligations onto trackable information that is in the public interest and that is reasonable compared to the obligations placed onto other types of personal information.

Drawing on the CCPA's description of profiling as involving the linking of personal information from more than one interaction, and Polonetsky's description of it as involving the linking of personal information from more than one context, *non-trackable information* can be defined as:

[231] Letter from David LeDuc, Vice President of Public Policy, The Networking Advert. Initiative, to California Attorney Gen. Xavier Becerra, 10 (Mar. 8, 2019) (on file with The Networking Advert. Initiative), https://thenai.org/wp-content/uploads/2021/07/naicommentletterccpaimplementingregulations.pdf [https://perma.cc/V9VY-XUP9].

[232] CAL. CIV. CODE § 1798.140(aj) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[233] *Id.* § 1798.140(v)(1).

[234] GDPR, *supra* note 1, at recital 26.

[235] EU HANDBOOK, *supra* note 192, at 91-92.

[236] Less commonly, a user may have set a browser to automatically clear cookies upon exit.

> The term "non-trackable information" means reasonably linkable information for there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.

The definition builds on the previous proposed definition of reasonably linkable information, but also requires that the logical association be not reasonably possible over time.

If reasonably linkable information fails to meet the definition of non-trackable information, then it remains trackable:

> The term "trackable information" means reasonably linkable information that is not non-trackable information.

2. Is the Information Reasonably Identifiable?

The second most privacy-preserving form of reasonably linkable information is *pseudonymous information*. Part III.A discussed information relating to a person or household that is identifiable but has not yet been identified, and that is tracked over time. Such personal information typically involves the use of persistent identifiers such as device identifiers or advertising identifiers that can be used to track a person or household over time.

Almost all online services and apps collect device identifiers. These device identifiers very often include IP addresses, see e.g., the privacy policies of Chase, Uber, and United.[237] Apps that run on mobile devices also often collect the IMEI identifiers of mobile devices, see e.g., the privacy policies of Google, Microsoft, and Apple.[238] Often, privacy policies state that they collect device identifiers, but fail to specify which ones, see e.g., the privacy policies of AT&T, Comcast, Facebook, Pinterest, and Twitter.[239]

Almost all online advertising-supported service and apps also collect advertising identifiers. Such advertising identifiers are usually associated with

[237] JPMORGAN CHASE & CO., *supra* note 211 (under "Usage and Other Information" and "Chase Mobile"); *Uber Privacy Notice*, UBER TECHNOLOGIES INC., https://www.uber.com/legal/en/document/?name=privacy-notice&country=united-states&lang=en (last updated Dec. 22, 2021) (under III.A.2 "Device data") [https://perma.cc/LL9R-B9A5]; *Customer Data Privacy Policy*, UNITED AIRLINES INC., (last updated Mar. 12, 2021), https://www.united.com/ual/en/us/fly/privacy.html (under "Information we collect automatically" and "Information we collect through our mobile application(s)").

[238] GOOGLE, *supra* note 152, at "Unique identifiers"; MICROSOFT, *supra* note 181, at "Personal data we collect"; Apple, *supra* note 196, at "What personal information we collect" and at "Cookies and Other Technologies."

[239] AT&T, *supra* note 153 (under "The information we collect"); XFINITY, *supra* note 167 (under "The Personal Information We Collect and How We Collect It"); FACEBOOK, *supra* note 175 (under "Identifiers"); PINTEREST, *supra* note 174, under ("We also get technical information when you use Pinterest"); TWITTER, *supra* note 183 (under "You should read this policy in full, but here are a few key things we hope you take away from it" and then "Log Data").

a particular device, and thus serve as de-facto device identifiers. Most commonly, services and apps collect Apple and Android advertising identifiers, see e.g., the privacy policies of KAYAK, The Weather Channel, and Zillow.[240]

However, privacy policies differ in whether they include, in the scope of personally identifiable information, device identifiers and information that is associated with device identifiers. Many privacy policies limit the scope of personally identifiable information to an identifier that itself identifies a person, and perhaps to information that the provider of that service or app links to that identifier. Although such privacy policies almost always disclose that the service or app collects device identifiers, they do not typically discuss whether device identifiers are considered by the provider to qualify as a method of identification of a person. This leaves open the question of whether these privacy policies consider device identifiers, and information that is associated with device identifiers, to constitute personally identifiable information.

Indeed, providers of services and apps often argue that these device identifiers do *not* identify a person, and thus that information associated with device identifiers or advertising identifiers does *not* constitute personally identifiable information. Google argued that device identifiers are often *not* associated with a person's identity; and thus one should question whether Google's privacy policy considers information associated with a device identifier to constitute personally identifiable information.[241] The Internet & Television Association (NCTA), a trade association representing cable Internet Service Providers, argued that IP addresses *cannot* identify an individual on their own.[242] The Internet Advertising Bureau (IAB), a trade association representing Internet advertisers and ad brokers, argued that an "anonymous identifier" should *not* qualify as personally identifiable information.[243] The Network Advertising Initiative, a trade association representing Internet advertising companies, argued that IP addresses are not *personal information* under CCPA, unless a business "has linked it, or reasonably could link it, with additional pieces of information known by the

[240] KAYAK, *supra* note 155 (under "Information We Collect and Use"); THE WEATHER CO., *supra* note 154 (under "1.B"); *Privacy Policy*, ZILLOW GRP., https://www.zillowgroup.com/zg-privacy-policy/ (last updated Jan. 29, 2021) (under "Device information") [https://perma.cc/3VNC-MSXN].

[241] Comments of Google at 3, (Feb. 8, 2019) (on file with California Office of the Attorney Gen.) https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf ("where companies collect device-identifying information online and do not associate that information with a consumer's name, email address, or other identifying information").

[242] Protecting the Privacy of Customers of Broadband and Other Telecomm. Servs., *Report and Order*, 31 FCC Rcd. 13911, para. 94 n.239 (2016) [hereinafter *FCC Order*].

[243] *Id.*

business to identify a particular consumer or household, such as name or residential address."[244]

The ambiguity of whether information relating to a person by reference to a device identifier is included in privacy policy disclosures demonstrates the importance of clearly spelling out in a privacy law that device identifiers are a common method of linking information to a person. The GDPR classifies a device identifier, and any other information associated with it, as *personal data* if and only if it can be attributed to a natural person, including by the use of additional information.[245] So the question remains: can a device identifier be attributed to a person? EC guidance gives advertising identifiers as an example of *personal data* without limitation, but the question has likely not been definitively answered.[246] The CCPA is also less than clear on this issue. The original version of the CCPA explicitly included device identifiers in its definition of a *unique identifier*, which in turn implies that device identifiers are, without limitation, a form of identification of a person. However, the recently revised version of the CCPA may be interpreted to classify device identifiers and the information associated with it as *personal information* if and only if the device is "linked to" or "could be reasonably linked to" a consumer or family.[247]

The ability of a business to use a device identifier to establish the identity of a person depends on the nature of the device identifier and the availability of information that associates the device identifier with a natural person. Advertising identifiers are frequently shared by devices, and they are shared widely within the advertising ecosystem. There is additional reasonably available information that associates an advertising identifier with a natural person. It should be presumed that a person's identity can be reasonably established using an advertising identifier, and thus that the combination of an advertising identifier with other personal information constitutes *reasonably identifiable information*. It is possible that a device identifier is shared by a device only in a pseudonymous fashion, and that subsequent user actions do not render that identifier sufficient to identify a person. However, in general, any persistent identifier that is shared widely within the advertising ecosystem will render that identifier sufficient to identify a person, because eventually that information will be associated with a person's identity, e.g., when a person registers with a website or purchases an item.

[244] E-mail from Leigh Freund, President & Chief Executive Officer, The Networking Advert. Initiative, to California Attorney Gen. Xavier Becerra, 4 (Feb. 25, 2020) (on file with The Networking Advert. Initiative), https://thenai.org/wp-content/uploads/2021/07/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020-1.pdf [https://perma.cc/4KNC-ARWD].

[245] GDPR, *supra* note 1, at recital 26.

[246] *What is Personal Data?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/B9FF-ZY3A] (under "Examples of personal data").

[247] CAL. CIV. CODE §§ 1798.140(x), .140(aj) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

The GDPR does not distinguish between persistent and non-persistent indirect identifiers in its definition of *pseudonymisation*:

> [T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[248]

Thus, under the GDPR, the use of persistent indirect identifiers might result in pseudonymous personal data used for tracking, whereas the use of non-persistent indirect identifiers might result in pseudonymous personal data not used for tracking. The GDPR considers both types of information to be personal data.[249]

To avoid this confusing use of terminology, this proposal uses the term *non-trackable information* (as defined above) to describe the use of non-persistent indirect identifiers, and the term *pseudonymous information* to describe the use of persistent indirect identifiers. Drawing upon the GDPR's description of pseudonymous information as resulting in the inability to attribute the information to a specific person without the use of additional information, and adding a reasonableness test, *pseudonymous information* can be defined as:

> The term "pseudonymous information" means trackable information for which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.

The definition builds on the previous proposed definition of *trackable information*, but also requires that the information cannot be associated with other reasonably linkable information such that the combined information can be used to reasonably identify the related person or household.

If *trackable information* fails to meet the definition of *pseudonymous information*, then it remains reasonably identifiable:

[248] GDPR, *supra* note 1, at art. 4(5).

[249] *Id.*

The term "reasonably identifiable information" means trackable information that is not pseudonymous information.

C. Defining De-Identified Information and Anonymous Information

The GDPR defines *anonymous information*, but not *de-identified information*.[250] The CCPA defines *de-identified information*, but not *anonymous information*.[251] The two definitions are not the same. This subsection crafts definitions of both.

1. Is the Information Anonymous?

The GDPR defines *anonymous information* as "information which does not relate to an identified or identifiable natural person."[252]

This definition simply inverts the definition of *personal data*, and thus includes (a) information that is not personal and (b) information that is personal but whose degree of identifiability falls short of *personal data*. There are several problems with this definition. First, it needlessly includes information that does not relate to an individual or household, and thus conflates anonymous information with non-personal information. More critically, it fails to distinguish between anonymous information and de-identified information. The GDPR simply excludes both from *personal data*, and then exempts them from notice and choice requirements.

Polonetsky describes anonymous information as personal information in which both direct and indirect identifiers have been removed or transformed so that they cannot link back to any individual, and in which the method for removal or transformation includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification.[253] As an example of an anonymization technique that can provide such guarantees, Polonetsky mentions differential privacy algorithms, which can hide whether or not an individual is present in a dataset.

Privacy policies often overreach in their claims that personal information is anonymous. AT&T defines Anonymous Information as "[i]nformation that doesn't directly identify and can't reasonably be used to identify an individual customer or user."[254] Anonymous Information is thus defined by AT&T as all information that AT&T does not consider to be Personal Information, which it defines as "[i]nformation that directly identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address."[255] AT&T then explains that "[w]e treat identifiers like cookies, advertising

[250] *Id.* at recital 26.

[251] CAL. CIV. CODE § 1798.140(m).

[252] GDPR, *supra* note 1, at recital 26.

[253] Polonetsky et al., *supra* note 95, at 618.

[254] AT&T, *supra* note 153 (under "Definitions").

[255] *Id.*

identifiers, device identifiers, and household identifiers as Anonymous Information except in circumstances where they can be used to identify you."[256] However, the information is almost certainly personal, and is presumably private. If it includes an identifier such as an advertising identifier or device identifier, then it is also linkable, not de-identified, and trackable. Thus, it certainly does not qualify as *anonymous information.* Under the GDPR, it almost certainly would be categorized as *personal data*, and under the CCPA as *personal information.*

KAYAK defines Anonymized Information as "information that cannot be linked to you or any other specific user using any means available to us, either because it was collected anonymously or has been subsequently anonymized."[257] KAYAK states that "[i]nformation that is anonymous or has been anonymized is no longer considered 'personal information.'"[258] KAYAK appears to include in the scope of Anonymized Information, and thus exclude from the scope of Personal Information, information that it considers to be "de-identified usage data" that is associated with a mobile advertising identifier.[259] Indeed, KAYAK states that Anonymized Information "may be subsequently used for any purpose."[260] KAYAK's descriptions of Anonymized Information are inconsistent. If the information can truly not be linked to a person or household, including to a non-identifiable person or household, then it would qualify as *anonymous information*. However, if the information includes a mobile advertising identifier, then it neither qualifies as *anonymous information*, nor *de-identified information*, nor even as *non-trackable information*.

For its "eero" branded Wi-Fi products Amazon defines Anonymous Data as "data that, either in its original form or as the result of anonymization procedures that we perform on Personal Data, is not associated with or linked to your Personal Data."[261] Amazon asserts that "Anonymous Data does not, by itself, permit the identification of individual persons."[262] Amazon explains that, "[w]e may create Anonymous Data records from Personal Data by using various procedures to remove or obscure information (such as your name, email address, phone number or IP address) that makes the data personally identifiable to you," and then reserves the right to use and share Anonymous Data for any purposes, apparently without disclosure.[263] Amazon's description of Anonymous Data are too vague to allow classification. At best, Amazon's procedures to remove or obscure information may result in *anonymous information*, if the procedures include mathematical and technical guarantees that are sufficient on their own to prevent reidentification.

[256] *Id.*

[257] KAYAK, *supra* note 155 (under "How we use your information").

[258] *Id.* (under "How we use your information").

[259] *Id.* (under "Our Advertising Cookies").

[260] *Id.* (under "How we use your information").

[261] *Privacy for eero Devices, Applications and Services*, EERO https://eero.com/legal/privacy (last updated Feb. 28, 2020) (under "Types of data we collect") [https://perma.cc/3H7N-57YT].

[262] *Id.* (under "Types of data we collect").

[263] *Id.* (under "Use of your Personal Data").

However, Amazon's procedures to remove or obscure information may not have such guarantees, and may easily be *de-identified information, non-trackable information,* or *pseudonymous information*. Furthermore, given that Amazon only requires that Anonymous Data not "by itself" permit the identification of a person, it is possible that it is linkable to information that does permit the identification of a person, in which case the information is properly classified as *reasonably identifiable information*.

The ability, or lack thereof, to associate or link information to an individual or household features prominently in the distinction between anonymous information and other types of more identifiable personal information. Indeed, the CCPA's definition of *personal information* relies strongly on the concept: "information that . . . is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[264]

Following the guidance in Polonetsky that anonymous information includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification, this subsection focuses on the technical ability of associating information with a particular consumer or household; the following subsection considers whether the association can be reasonably made. Garfinkel (2015) defines linkable information as "information about or related to an individual for which there is a possibility of logical association with other information about the individual."[265]

This test can be adapted to the proposed definition of *personal information*:

> The term "anonymous information" means personal information for which there is no possibility of logical association with other information relating to the person or household to whom the personal information relates.

If *personal information* is not anonymous, it should be classified it as *linkable information*, defined as:

> The term "linkable information" means personal information that is not anonymous information.

Privacy laws sometimes also distinguish between anonymous information and aggregate information. Polonetsky considers aggregated anonymous information to be a subset of anonymous information. In aggregated anonymous information, the data are so highly aggregated that the aggregation itself serves as a mathematical and technical guarantee so as to prevent reidentification.[266]

[264] CAL. CIV. CODE § 1798.140(v)(1) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[265] GARFINKEL, *supra* note 97, at 42.

[266] Polonetsky et al., *supra* note 95, at 618.

The CCPA defines *aggregate consumer information* as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device," and then explains that it does not include "one or more individual consumer records that have been deidentified." [267] The CCPA then excludes *aggregate consumer information* from *personal information*. The GDPR similarly considers *aggregate data* to be a subset of *anonymous information*, and then excludes it from *personal data*.[268]

That said, there is no need to define in a consumer privacy law a category of aggregate information because it is typically afforded the same treatment as other types of *anonymous information*.

2. Is the Information De-Identified?

Polonetsky distinguishes de-identified information from anonymous information based on the difficulty of associating the information with the person to whom it is related. In order to qualify as either de-identified information or anonymous information, both direct and indirect identifiers must have been removed or transformed so that they cannot link back to any individual. Whereas for anonymous information the method for removal or transformation includes mathematical and technical guarantees that are sufficient on their own to distort the data so as to prevent reidentification, for de-identified information such mathematical and technical guarantees are absent and legal controls take the place of technological controls. As examples of de-identification techniques that remove both direct and indirect identifiers, but which cannot provide mathematical and technical guarantees, Polonetsky mentions suppression, generalization, perturbation, and swapping algorithms. Garfinkel provides an overview of these types of algorithms.[269]

Privacy policies often make overstated claims that personal information is de-identified. KAYAK classifies as "de-identified usage data" mobile advertising identifiers, "anonymous device identifiers," and cookies.[270] Such identifiers result in a reasonable possibility of logical association with other information relating to the person or household to whom the information relates, and thus it is not *de-identified information*. Furthermore, such identifiers are persistent, and thus the associated information is not *non-trackable information*.

The proposed definition of *anonymous information* already captures the subset of *personal information* in which reidentification is prevented solely using technological controls. If such technological controls are absent, the information remains classified as *linkable information*. It remains to delineate *linkable information* for which the logical association is possible but not

[267] CAL. CIV. CODE § 1798.140(b).

[268] GDPR, *supra* note 1, at recital 162.

[269] GARFINKEL, *supra* note 97, at 20.

[270] KAYAK, *supra* note 155 (under "Our Advertising Cookies").

reasonable given the current state of technology, the availability of information with which it can be associated, and legal controls.

The CCPA defines *de-identified information* as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer . . . ."[271]

The intent is to exempt from the CCPA's definition of *personal information* a category of information that can be logically associated with an individual or household, but for which the association cannot be reasonably made due to a combination of technological and legal controls.

The CCPA's definition can be adapted to build on the proposed definition of *linkable information*:

> The term "de-identified information" means linkable information for which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.

This completes the set of definitions of different types of personal information. The logical flow used to classify them is illustrated in Figure 5.

[271] CAL. CIV. CODE § 1798.140(m).

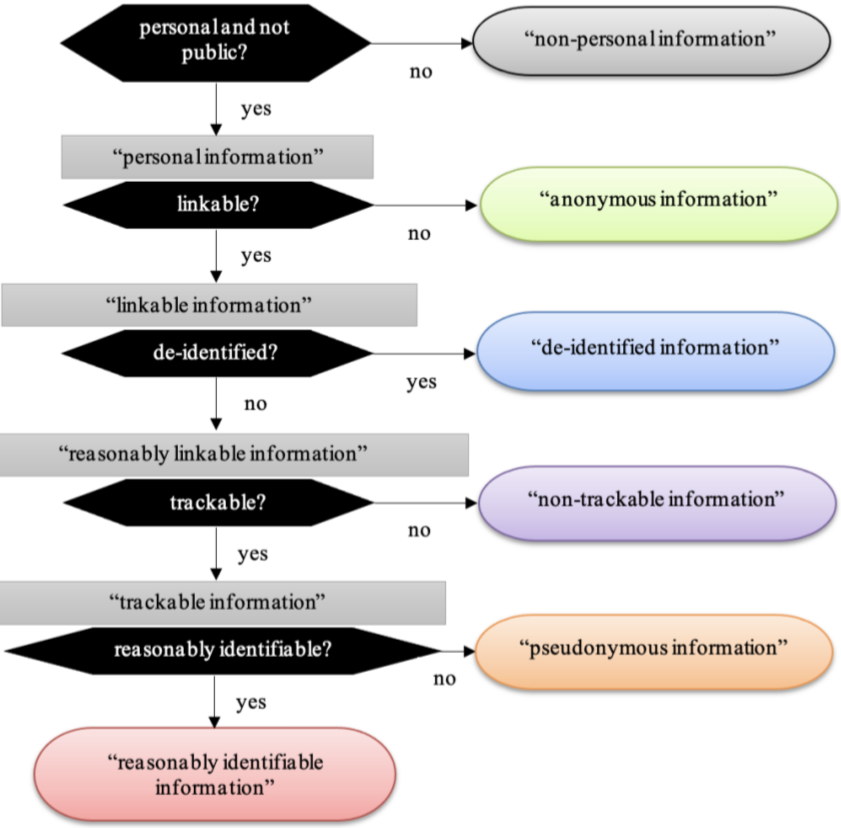


Figure 5. Classification of Information

D. Defining Sensitive Information and Functional Use

The choice framework proposed in Part V treats sensitive personal information differently than non-sensitive personal information, and it treats use for functional purposes differently than use for non-functional purposes. This subsection crafts definitions of these terms.

1. Sensitive Personal Information

The GDPR's category of sensitive personal data includes specific types of information relating to a person's physical characteristics: "genetic data, biometric data [processed] for the purpose of uniquely identifying a natural person, data concerning health" and "personal data revealing racial or ethnic origin."[272] The GDPR's definition also includes specific types of information relating to a person's behavior or beliefs: "personal data revealing . . . political opinions, religious or philosophical beliefs, or trade union membership" and "data concerning a natural person's sex life or sexual orientation."[273] The CCPA's definition of *sensitive personal information* similarly includes

[272] GDPR, *supra* note 1, at art. 9(1).
[273] *Id.*

genetic data, biometric information, health information, racial or ethnic origin, religious or philosophical beliefs, and sex life or sexual orientation.[274]

However, limiting the scope of sensitive information to these specific types is insufficient when personal information on the Internet is often not easily categorized. Personal information collected on the Internet often includes a list of websites that a consumer has visited, and it may include the content of communications. In 2016, the Federal Communications Commission (FCC) issued the Broadband Privacy Order, which focuses on consumer privacy for broadband Internet service.[275] Given this focus, the FCC Order is interesting for its guidance on which types of Internet related activity should be classified as sensitive. The Order classifies as sensitive "precise geo-location information," recognizing the prevalence of collection of personal information on mobile devices and the wealth of detail that location information can reveal.[276] The Order classifies as sensitive the "content of communications," citing the long legal history of protecting its privacy in different forms of communications.[277] The FCC Order also classifies as sensitive "web browsing history," explaining that:

> [A] user's browsing history can provide a record of her reading habits, . . . her video viewing habits, . . . who she communicates with, . . . when and with what entities she maintains financial or medical accounts, her political beliefs, . . . attributes like gender, age, race, income range, and employment status, . . . a customer's financial status, familial status, race, religion, political leanings, age, and location.[278]

Finally, the FCC Order also classifies as sensitive "application usage history," explaining that:

[274] CAL. CIV. CODE § 1798.140(ae).

[275] *FCC Order*, *supra* note 242. The Order was repealed by the United States Congress in 2017. Joint Resolution, Pub. L. No. 115-22 (2017).

[276] *Id.* at para. 179.

[277] *Id.* at para. 180.

[278] *Id.* at para. 183.

> [T]he user's newsreader application will give indications of what he is reading, when, and how; an online video player's use will transmit information about the videos he is watching in addition to the video contents themselves; an email, video chat, or over-the-top voice application will transmit and receive not only the messages themselves, but the names and contact information of his various friends, family, colleagues, and others; a banking or insurance company application will convey information about his health or finances; even the mere existence of those applications will indicate who he does business with.[279]

Precise geo-location information, the content of communications, web browsing history, and application usage history should all be classified as sensitive information. A definition that combines these types of information with the types given in the GDPR and the CCPA is:

> The term "sensitive," when used in conjunction with any type of personal information, means personal information that relates to sensitive characteristics of a person or household, including, but not limited to:
> (A) private personal identifiers, including social security number, driver's license number, state identification card number, and passport number;
> (B) private physical characteristics, including genetic data, biometric data, health data, and racial or ethnic origin; or
> (C) personal information about behavior or beliefs, including political opinions, religious or philosophical beliefs, union membership, sex life or sexual orientation, financial information, information pertaining to children, precise geo-location, content of communications, web browsing history, and application usage history.
> The term "non-sensitive," when used in conjunction with any type of personal information, means personal information that is not sensitive information.

2. Functional Use

The GDPR requires a lawful basis for processing of personal data.[280] One such lawful basis for the processing of non-sensitive personal data is a contract between the user and the controller, if the processing is necessary for the performance of the contract.[281] EU guidance explains that "what is 'necessary for the performance of a contract' is not simply an assessment of

[279] *Id.* at para. 184.
[280] GDPR, *supra* note 1, at art. 5(1).
[281] *Id.* at art. 6(1)(b).

what is permitted by or written into the terms of a contract."[282] It further explains that the *necessity* clause limits processing authorized by terms and conditions to that which "cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur."[283] Personalization of content qualifies if it is "an intrinsic aspect" of the service."[284] However, processing of personal data for the purposes of improving a service is not considered necessary.[285] Neither is processing of personal data for the purposes of behavioral advertising.[286]

The CCPA limits the disclosure of personal information that may be mandated by terms and conditions of a service to those required for a *business purpose*, which it defines as the "use of personal information for a business's operational purposes . . . provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose . . . ."[287] The use under this exception must be related to the functionality of the service. Behavioral advertising does not qualify.[288] But the CCPA then proceeds to give an exhaustive list of business purposes, including auditing, security, debugging, customer service, internal research, and non-personalized advertising.[289]

The GDPR's requirement that functional use be determined by a contract is unnecessarily limiting. Applications often offer elective functionality, e.g., a map can provide turn-by-turn directions if and only if the user allows it to access the user's location. Such elective functionality may not be written into any contract. The CCPA's requirement that functional use be limited to a specific list in the statute is also unnecessarily limiting. A better approach is to simply tie functional use to the functionality provided, and to exclude the use of personal information to subsidize a service:

> The term "functional use" means the technical use of personal information to provide functionality. Functional use does not include the use of personal information in exchange for consideration from a third party.

Any functional use of personal information under this definition should qualify under the GDPR as necessary for the performance of a contract if the functional use were incorporated into a contract between the user and the controller. However, this definition does not require a contract. Most of the uses of personal information that qualify under the CCPA as a business purpose would qualify as a functional use, including security, debugging, and

[282] EUROPEAN DATA PROT. BD., GUIDELINES 2/2019 ON THE PROCESSING OF PERSONAL DATA UNDER ARTICLE 6(1)(B) GDPR IN THE CONTEXT OF THE PROVISION OF ONLINE SERVICES TO DATA SUBJECTS para. 23 (Oct. 8, 2019).

[283] *Id.* at para. 30.

[284] *Id.* at para. 57.

[285] *Id.* at paras. 48-49.

[286] *Id.* at paras. 51-56.

[287] CAL. CIV. CODE § 1798.140(e) (Deering, LEXIS through Ch. 11 of 2022 Reg. Sess.).

[288] *Id.* § 1798.140(e)(4).

[289] *Id.* § 1798.140(e).

customer service. Internal research would not qualify as a functional use, despite its inclusion in the CCPA as a business purpose. Personalization features of an app, such as those discussed in Table 4 qualify as functional use, although they might not qualify under the CCPA as a business purpose.

E. Defining Processing and Choice

1. Collection, Use, and Sharing

The GDPR defines *processing* as:

> [A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[290]

Processing thus includes collection, use, and sharing of personal data. Although some of the GDPR's requirements are specific to either collection, use, or sharing, the GDPR does not separately define these terms.

In contrast, the CCPA defines separate terms for collection and sharing, but not for use. It defines *collection* as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."[291] It defines two types of sharing, both of which include "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information."[292] One type, called *selling*, involves the sale of personal information to another entity "for monetary or other valuable consideration."[293] The other type, called *sharing,* involves the sharing of personal information with another entity specifically for cross-context behavioral advertising, whether or not it involves monetary or other valuable consideration.[294] Both definitions exclude sharing of personal information for certain purposes, including consumer-directed disclosure.

It is helpful to distinguish between collection, use, and sharing when tailoring notice and consent requirements. Drawing from the terms defined in the GDPR and the CCPA, these terms could be defined as:

[290] GDPR, *supra* note 1, at art. 4(2).
[291] CAL. CIV. CODE § 1798.140(f).
[292] *Id.* §§ 1798.140(ad), .140(ah).
[293] *Id.* § 1798.140(ad).
[294] *Id.* § 1798.140(ah).

> The term "collection" of personal information means access to personal information by any means, including but not limited to gathering, recording, storing, obtaining, receiving, buying, or renting.
> The term "use" of personal information means any operation or set of operations performed on personal information, including but not limited to organization, structuring, adaptation, alteration, retrieval, consultation, alignment, or combination of personal information.
> The term "sharing" of personal information means disclosure by any means, including but not limited to disclosure by transmission, dissemination, making available, releasing, transferring, renting, selling, or otherwise communicating, except that it excludes disclosure to a contractor.

This definition of *sharing* differs the CCPA's definitions of *selling* and *sharing*. First, there is no need to limit the term to disclosure for consideration, since even disclosure that does not involve consideration impacts privacy. Second, there is no need to specifically define disclosure for particular purposes (e.g., cross-context behavioral advertising) or to exclude sharing of personal information for certain purposes (e.g., consumer-directed disclosure). It is cleaner and more comprehensible to address the purposes for sharing of personal information when formulating notice and choice provisions. Part VIII.F discusses the role of contractors and the reason to exclude disclosure to a contractor.

2. Choice

The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[295]

The CCPA includes a similar definition of consent.[296] EU guidance clarifies that the "freely given" requirement precludes "consent [that] is bundled up as a non-negotiable part of terms and conditions."[297] The GDPR explains that "clear affirmative action" could include "ticking a box . . . [or] choosing technical settings," but does not include "[s]ilence [or] pre-ticked boxes."[298] The GDPR's consent requirement is thus often described as opt-in consent. Incorporating the terms collection, use, and sharing results in:

[295] GDPR, *supra* note 1, at art. 4(11).

[296] CAL. CIV. CODE § 1798.140(h).

[297] EUROPEAN DATA PROT. BD., *Guidelines 02/2020 on Consent Under Regulation 2016/679* 7 (May 4, 2020).

[298] GDPR, *supra* note 1, at recital 32.

> The term "opt-in consent" to specified collection, use, and/or sharing of personal information means any freely given, specific, informed and unambiguous indication of the person's wishes, by a statement or by a clear affirmative action, by which the person signifies agreement to the specified collection, use, and/or sharing of personal information relating to that person.

The GDPR does not utilize the concept of an opt-out choice. The CCPA describes a user's right to opt-out of sharing or selling of personal information as "the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information."[299]

Aligning this definition with that of *opt-in consent* gives:

> The term "opt-out choice" of specified collection, use, and/or sharing of personal information means a choice by which a person can withdraw consent to the specified collection, use, and/or sharing of personal information relating to that person.

F. Defining Various Entities

Notice and choice requirements are applied to certain types of entities that collect, use, and share personal information. A consumer privacy law must delineate the entities to which these requirements apply.

1. Controllers and Contractors

Consumer privacy laws often distinguish between entities that make decisions about the collection, use, and sharing of personal information versus entities that are hired to implement specific tasks involving the collection and use of personal information.

To describe entities that make decisions about the collection, use, and sharing of personal information, the GDPR first defines a *controller* as an entity that "alone or jointly with others, determines the purposes and means of the processing of personal data."[300]

The CCPA similarly defines a *business* as an entity that "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information."[301]

A comprehensive consumer privacy law may apply to a broader class of entities than businesses.[302] There is no need to limit the definition of a *controller* to entities that themselves collect personal information or that on

[299] CAL. CIV. CODE § 1798.120(a).

[300] GDPR, *supra* note 1, at art. 4(7).

[301] CAL. CIV. CODE § 1798.140(d).

[302] A privacy law must also determine whether notice and choice requirements apply to all controllers, only to for-profit controllers, or only to large for-profit controllers.

behalf of which personal information is collected. An entity that does not itself collect personal information or that on behalf of which personal information is collected, but which nevertheless determines the purposes and means of the processing of personal information, should still be treated as controller, since it remains the entity that controls the collection, use, and sharing of personal information. Incorporating the definitions of *collection*, *use*, and *sharing* into the GDPR's definition of *controller* results in:

> The term "controller" means an entity that alone or jointly with others determines the purposes and means of the collection, use, and/or sharing of personal information.

To describe entities that are hired to implement specific tasks involving the collection and use of personal information, the GDPR defines a *processor* as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[303]

The CCPA similarly defines a *service provider* as "a person that processes personal information on behalf of a business[,] and that receives from or on behalf of the business[,] a consumer's personal information . . . ."[304]

Both the GDPR and the CCPA intend that an entity should only qualify as a *processor* (resp. *service provider*) to the extent that its processing of personal information is limited to the specific tasks it was hired by a controller to do. The GDPR limits a processor's handling of personal data to that which is "governed by a contract … that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, [and] the type of personal data and categories of data subjects."[305]

The CCPA limits a service provider's handling of personal information to that

[303] GDPR, *supra* note 1, at art. 4(8).

[304] CAL. CIV. CODE § 1798.140(ag)(1). The CCPA also defines a related term, *contractor*; *see* CAL. CIV. CODE § 1798.140(j)(1).

[305] GDPR, *supra* note 1, at art. 28(3).

> [F]or a business purpose pursuant to a written contract [that] prohibits the [service provider] from: (A) [s]elling or sharing the personal information; (B) [r]etaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract …; (C) [r]etaining, using, or disclosing the [personal] information outside of the direct business relationship between the service provider and the business; [and] (D) [c]ombining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer . . . .[306]

It is thus intended that an entity that processes personal information, and that doesn't qualify as a *processor* (resp. *service provider*) with respect to that processing, should be classified as a *controller* (resp. *business*). Both the GDPR and the CCPA rely on the phrase "on behalf of" to convey this meaning. However, it would be better if the definition tied back into the phrase "determines the purposes and means" used in the definition of *controller* in order to make it clear that an entity that processes personal information cannot escape being designated as either a *controller* or a *processor*.

Neither the term *processor* nor *service provider* convey the intent of this distinction. Instead, this proposal uses the term *contractor*:

> The term "contractor" means an entity that collects, uses, and/or shares personal information but does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information. An entity does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information if and only if it collects, uses, and/or shares personal information solely pursuant to a written contract that prohibits the entity from collecting, using, and/or sharing personal information for any purposes or using any means other than that specified by the controller(s) of that personal information.[307]

Similar to the CCPA's definition of service provider (but unlike the GDPR's definition of processor), this definition directly incorporates the requirement for the contract. However, this definition of contractor differs from the CCPA's definition of service provider. The CCPA limits the purposes for the processing of personal information by a service provider to a specified list of business purposes, including auditing, security, debugging,

[306] CAL. CIV. CODE § 1798.140(ag)(1). *See also* CAL. CIV. CODE § 1798.140(j)(1) for a similar provision regarding contractors.

[307] This article's use of the term *contractor* is not exactly the same as the CCPA's use of the term *contractor*.

customer service, internal research, and non-personalized advertising.[308] There is no need to limit a contractor's activities to a defined list. Instead, notice and choice requirements should differentiate between functional and non-functional activities. This distinction is addressed below.

2. First and Third Parties

Consumer privacy laws often distinguish between first parties and third parties. The first party is the party with whom a consumer intentionally interacts. The CCPA defines a *third party* as "a person who is not . . . [t]he business with whom the consumer intentionally interacts . . . [a] service provider to the business; or [a] contractor."[309] It is cleaner to first define a *first party*:

> The term "first party" means an entity with whom a consumer intentionally interacts.

Third parties are usually considered to include all other parties that process personal information. However, under the GDPR, a controller is responsible for the activities of its processors, and thus the controller remains the first party with respect to the actions of its processors.[310] Similarly, under the CCPA, a business is responsible for the activities of its service providers and contractors, and thus the business remains the first party with respect to the actions of its service providers and contractors. C*ontractors* should thus be excluded from the definition of a *third party*:

> The term "third party" means any entity other than a first party or a first party's contractors.

First parties are often controllers that collect and use personal information. First parties may also share personal information with a third party, who then becomes a controller by virtue of having collected personal information from the first party.

On the Internet, it is common that, as part of a consumer's interaction with a first party, the first party not only shares the IP address of the consumer with a third party but also enables the third party to directly collect further information from the consumer. For example, the first party may be a website, and the third party may be an advertiser on that website. Some advertisements are displayed using software that has the ability to collect further information. Although the ensuing interaction between the third party and the consumer is direct, the consumer is typically unaware of the third party's further collection of personal information.

[308] *See* CAL. CIV. CODE § 1798.140(e).

[309] *Id.* § 1798.140(ai).

[310] *See* GDPR, *supra* note 1, at art. 4(7)-(8). The GDPR defines *third party* somewhat similarly, but it uses the term exclusively in the context of consent; *see id.* at art. 4(10).

G. Legal Controls

The classification of various types of personal information relies on characteristics of that information. The CCPA recognizes that in order for information to maintain those characteristics, legal controls are often required.

1. Legal Controls on De-Identified Information

The discussion is most developed in the context of de-identified information. The FTC Report proposed three legal controls, but it framed these three legal controls as a safe harbor. Specifically, it proposed that information should be considered "not [] reasonably linkable to a particular consumer or device" if the business possessing the information implements three legal controls.[311] In contrast, the CCPA first requires that the information actually be de-identified, i.e. that it cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, and then in addition requires that a business that possesses *deidentified* information implement three legal controls.

The CCPA's higher level of protection is appropriate. If there is a reasonable possibility of logical association of *linkable information* with other information relating to the person or household to whom the *linkable information* relates, then it should not qualify as *de-identified information*, even if a business possessing that information implements the specified legal controls intended to prevent such association but fails to accomplish that goal. For this reason, a consumer privacy law should require legal controls on de-identified information:

> In order to qualify as de-identified information, the entity possessing that information must implement controls (A1) to (D1) below.

The first legal control in the FTC Report is that the business "must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[312] The CCPA somewhat similarly requires that a business possessing de-identified information "[t]ake reasonable measures to ensure that the information cannot be associated with a consumer or household."[313]

The FTC Report and the CCPA maintain this legal control for different reasons. In the FTC Report, a business's "reasonable level of justified confidence" that the information is de-identified is the principal element of the safe harbor. In the CCPA, however, the legal control is in addition to the requirement that the information actually be de-identified. There remains a

[311] *FTC Report*, *supra* note 91, at 21.
[312] *Id.*
[313] CAL. CIV. CODE § 1798.140(m)(1).

good reason to add a similar legal control because even if a business possesses de-identified information, it is in the public interest that the information not later be re-identified.

There is another difference between the FTC's phrasing and the CCPA's phrasing. The CCPA requires reasonable measures to ensure that the information "cannot be" re-identified, whereas the FTC requires reasonable measures to ensure that the information "cannot reasonably be" re-identified. The test should be "reasonably linkable," both to first qualify as *de-identified information* and also as a legal control.

Building on the proposed definition of *de-identified information*, the first legal control should be:

> (A1) It must take reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.

The second legal control in the FTC Report is that the business "must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data."[314] For the FTC, this legal control enables the FTC to act under Section 5 of the FTC Act if the commitment is violated. In a privacy law, there would likely be other and stronger methods of enforcement. Nevertheless, such a public commitment is in the public interest, and the CCPA mirrors this legal control.[315] Thus, the second and third legal controls should be:

> (B1) It must publicly commit to maintain and use the information only in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates.
> (C1) It must publicly commit to not attempt to associate the information with other information relating to the person or household to whom the linkable information relates.

The third legal control in the FTC Report is that if a business makes de-identified information available to other companies, it must "contractually prohibit such entities from attempting to re-identify the data."[316] This legal control ensures that the direct recipient of de-identified information doesn't re-identify the information. The CCPA takes this a step further, requiring that a business possessing de-identified information "[c]ontractually obligates any recipients of the information to comply with all provisions of this subdivision."[317] Thus, in addition to prohibiting direct recipients from re-

[314] *FTC Report*, *supra* note 91, at 21.
[315] CAL. CIV. CODE § 1798.140(m)(2).
[316] *FTC Report*, *supra* note 91, at 21.
[317] CAL. CIV. CODE § 1798.140(m)(3).

identification, it also requires recipients to make similar public commitments and to contractually prohibit any downstream recipients from re-identifying the information. This expanded legal control prohibits all downstream re-identification. The last legal control be:

> (D1) It must contractually obligate any third parties to whom it discloses the information to implement controls (A1) to (D1).

2. Legal Controls on Non-Trackable Information

As with de-identified information, the technological algorithm used to transform the personal information into non-trackable information is not sufficient to guarantee that tracking is not possible. There remains a need to add legal controls. Neither the GDPR nor the CCPA place legal controls on non-trackable information, since neither distinguishes such information from other types of personal data (under the GDPR) or personal information (under the CCPA). However, the legal controls placed in the previous subsection on de-identified information can be mirrored here:

> In order to qualify as non-trackable information, the entity possessing that information must implement controls (A2) to (D2) below.
>
> (A2) It must take reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
>
> (B2) It must publicly commit to maintain and use the information only in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
>
> (C2) It must publicly commit to not attempt to associate the information with other information relating to the person or household obtained from another context or another interaction with the person or household.
>
> (D2) It must contractually obligate any third parties to whom it discloses the information to implement controls (A2) to (D2).

3. Legal Controls on Pseudonymous Information

Pseudonymous information requires legal controls to ensure that the related person or household is not identified. Neither the GDPR nor the CCPA place legal controls on trackable information, since neither distinguishes such information from other types of personal data (under the GDPR) or personal information (under the CCPA). However, the legal controls used above can be mirrored here:

> In order to qualify as pseudonymous information, the entity possessing that information must implement controls (A3) to (D3) below.
> (A3) It must take reasonable measures to ensure that the information remains in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.
> (B3) It must publicly commit to maintain and use the information only in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information.
> (C3) It must publicly commit to not attempt to identify the person or household to whom the information is related.
> (D3) It must contractually obligate any third parties to whom it discloses the information to implement controls (A3) to (D3).

IX. CONCLUSION

Part III presented a proposal for splitting the scope of personal data as defined in the GDPR or the CCPA into three different sets, based on whether or not personal information is reasonably identifiable and whether or not it is used for tracking. Statutory definitions of these three classifications were developed in Part VIII.

These three classifications of personal information enable the creation of choice framework that utilizes all three options: mandating use through terms and conditions, requiring an opt-out choice, and requiring opt-in consent. The proposed choice framework, developed in Part V, incentivizes the use of pseudonymous information instead of readily identifiable information, and incentivizes the use of one-time identifiers and thereby reduces tracking. Neither the GDPR nor the CCPA incentivizes pseudonymization or disincentivizes tracking through their choice frameworks.

Part VII presented a proposal for corresponding notice requirements. Businesses should disclose the classification of each category of personal information collected, so that consumers may understand the associated privacy risks and make informed choices whether to allow this personal information to be collected. Businesses should disclose whether each use of personal information enables functionality, so that consumers may make informed choices whether to allow each use of their personal information. The sources and recipients should be disclosed, so that consumers may make informed choices whether to allow their personal information to be shared.

There are clearly alternative policy options to these proposals for notice and choice. One could define fewer classifications of personal information, at the cost of not being able to distinguish between them in a choice framework.

One could modify the choice framework in Table 7, and either shift some uses and sharing from opt-out to opt-in to disincentivize them, or one could shift some uses and sharing from opt-in to opt-out to lower the disincentive. However, alternative policy options should be evaluated to determine the tradeoffs between simplicity, privacy protection, and economic impact.

Finally, any notice and choice requirements must be accompanied by statutory text that spells out how consumers can exercise their rights.

APPENDIX: STATUTORY TEXT

Sec. 1. Definitions

(1) **Anonymous Information:** The term 'anonymous information' means personal information for which there is no possibility of logical association with other information relating to the person or household to whom the personal information relates.

(2) **Collection:** The term 'collection' of personal information means access to personal information by any means, including but not limited to gathering, recording, storing, obtaining, receiving, buying, or renting.

(3) **Communications Service:** The term 'communications service' means interstate or foreign communications by wire or radio

(4) **Controller:** The term 'controller' means an entity that alone or jointly with others determines the purposes and means of the collection, use, and/or sharing of personal information.

(5) **Contractor:** The term 'contractor' means an entity that collects, uses, and/or shares personal information but does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information. An entity does not alone or jointly with others determine the purposes and means of the collection, use, and/or sharing of personal information if and only if it collects, uses, and/or shares personal information solely pursuant to a written contract that prohibits the entity from collecting, using, and/or sharing personal information for any purposes or using any means other than that specified by the controller(s) of that personal information.

(6) **De-Identified Information:** The term 'de-identified information' means linkable information for which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates,

(B) publicly commits to maintain and use the information only in a form in which there is no reasonable possibility of logical association with other information relating to the person or household to whom the linkable information relates,

(C) publicly commits to not attempt to associate the information with other information relating to the person or household to whom the linkable information relates, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(7) **First Party:** The term 'first party' means an entity with whom a consumer intentionally interacts.

(8) **Functional Use:** The term 'functional use' means the technical use of personal information to provide functionality. Functional use does not include the use of personal information in exchange for consideration from a third party.

(9) **Linkable Information:** The term 'linkable information' means personal information that is not anonymous information.

(10) **Non-Trackable Information:** The term 'non-trackable information' means reasonably linkable information for there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household,

(B) publicly commits to maintain and use the information only in a form in which there is no reasonable possibility of logical association of the information with other information relating to the person or household obtained from another context or another interaction with the person or household,

(C) publicly commits to not attempt to associate the information with other information relating to the person or household obtained from another context or another interaction with the person or household, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(11) **Non-Sensitive:** The term 'non-sensitive', when used in conjunction with any type of personal information, means personal information that is not sensitive information.

(12) **Opt-In Consent:** The term 'opt-in consent' to specified collection, use, and/or sharing of personal information means any freely given, specific, informed and unambiguous indication of the person's wishes, by a statement or by a clear affirmative action, by which the

person signifies agreement to the specified collection, use, and/or sharing of personal information relating to that person.

(13) **Opt-Out Choice:** The term 'opt-out choice' of specified collection, use, and/or sharing of personal information means a choice by which a person can withdraw consent to the specified collection, use, and/or sharing of personal information relating to that person.

(14) **Personal Information:** The term 'personal information' means any information relating to a natural person or to a household, excluding publicly available information.

(15) **Pseudonymous Information:** The term 'pseudonymous information' means trackable information for which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information, providing that the controller:

(A) takes reasonable measures to ensure that the information remains in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information,

(B) publicly commits to maintain and use the information only in a form in which the related person or household is not reasonably identifiable using that personal information and other reasonably linkable information,

(C) publicly commits to not attempt to identify the person or household to whom the information is related, and

(D) contractually obligates any third parties to whom it discloses the information to implement controls (A), (B), and (C).

(16) **Publicly Available Information:** The term 'publicly available information' means information relating to a natural person or to a household (a) in publicly available government records, (b) that the person or household to whom the personal information is related has made publicly available, or (c) that was made publicly available by widely distributed media.

(17) **Reasonably Identifiable Information:** The term 'reasonably identifiable information' means trackable information that is not pseudonymous information.

(18) **Reasonably Linkable Information:** The term 'reasonably linkable information' means personal information for which there is a reasonable possibility of logical association with other information relating to the person or household to whom the personal information relates.

(19) **Sensitive:** The term 'sensitive', when used in conjunction with any type of personal information, means personal information that relates to sensitive characteristics of a person or household, including, but not limited to:

(A) private personal identifiers, including social security number, driver's license number, state identification card number, and passport number;

(B) private physical characteristics, including genetic data, biometric data, health data, and racial or ethnic origin; or

(C) personal information about behavior or beliefs, including political opinions, religious or philosophical beliefs, union membership, sex life or sexual orientation, financial information, information pertaining to children, precise geo-location, content of communications, web browsing history, and application usage history.

(20) **Sharing:** The term 'sharing' of personal information means disclosure by any means, including but not limited to disclosure by transmission, dissemination, making available, releasing, transferring, renting, selling, or otherwise communicating, except that it excludes disclosure to a contractor.

(21) **Third Party:** The term 'third party' means any entity other than a first party or a first party's contractors.

(22) **Trackable Information:** The term 'trackable information' means reasonably linkable information that is not non-trackable information.

(23) **Use:** The term 'use' of personal information means any operation or set of operations performed on personal information, including but not limited to organization, structuring, adaptation, alteration, retrieval, consultation, alignment, or combination of personal information.

Sec. 2. Notice

(a) **Privacy Policy:** A controller shall maintain a publicly accessible privacy policy. The privacy policy shall disclose accurate information regarding the controller's collection, use, and sharing of personal information sufficient for consumers to make informed choices regarding the use of the controller's services.

(b) **Categories Of Personal Information:** The privacy policy shall disclose the categories of personal information collected and used, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

(c) **Methods And Sources:** The privacy policy shall disclose, for each category of personal information collected:

(1) the method of collection (if the personal information is collected by or on behalf of the controller), and

(2) the sources of collection (if the personal information is shared with the controller by another entity).

(d) **Purposes:** The privacy policy shall disclose, for each category of personal information collected or used, the purposes for which the category of personal information is collected or used.

(e) **Functional Use:** The privacy policy shall disclose, for each category of personal information collected or used and each such purpose, whether the use constitutes functional use, and if so, the functionality enabled by the collection and use of that category of personal information.

(f) **Shared Personal Information:** The privacy policy shall disclose the categories of personal information shared, and for each such category, the classification(s) of that category. The classifications shall consist of reasonably identifiable information, pseudonymous information, non-trackable information, de-identified information, and anonymous information.

(g) **Recipients:** The privacy policy shall disclose the third parties with which the controller shares personal information. For each such third party, the privacy policy shall disclose the categories of personal information shared with that third party, the purposes for which the controller shares each category of personal information with that third party, and any contractual limits on the third party's use and further sharing of that personal information. If a controller enables any third parties to collect additional personal information, the controller's privacy policy shall disclose the third parties so enabled and any contractual limits on such collection.

Sec. 2. Choice

(a) **Markets With Effective Competition:** A controller in a market with effective competition, except for a controller offering telecommunications (insofar as it receives or obtains personal information by virtue of its provision of telecommunications), shall

(1) **Opt-Out of Non-Functional Use:** offer consumers an opt-out choice from the controller's collection and use for non-functional purposes (if any) of the consumer's non-sensitive reasonably identifiable information and sensitive pseudonymous information,

(2) **Opt-In To Non-Functional Use:** obtain opt-in consent for the controller's collection and use for non-functional purposes (if any) of the consumer's sensitive reasonably identifiable information,

(3) **Opt-Out of Sharing:** offer consumers an opt-out choice from the controller's sharing (if any) of the consumer's non-sensitive pseudonymous information and sensitive non-trackable information, and

(4) **Opt-In To Sharing:** obtain opt-in consent for the controller's sharing (if any) of the consumer's reasonably identifiable information and sensitive pseudonymous information.

(b) **Markets Without Effective Competition and Communications Services:** A controller in a market without effective competition, and a controller offering a communications service (insofar as it receives or obtains personal information by virtue of its provision of a communications service), shall

(1) **Opt-Out of Non-Functional Use:** offer consumers an opt-out choice from the controller's collection and use for non-functional purposes (if any) of the consumer's non-sensitive pseudonymous information and sensitive non-trackable information,

(2) **Opt-In To Non-Functional Use:** obtain opt-in consent for the controller's collection and use for non-functional purposes (if any) of the consumer's reasonably identifiable information and sensitive pseudonymous information,

(3) **Opt-Out of Sharing:** offer consumers an opt-out choice from the controller's sharing (if any) of the consumer's non-sensitive non-trackable information, and

(4) **Opt-In To Sharing:** obtain opt-in consent for the controller's sharing (if any) of the consumer's reasonably identifiable information, pseudonymous information, and sensitive non-trackable information.

We Don’t All Look the Same: Police Use of Facial Recognition and the *Brady* Rule

Jaylla Brown[*]

TABLE OF CONTENTS

[*] J.D., May 2022, The George Washington University Law School. B.A. 2019, Political Science, Hampton University. While I cannot list every person that has helped me make this happen, I would like to specifically thank my mother, Susan Brown, for her support throughout this journey, and both my grandmothers Rev. Nancy A. Brown and Patricia Onakoya for instilling in me the importance of education, journalism, and advocacy.

I. INTRODUCTION

Julia and Rosie Williams, two sisters from Farmington Hills, Michigan, were two and five years old when they watched their father get wrongfully arrested in their front yard on January 9, 2020. The girls looked on in tears as they saw their father pull into their driveway and immediately be handcuffed by police. It would be thirty hours until the Williams sisters saw their father again. After a day of disappearance, he told his family that he was arrested because of a computer error.

Their father was brought downtown to the police station to be questioned by detectives in a small room. While in this room, the detectives showed him two grainy stills taken from surveillance footage and a picture of his previous driver's license. In response to him telling the detectives that the man in the pictures from the surveillance footage was not him, a detective responded, "I guess the computer got it wrong too?" The father took a picture from the surveillance footage, held it next to his face and said, "I hope you don't think all Black people look alike." Despite his protest, Mr. Williams was detained and later released on bail. Luckily, his case was dismissed at his arraignment hearing because there was a second witness who had not identified Mr. Williams as the defendant.

Notwithstanding the dismissal of Mr. Williams' case, his daughters still live with the trauma of seeing their father get arrested for a crime he did not commit based on flawed facial recognition technology. But what would have happened if her father had to go to trial? Would he have access to the evidence he needed to defend himself in court? How would his lawyer build a case without any knowledge of the system that misidentified her client? Would the prosecutor be kind enough to inform the defense of the role facial recognition played in convicting him?

All of these questions arise when police cannot identify who they saw perpetrating a crime, so they rely on facial recognition to help them identify an unknown face.[1] While investigating a crime, the police can photograph a suspect and then use facial recognition to search that image against a database of mugshots and driver's licenses to help them identify that suspect by name.[2]

The fallible nature of facial recognition makes it particularly dangerous when used by law enforcement. Police sometimes use this technology in a manner that can be likened to a "virtual line-up."[3] However in this line-up, a human does not point to the suspect, an algorithm does.[4]

Many factors can influence the accuracy of this line-up. Most algorithms require human operation, so the operator's competence and lack

[1] CLARE GARVIE ET AL., CTR. ON PRIV. & TECHNOLOGY GEO. L., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/V3CL-U35Z].

[2] *Id.* at 11-12.

[3] *Id.* at 1.

[4] *Id.*

of bias are crucial.[5] Additionally, there are factors that affect the accuracy of the algorithm itself. Facial recognition algorithms have higher rates of misidentification for Native Americans, African Americans, and Asian Americans.[6] They also have higher error rates for identifying women in comparison to men.[7] The least accurate error rates are most commonly seen in subjects who are female, Black, and eighteen to thirty years old.[8] Facial recognition technology performs worst on darker-skinned females, with the highest rate of error at 34.7%.[9] The darker the skin, the more errors, and gender orientation makes algorithm accuracy even more difficult to achieve.[10]

Given the substantial risk of misidentification for women and Black people by facial recognition, defendants should be able to challenge these factors in order to argue that they have been falsely matched based on their race or gender. If the operation of a system or the algorithm itself is flawed, then the identification decision is flawed. If a defendant can produce evidence that exposes a faulty identification, they can argue that the system identified the wrong suspect. This is impossible if the defendant does not have access to that evidence. If the prosecution is aware of any materially exculpable evidence for the accused, there is a Constitutional obligation to disclose it.[11] But, if the prosecution fails to do so, the defense is handicapped.[12]

In *Brady v. Maryland*, the Supreme Court held that nondisclosure of exculpatory evidence to the defendant violates the Due Process Clause of the Fourteenth Amendment, which entitles defendants to the right to a fair trial.[13] Scholars have suggested the *Brady* rule poses a doctrinal solution for access to facial recognition evidence.[14] However, this Note focuses specifically on *Brady* as a solution for defendants who have been misidentified by the technology based on their race or gender. These defendants are most likely to be misidentified by facial recognition and pursued as suspects by law enforcement.[15] The purpose of this Note is to demonstrate how evidence of racial or gender disparities impacting the accuracy of facial recognition

[5] Amici Curiae Brief of ACLU et al. in Support of Petitioner at 15-16, Lynch v. State, 2019 WL 3249799 (Fla. July 19, 2019) (No. SC19-298).

[6] PATRICK GROTHER ET AL., NAT'L INST. OF STANDARDS & TECHNOLOGY, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 7 (2019).

[7] *Id.* at 2.

[8] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV.: SCI. NEWS (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/3WC6-PDYG].

[9] JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION 1 (Sorelle A. Friedler & Christo Wilson eds., 2018).

[10] Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/99YE-MXTB].

[11] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

[12] *See* Elizabeth Napier Dewar, *A Fair Trial Remedy for* Brady *Violations*, 115 YALE L.J. 1450, 1452 (2006).

[13] *See Brady*, 373 U.S. at 86.

[14] *See* Rebecca Darin Goldberg, *You Can See My Face, Why Can't I? Facial Recognition and Brady*, COLUM. HUM. RTS. L. REV. ONLINE, Apr. 12, 2021.

[15] *Id.* at 271-72.

technology qualifies as *Brady* material that the prosecution is obligated to disclose.

Despite defendants' need to access evidence about whether facial recognition was used in order to challenge its accuracy and to prevail on a misidentification defense, the Florida First District Court of Appeal ruled that defendants are not even entitled to view photos of other potential suspects identified by a facial recognition search that led to their arrest.[16] The court reasoned that because there is no reasonable probability the result of a trial would change if this evidence was disclosed to a defendant, there is no defendants' right to disclosure under *Brady*.[17] This opinion comes from *Lynch v. State*, where the court ultimately sentenced a Black man to eight years in jail for selling cocaine in 2016.[18] Lynch planned to use other photos that the facial recognition software produced alongside his to prove that he had been misidentified.[19] He argued that since the other matches were also potential suspects returned by the system, they would cast doubt on his identification as the defendant.[20] The court rejected Lynch's argument and he was never able to see the other photos produced by the system.[21]

The facial recognition system that identified Lynch, along with the pictures of four other potential suspects he was never able to see, is called the Face Analysis Comparison and Examination System (FACES).[22] Pinellas County Sheriff Department in Florida launched FACES in 2001, and since then it has become one of the most advanced statewide facial recognition systems in the country.[23] In 2020, the Department indicated that there were no plans of discontinuing the use of FACES despite the recent criticism that police use of facial recognition technology has received.[24]

This Note will explain why police use of facial recognition technology for criminal identification should be defined as exculpatory evidence that prosecutors have a duty to disclose under *Brady*. Part II, Section A will explain what facial recognition is and how it works. Section B will outline the racially discriminatory implications underlying facial recognition systems. Section C will discuss how law enforcement uses facial recognition. Section D will detail the *Lynch* case which illustrates how a Florida court has treated

[16] *Lynch v. State*, 260 So. 3d 1166, 1169-70 (Fla. Dist. Ct. App. 2018).

[17] *Id.*

[18] Aaron Mak, *Facing Facts: A Case in Florida Demonstrates the Problems with Using Facial Recognition to Identify Suspects in Low-Stakes Crimes*, SLATE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/7XH3-MDXR].

[19] *Id.*

[20] Brief for Lynch at *17-18, *Lynch v. Florida*, No. 1D16-3290, 2017 WL 11618201 (Fla. App. 1 Dist. May 25, 2017).

[21] *Lynch*, 260 So. 3d at 1170.

[22] Amici Curiae Brief of ACLU et al., *supra* note 5, at 3.

[23] Jerry Iannelli, *Miami-Dade Cops Want Permanent Access to Controversial Facial Recognition Database*, MIA. NEW TIMES (Nov. 8, 2019, 9:00 AM), https://www.miaminewtimes.com/news/miami-dade-police-department-wants-to-use-pinellas-county-faces-facial-recognition-database-11313634 [https://perma.cc/3AG5-24P8].

[24] Malena Carollo, *Florida Police Embrace Facial Recognition Despite Pushback*, GOV'T TECHNOLOGY (June 26, 2020), https://www.govtech.com/public-safety/florida-police-embrace-facial-recognition-despite-pushback.html [https://perma.cc/C7TV-3YAP].

facial recognition as evidence in criminal court. Section E will explain what the *Brady* rule is. Part III will assert why facial recognition technology evidence qualifies as *Brady* material for minorities and women of color. Part III, Section A will explain why police misuse of facial recognition qualifies as *Brady* material for said defendants. Finally, Section B will explain why evidence of poor algorithm quality qualifies as *Brady* material.

II. BACKGROUND

A. What Is Facial Recognition?

Facial recognition is a form of biometrics that was created in the mid-1960s.[25] Biometrics is a technical term for body measurements and calculations such as DNA and fingerprints.[26] Biometrics is used to compare one piece of information to a dataset in order to determine someone's identity.[27] Where biometrics could involve a fingerprint analysis—comparing one fingerprint against a database of fingerprints to find a match—facial recognition aims to verify a person's identity by comparing a face against a dataset of other faces to produce a match.[28] The face that is compared to the dataset is called a probe image, which can be sourced from a photograph or video.[29]

Before the software can match someone's face to others in a given database, an algorithm is used to find the person's face within the reference image.[30] Then, the system reads the geometry of the face to determine key characteristics such as the distance between the eyes and the distance from the forehead to the chin.[31] Those characteristics make up a "facial signature" which is a mathematical formula that the system can understand.[32] After the facial signature is created, the system "normalizes" the face by scaling, rotating and aligning it to optimize positioning for comparison to the dataset of other faces.[33] Lastly, the algorithm examines pairs of faces and assigns a numerical score that reflects the similarity of the matches.[34]

[25] CRIMINAL CTS. COMM., N.Y.C. BAR ASS'N, POWER, PERVASIVENESS AND POTENTIAL: THE BRAVE NEW WORLD OF FACIAL RECOGNITION THROUGH A CRIMINAL LAW LENS (AND BEYOND) 1 (2020).

[26] *Id.*

[27] *Id.*

[28] *Street-Level Surveillance: Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition [https://perma.cc/AZP9-FRB7].

[29] Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, CHAMPION, July 2019, at 14.

[30] GARVIE ET AL., *supra* note 1, at 9.

[31] Steve Symanovich, *What Is Facial Recognition? How Facial Recognition Works*, NORTON (Aug. 20, 2021), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html#:~:text=Facial%20recognition%20software%20reads%20the,The%20result%3A%20your%20facial%20signature. [https://perma.cc/9PMA-53QT].

[32] *Id.*

[33] GARVIE ET AL., *supra* note 1, at 9.

[34] *Id.*

The algorithm that examines and compares the probe image to the faces in a database is a machine learning system.[35]A machine learning system must be trained to examine and analyze faces. The data used to train an algorithm is called a "training data set" comprised of faces that help the system practice identifying facial characteristics for comparison.[36] But the demographics of that training set strongly influence the algorithm's ability to accurately interpret a diversity of faces.[37] For example, "if a training set is skewed towards a certain race, the algorithm may be better at identifying members of that group as compared to individuals of other races."[38] This concept is known as "overfitting" to the training data.[39]

Facial recognition algorithms tend to be probabilistic in nature.[40] They do not produce a binary "yes or no" answer, but instead identify more likely to less likely matches.[41] This type of algorithm is referred to as a "one-to-many" search algorithm because it compares the facial signature from a probe image to all the facial features found in the faces from the dataset.[42] Once each match has been assigned a numerical value or "score" that reflects the level of similarity, that value is compared against a threshold value that helps the system determine whether the two faces represent the same person.[43] The threshold value, set by algorithm developers, determines how high the match score must be to signify that the two images are of the same person.[44] The key components that affect the accuracy of facial recognition software fall into two categories: (1) the operation of the system, and, (2) the development of the algorithm. Each of these can be problematic.

B. Problems with Facial Recognition

1. Operational Flaws

Like any other technology or system, the success and accuracy of it largely depends on how well it is being operated. "Since face recognition accuracy remains far from perfect, experts agree that a human must double-check the results of face recognition searches to ensure that they are correct."[45] It follows that the more skilled the human reviewer, the more accurate the search is.[46] But issues arise when the human reviewer is not

[35] *See* P'SHIP ON AI, UNDERSTANDING FACIAL RECOGNITION SYSTEMS 4 (2020).

[36] Alexandre Gonfalonieri, *How to Build a Data Set for Your Machine Learning Project*, TOWARDS DATA SCI. (Feb. 13, 2019), https://towardsdatascience.com/how-to-build-a-data-set-for-your-machine-learning-project-5b3b871881ac [https://perma.cc/A8L4-QSPT].

[37] GARVIE ET AL., *supra* note 1, at 9.

[38] *Id.*

[39] *See* Daniel Nelson, *What Is Overfitting?*, UNITE.AI (Aug. 23, 2020), https://www.unite.ai/what-is-overfitting/ [https://perma.cc/RQ6G-HJPY].

[40] GARVIE ET AL., *supra* note 1, at 9.

[41] *Id.*

[42] *See* GROTHER ET AL., *supra* note 6, at 5.

[43] *See id.* at 4.

[44] P'SHIP ON AI, *supra* note 35, at 6.

[45] GARVIE ET AL., *supra* note 1, at 49.

[46] *Id.*

knowledgeable on how the facial recognition technology works or how it has a substandard ability to recognize faces.[47] Adequate operational training greatly impacts the success of a facial recognition program because it helps to avoid human errors that stem from implicit bias, lack of expertise, or incompetence. However, the lack of uniform operational standards for the people using facial recognition fails to hold entities accountable to provide effective training.[48]

a. Human Review Bias

Human reviewers are susceptible to biases that can negatively impact their ability to check the results produced by an algorithm depending on what information the software gives them. Some state forensic scientists may feel pressure to interpret results in a way that is favorable to the state government pushing for a conviction.[49] Some facial recognition systems, such as Florida's FACES, show candidates' criminal history alongside the results that are matched to a probe image.[50] If a facial recognition search returns multiple possible matches for a suspect along with the criminal history of each suspect, the analyst may be biased against the person with the longest or most severe history, and, thus, more likely to confirm that person as the actual match. A study on a subjectivity and bias when operating DNA analysis, a different but comparable forensic tool to facial recognition, found that forensic DNA analysts were influenced and possibly biased by extraneous information concerning the DNA they examined.[51] Developers of facial recognition systems must account for these risks when training their operators.

Along with the risk of human reviewers being influenced by tangential information, there are also psychological biases that can impact a person's neutrality when reviewing potential matches. According to an experiment conducted in 2015, researchers found that people are better at making judgements about face pairings with faces that they know rather than those they do not.[52] Not only are unfamiliar faces harder for humans to recognize, but evidence shows that people are generally better at recognizing those from their same race, which creates dire risks for people of color.[53]

In-depth training for human reviewers could address implicit bias concerns when operating facial recognition. One study tested the accuracy of Australian passport personnel after using an algorithm to check for duplicate passport applications.[54] The personnel who receive limited instruction in face

[47] *Id.*

[48] Goldberg, *supra* note 14, at 270.

[49] Amici Curiae Brief of ACLU et al., *supra* note 5, at 3.

[50] *Id.* at 16 (arguing that analysts' bias may be exacerbated when they are aware of the identified individual's criminal history when interpreting the results of a facial recognition search).

[51] *Id.* (citing Itiel E. Dror & Greg Hampikian, Subjectivity and Bias in Forensic DNA Mixture Interpretation, 51 SCI. & JUST. 204, 205–07 (2011)).

[52] Kay L. Ritchie et al., *Viewers Base Estimates of Face Matching Accuracy on Their Own Familiarity: Explaining the Photo-ID Paradox*, 141 COGNITION 161 (2015).

[53] GARVIE ET AL., *supra* note 1, at 49.

[54] *Id.*

matching were only accurate fifty percent of the time compared to the trained facial examiners who outperformed them by twenty percent .[55] Despite the benefits that human training can have, not all facial recognition systems train their operators the same.

b. Poor Personnel Training

There are some private companies and entities that employ operational guidelines for their facial recognition technology, but there is no national standard for how these analysts should be trained for reviewing results.[56] A lack of uniformity in training and operations oversight leaves room for varied efforts by human operators to ensure that the results produced by facial recognition systems are accurate. One facial recognition search conducted by Detroit police yielded six possible suspect matches, which were then shown to a security guard who never saw the person in question but was tasked with confirming the correct match for identification.[57] In that instance, the only human review on the facial recognition results was an untrained outside individual. Some facial recognition searches evade human review altogether when police conduct facial recognition searches in the field with their mobile devices, and the algorithm produces instantaneous results.[58] Until the personnel operating facial recognition systems are held to a uniform standard, the risk for human error remains one of the biggest operational flaws to which the technology is susceptible.

2. Algorithmic Flaws

Facial recognition systems vary in their ability to identify people, and no system is 100% accurate.[59] Most facial recognition systems are built using algorithms to detect faces,[60] which is a crucial part of the system. Algorithm accuracy is influenced by the quality of the probe image being searched, the enrollment database the image is compared to, the training set database the algorithm is developed with, and the match thresholds set by developers.[61] All these factors influence the algorithm's ability to accurately return matches in a search, and conditions like race, sex, and gender are an added layer that

[55] *Id.*

[56] CRIMINAL CTS. COMM., *supra* note 25, at 21.

[57] Letter from Phil Mayor, Senior Staff Att'y, ACLU Fund of Michigan, to Chief Investigator, Detroit Pub. Safety Headquarters (June 24, 2020). This is referring to an incident of false identification of Robert Williams by Detroit Police Department when they used facial recognition and will be discussed later in Part II, Section C. How Law Enforcement Uses Facial Recognition.

[58] GARVIE ET AL., *supra* note 1, at 50.

[59] JENNIFER LYNCH, ELEC. FRONTIER FOUND., FACE OFF: LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY 6 (Gennie Gebhart ed., 2019).

[60] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/4WY6-TCY7].

[61] P'SHIP ON AI, *supra* note 35, at 4.

complicates developing the best algorithm to identify individuals with precision.

a. Probe Image Quality

As previously mentioned, most one-to-one facial recognition systems require a probe image as a basis for comparison to find a match within a database.[62] The quality of a probe image heavily influences the system's ability to return an accurate match.[63] If the probe image is at a low resolution, it is more difficult for the algorithm to decipher the facial signature of the probe at the stage before comparison.[64] Factors such as angle lighting and the newness of the technology used to capture the image all impact the quality of the probe image.[65] All of these variables should be taken into consideration when evaluating the risk of error caused by a low quality probe image used in a facial recognition search.

b. The Enrollment Database

The quality of the enrollment database that the probe image is compared against is also important to the overall accuracy of the algorithm. Problems arise when this database is not adequately representative of the population that the facial recognition technology is being used on. "Law enforcement search their probe images against a database of mug shots, driver's licenses, or . . . unsolved photo file[s]," so these are the sources for their enrollment database.[66] However, the issue of racial bias arises because "years of well-documented racially biased police practices" have resulted in a disproportionate number of African Americans, Latinos, and immigrants included in criminal databases.[67] San Francisco is a prime example of the racial implications resulting from the over-policing of Black communities. "Over-policing" is defined as strategic police practices in which studies show that when police increase their presence in Black communities, there is an increased likelihood of disproportionate levels of stops, searches, arrests, and pretrial detention for Black people.[68] "African American women make up only 5.8% of San Francisco's total female population, but constituted 45.5% of all female arrests in 2013."[69] The overrepresentation of minorities, especially African Americans, in mugshot enrollment databases means that

[62] Jackson, *supra* note 29, at 14.

[63] Amici Curiae Brief of ACLU et al., *supra* note 5, at 5.

[64] *Id.* at 5-6.

[65] *Id.* at 6.

[66] GARVIE ET AL., *supra* note 1, at 11.

[67] *Id.* at 57 (citing NAACP, Criminal Justice Fact Sheet (2009) ("A Black person is five times more likely to be stopped without just cause than a white person . . . 32% of the US population is represented by African Americans and Hispanic, compared to 56% of the US incarcerated population being represented by African Americans and Hispanics").

[68] *See* ELIZABETH HINTON ET AL., AN UNJUST BURDEN: THE DISPARATE TREATMENT OF BLACK AMERICANS IN THE CRIMINAL JUSTICE SYSTEM 2 (2018).

[69] GARVIE ET AL., *supra* note 1, at 56.

they are statistically more likely to be matched to a probe image when it is searched against an overwhelming number of Black faces.

In a study that examined the accuracy of a facial recognition software created by Amazon, the system misidentified twenty-eight members of Congress who were overwhelmingly people of color.[70]Amazon's "Rekognition" face recognition software used 25,000 publicly available arrest photos which resulted in false-positive matches for six members of the Congressional Black Caucus.[71] Among those members was the late "civil rights legend," John Lewis.[72] The *New York Times* labeled him a "towering figure of the Civil Rights Era" who "led one of the most famous marches in American history."[73] However, his longtime recognition on the national political stage had no bearing on the software that identified his face as a match to a convicted criminal. The test done on "Rekognition" revealed the shortcomings of facial recognition algorithms as opposed to the likelihood of a person identifying the face of an easily well-known political figure.

c. The Training Database

The alternative to mugshot enrollment databases also inadequately addresses the problem of racial bias. Most developers for facial recognition algorithms only have access to an open-source collection of images because of the time and cost required to create their own dataset.[74] The disadvantage of using open-source collections is that they are often limited in diversity.[75] A popular open-source dataset named "Labeled Faces in the Wild" was estimated to be comprised of 77.5% males and 83.5% white people.[76] When developers use open-source datasets like these, the algorithm quality is diminished because that dataset is not representative of real-world conditions that would encompass a diverse plethora of faces that the system would need to understand how to match.[77]

Lack of diversity in training sets that are used during the developing stages of facial recognition algorithms create a higher risk for overfitting. Overfitting is essentially "built-in racial bias."[78] An NIST study found that more diverse training data can be effective at reducing false positives.[79]

[70] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/EGC4-7TKR].

[71] *Id.*

[72] *Id.*

[73] Katharine Q. Seelye, *John Lewis*, *Towering Figure of Civil Rights Era, Dies at 80*, N.Y. TIMES (Aug. 4, 2020), https://www.nytimes.com/2020/07/17/us/john-lewis-dead.html [https://perma.cc/RA6T-KSUT].

[74] Open Data Science, *The Impact of Racial Bias in Facial Recognition Software*, MEDIUM (Oct. 15, 2018), https://medium.com/@ODSC/the-impact-of-racial-bias-in-facial-recognition-software-36f37113604c [https://perma.cc/9Y7N-DHDV].

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] GROTHER ET AL., *supra* note 6, at 71.

Conversely, the study found that false positives and false negatives likely resulted from a lack of demographic diversity in training data.[80] A "false positive" means that the algorithm matches the probe photo to an image in the database, but the match is incorrect.[81] A "false negative" is when the algorithm fails to match the probe image to an image that is, in fact, contained in the database.[82] Both of these errors should be avoided in facial recognition.

On the one hand, a criminal database mostly comprised of Black faces is problematic because it could lead to false positive matches disproportionate to the number of Black people in the system. Conversely, when an overwhelmingly white male database is used to train the algorithm, it makes it more difficult for the algorithm to accurately examine and match non-white people which also leads to false positives and negatives. In sum, the database that an image is being searched against must be diverse, but not overly representative of any one race or gender, and the database used to train the algorithm to work must be diverse enough so that it has the capacity to accurately examine a probe image regardless of race or gender.

d. The Match Threshold

Match thresholds are another variable that can impact algorithm accuracy in facial recognition. As previously mentioned, match thresholds are set values against which the algorithm compares its match score to determine if it has found a match to the probe image. The higher the match threshold, the fewer results produced, which garners a stronger possibility that the actual match will be missed by the system (creating a false negative).[83] On the other hand, the lower the threshold value, the more results produced (meaning a higher chance for false positives).[84] The threshold value has a significant impact on facial recognition results and therefore has the potential to create issues where the search should be more stringent or in instances where the goal of the search is to cast a wide net.[85] This algorithm component works in tandem with the skill of the analyst because a wider range of results would require more judgement from the person operating the system, while a narrower search return causes the analyst to rely more heavily on the algorithm accuracy as opposed to their own judgement.

e. Algorithm Accuracy for Intersectional Demographics

Numerous studies have been performed which reflect the low accuracy rates in facial recognition algorithms based on race, gender, age, and sexual orientation. An MIT researcher conducted an intersectional demographic and

[80] *Id.*
[81] Amici Curiae Brief of ACLU et al., *supra* note 5, at 6 n. 15.
[82] *Id.*
[83] P'SHIP ON AI, *supra* note 35, at 6.
[84] *Id.*
[85] *Id.* at 7.

phenotypic analysis on facial recognition algorithm accuracy.[86] The study classified subjects by phenotypic subgroup (dark-skinned females, light-skinned females, light-skinned males, and dark-skinned males) in order to test algorithm accuracy of race and gender classification simultaneously.[87] Because people have multiple identities that intersect and are not exclusive, such as white women or transgender Black men, it was important to test how algorithms perform when categorizing faces belonging to multiple classifications. Given the poor accuracy for algorithms when identifying Black people and women generally, it made sense that the poorest algorithmic accuracy was seen in dark-skinned women.[88] This study reflects the nuanced disparity in facial recognition among members of the same race.

C. Problems with Law Enforcement Use of Facial Recognition

Law enforcement mainly uses facial recognition for one of two purposes, facial verification or facial identification, the latter of which is most relevant for purposes of this Note.[89] Police use facial identification to identify unknown people in photos and videos.[90] Facial identification is used as an investigative tool by law enforcement.[91] Facial recognition is used to help police narrow leads on suspects, and once a suspect is identified, law enforcement and prosecution gather other incriminating evidence against that person to be used in court and in charging documents.[92] The inherent issue with using facial recognition during the investigative process is that it can be concealed because the police have no legal duty to disclose information about their investigations, and the prosecution only has to disclose what they plan to use for trial.[93]

Given all the factors that impact the accuracy of facial recognition, the biggest problem with law enforcement using it during investigation lies in the risk that police could misidentify a suspect during their investigation which then taints the entire case going forward. Although the police should further investigate a lead chosen by facial recognition, there is a concern that law enforcement relies too heavily on the technology to get an arrest. Because of a lack of standards for facial recognition and a lack of transparency surrounding its use in police departments, the risk for misidentification is high when police rely too heavily on this technology and no uniform standards exist to prevent its misuse.

[86] BUOLAMWINI, *supra* note 9, at 10.
[87] *Id.*
[88] *See id.*
[89] GARVIE ET AL., *supra* note 1, at 10.
[90] *Id.*
[91] Jackson, *supra* note 29, at 16.
[92] *Id.*
[93] *Id.*

The individuals who have been falsely arrested based on a bad facial recognition match focused on in this Note are all Black men.[94] The common thread throughout their cases were the steps that police took, or did not take, directly after facial recognition systems produced their pictures as matches to a suspect. These scenarios highlight the problematic nature of police use of facial recognition and how the veil of the investigatory stage insulates police departments from accountability.

The false arrest of Robert Julian-Borchak Williams is a perfect example of the faulty investigatory steps that police take when relying on equally faulty facial recognition technology. In October 2018, the Detroit Police Department (DPD), began an investigation into a store robbery committed by an unidentified Black man captured on surveillance footage.[95] Five months later, DPD ran the suspect's image through a facial recognition software which returned Williams as a match to the suspect.[96] Four months later, DPD showed a picture of Williams alongside five other pictures to a security guard who worked at the site of the robbery, and did not witness the robbery itself, but watched the surveillance footage from that day.[97] On the basis of this security guard's identification of Williams, DPD obtained an arrest warrant for him.[98] Six months later, DPD called Williams and told him to report to the station to surrender. When Williams refused to do so, DPD showed up at his house and arrested him.[99] He was interrogated and held for thirty hours until he was released on bail. Ultimately, the prosecutor dropped all charges at the probable cause hearing due to "insufficient evidence".[100] According to NPR, the use of facial recognition technology was disclosed on Williams' charging documents, so his lawyer had asserted that the system had falsely identified him.[101]

Another victim of facial recognition misidentification is Nijeer Parks, who was accused of shoplifting candy and trying to hit a police officer with a car in February 2019.[102] Much like the officers in the *Lynch* case, described in the following section of this Note, the police were unable to identify the man who they saw commit the crime when it occurred, so they sent a reference photo from the ID they retrieved at the scene to search using facial recognition software.[103] After the system produced Mr. Parks as a match, the officers

[94] *See generally* Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/Y9UA-QZ76]; Mak, *supra* note 18.

[95] Mayor, *supra* note 57.

[96] *Id.*

[97] *Id.* The security guard was not present at the armed robbery but was presented with the footage by police to help confirm the suspect that the facial recognition software had matched with the person in the video.

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] Hill, *supra* note 94.

[103] *Id.*

obtained a warrant.[104] When Parks' grandmother told him there was a warrant out for his arrest, he called the police station to clear up the mistake, but when he arrived, officers interrogated and arrested him.[105] Parks sat in jail for ten days while police failed to check for DNA or fingerprints to confirm that he was at the scene of the crime.[106] Swayed by his fear of the criminal justice system, Parks almost took a plea deal despite his innocence.[107] Parks' case was dismissed four months after his last hearing because he obtained proof that he was more than thirty miles away when the crime occurred.[108]

When comparing the incidents of facial recognition misidentification by police departments, there is a common theme of overconfidence in the results produced by these algorithms. Both the Detroit and New Jersey police departments employed limited checks before hotly pursuing the false matches of their searches. Neither of the cases went to trial, so most of the scrutiny rests on law enforcement's poor investigatory decisions and the part that they played in the false arrests of two Black men based on algorithm error. But, if these types of cases do go to trial, the next important question is whether courts will consider evidence of faulty facial recognition technology used during police investigations as "exculpatory" within the context *Brady*? This issue was brought to light for the first time when a defendant challenged the evidentiary standards for facial recognition in court, in *Lynch v. Florida*.[109]

D. Facial Recognition in Courts: Lynch v. Florida

On September 12, 2015, undercover officers bought cocaine from someone who called himself "Midnight."[110] One of the officers "used his cellphone to surreptitiously snap photos of Midnight during the transaction."[111] The officers sent the cell phone pictures, the name Midnight, and the address where the crime occurred to a crime analyst to find a name that matched the photos they had taken.[112] Sixteen days after the officers purchased the cocaine from Midnight, they received notification from the crime analyst of a match to the picture they sent.[113] The analyst testified that the program allowed her to filter the race and gender of the search to which

[104] *Id.*

[105] Elura Nanos, *Third Innocent Black Man to Be Misidentified by Facial Recognition Software Sues Police Department and Prosecutor for False Arrest and Imprisonment*, LAW & CRIME (Dec. 31, 2020), https://lawandcrime.com/civil-rights/third-innocent-black-man-to-be-misidentified-by-facial-recognition-software-sues-police-department-and-prosecutor-for-false-arrest-and-imprisonment/ [https://perma.cc/GNU3-7Z36].

[106] *Id.*

[107] *Id.*

[108] Hill, *supra* note 94.

[109] *See* Lynch v. State, 260 So. 3d 1166, 1170 (Fla. Dist. Ct. App. 2018).

[110] Benjamin Conarck, *How a Jacksonville Man Caught in The Drug War Exposed Details of Police Facial Recognition*, FLA.-TIMES UNION (May 26, 2017, 11:00 AM), https://www.jacksonville.com/news/metro/public-safety/2017-05-26/how-jacksonville-man-caught-drug-war-exposed-details-police [https://perma.cc/93PY-CYHS].

[111] *Lynch*, 260 So. 3d at 1168-69.

[112] *Id.*

[113] *See* Appellant's Motion for Rehearing and Written Opinion at 7, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

she input "Black male," and also narrowed the search to "Duval County booking photos".[114] That match was to a man named Willie Allen Lynch, who was later arrested for selling cocaine.[115]

At the pre-trial hearing, the crime analyst testified that she used the facial recognition program, FACES, to compare the photo of Midnight against other photos in a law enforcement database.[116] The analyst explained that the software would assign a number of stars indicating the likelihood of a match.[117] There were also other photos that the system returned as possible matches, but she only sent the officers a picture of Lynch along with his criminal history.[118] She admitted that she did not know how many stars were possible or what the number of stars meant, but that Lynch's photograph only had one star next to it.[119] Lynch did not learn that facial recognition was used to identify him until months after the trial began; this was during deposition of the investigators, as it was not mentioned in his arrest report.[120] The defendant filed a motion seeking to compel the State to produce the other photos that FACES returned—to which the court denied.[121] The court convicted Lynch and he was sentenced to eight years in prison.[122]

On appeal, Lynch argued that he should have had access to the other photos that FACES returned because they would have cast doubt on the State's case.[123] He contended that by not providing these photos, the State violated *Brady v. Maryland*.[124] The appellate court rejected this argument on the basis that Lynch failed to show that "there is a reasonable probability that the result of the trial would have been different if the suppressed documents had been disclosed to the defense."[125] The court reasoned that because his sole defense was misidentification, and the police wholly relied on the facial recognition system to identify him as "Midnight," he would need the other pictures to show he was not the suspect.[126] Lynch presented other arguments which were all rejected, and, subsequently, the trial court decision was affirmed.[127]

E. What Is the Brady Rule?

In *Brady*, the Supreme Court held that suppression of evidence favorable to the accused amounts to the denial of due process.[128] Under the

[114] *Id.* at 3.
[115] *Lynch*, 260 So. 3d at 1169.
[116] *Id.*
[117] *Id.*
[118] *Id.* at 1170.
[119] *Id.*
[120] Mak, *supra* note 18.
[121] *See Lynch*, 260 So. 3d at 1169.
[122] *Id.* at 1168.
[123] *Id.* at 1169-70.
[124] Brady v. Maryland, 373 U.S. 83, 87 (1963).
[125] *See Lynch*, 260 So. 3d at 1170.
[126] *Id.*
[127] *Id.* at 1172.
[128] *Brady*, 83 U.S. at 87.

Due Process Clause of the Constitution, the prosecution has a duty of disclosure if failing to do so would deprive the defendant of his right to a fair trial.[129] Although the Supreme Court has never classified facial recognition evidence as *Brady* material, many of the Court's decisions about the *Brady* doctrine create a framework to draw comparisons between traditional *Brady* material and facial recognition technology.[130]

In *Brady*, the Court held that the suppression of evidence favorable to an accused upon request violates due process where the evidence is "material either to guilt or punishment."[131] In that case, the petitioner was convicted of murder, but the State withheld a statement in which another individual admitted to committing the homicide.[132] While the Supreme Court noted that there was doubt in considering how much good the undisclosed confession would have done the defendant, the Court ultimately concluded that withholding the statement was prejudicial to the defendant, and, therefore, his due process rights were violated.[133]

The *Brady* Court sets forth a two-part test for whether the State is required to turn over evidence. The evidence in question must be (1) favorable to the defense and (2) material to the defendant's guilt or punishment.[134] Evidence is "material" when there is a "reasonable probability" that, if disclosed, the result of the proceeding would have been different.[135] A showing of materiality does not require demonstration by a preponderance of the evidence that disclosure of the suppressed evidence would have resulted ultimately in an acquittal.[136] Rather, the touchstone of materiality is whether in the absence of the evidence, the defendant has received a fair trial.[137] "*Brady* material" is defined as evidence that is materially exculpatory.[138] This means that the government's evidentiary suppression has undermined confidence in the outcome of the trial.[139]

"When the reliability of a given witness may well be determinative of guilt or innocence," nondisclosure of evidence affecting credibility falls within this general rule.[140] This principle, articulated in *Giglio*, represents the idea that evidence that impeaches a witness may constitute *Brady* material because it casts doubt on the guilt of a given defendant. Evidence that casts doubt on the reliability of the State's case against a defendant is "favorable" to the defense.

The *Kyles* case is instructive in determining whether a defendant has satisfied the materiality prong of the *Brady* test. In *Kyles*, the defendant was

[129] United States v. Agurs, 427 U.S. 97, 108 (1976).

[130] *See generally Brady,* 83 U.S. at 87; Giglio v. United States, 405 U.S. 150, 154 (1972); Kyles v. Whitley, 514 U.S. 419, 434 (1995).

[131] *Brady*, 83 U.S. at 87.

[132] *Id.* at 84.

[133] *Id.* at 88.

[134] *Id.* at 87.

[135] United States v. Bagley, 473 U.S. 667, 682 (1985).

[136] Kyles v. Whitley, 514 U.S. 419, 434 (1995).

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] Giglio v. United States, 405 U.S. 150, 154 (1972) (internal citation omitted).

tried and convicted of first-degree murder.[141] The Court found that the net effect of the evidence suppressed by the State amounts to a reasonable probability that its disclosure would have produced a different result.[142] Put differently, in answering the question of materiality, the Court considers all favorable evidence collectively, not separately. In *Kyles*, the Court held that the prosecutor was required to disclose evidence that the police ignored during their investigation because that evidence served to exculpate the defendant.[143]

III. FACIAL RECOGNITION EVIDENCE IS *BRADY* MATERIAL FOR A MISIDENTIFICATION DEFENSE

Evidence of police misuse of facial recognition and poor algorithm quality is *Brady* material for defendants alleging misidentification based on race or gender. For evidence to be classified as *Brady* material, the defendant must show that the evidence is both favorable and material.[144] To avoid the fundamental unfairness of police reliance on facial recognition technology that impacts racially vulnerable defendants, under the *Brady* rule, courts should require the prosecution to disclose its use. Once defendants are aware that facial recognition was used by police leading up to their arrest, there are two types of facial recognition evidence that warrants disclosure under *Brady*. Part III, Section A will show how evidence of faulty operation tactics committed by police using facial recognition qualifies as *Brady* material. Section B will describe how evidence of poor algorithm quality in facial recognition used by the police meets the *Brady* evidentiary standard.

A. Evidence of Poor Operating Choices Taken by Police Departments when Using Facial Recognition Qualifies as Brady Material

The previously mentioned incidents of Mr. Williams, Mr. Parks, and Mr. Lynch all illustrate real-world examples of what can go wrong at each stage of investigation, and later at trial, when facial recognition is involved. Most of these problems arose because there is no uniform standard for how police departments and analysts should use facial recognition technology to avoid issues that prove detrimental to the people they police.

1. Evidence Indicating Poor "Human Review"

The central issue with how police departments operate their facial recognition technology is a lack of training for the person reviewing the

[141] *Id.* at 421.

[142] *Id.* at 421-22.

[143] *See generally* Kyles v. Whitley, 514 U.S. 419, 446-48 (1995) (the police ignored a tip that the defendant had been framed, they disregarded evidence that supported this theory and the prosecution never disclosed this information to the defendant).

[144] *See generally* Brady v. Maryland, 373 U.S. 83, 87 (1963).

algorithm results or a complete absence of human review at all. Any evidence that demonstrates inadequate training for the person that reviewed the results of a facial recognition search is material and favorable to the defendant and is thus *Brady* material.

Evidence of poor personnel training is material to a misidentification defense because it is a crucial factor tied to the reliability of a facial recognition search. The reliability of facial recognition search results is comparable to the credibility of a witness called to identify a defendant in court. If there is evidence that undermines a witness' credibility whose testimony the government solely relies on for their case, that witness' credibility becomes an important issue of the case as a whole.[145] Like in *Lynch*, the prosecution and police based their identification of the defendant solely on his match that was produced by FACES and thus any evidence undermining the reliability of that match is a material issue of his case.

Along with being material, the evidence must also be favorable to the defendant to satisfy *Brady*.[146] An example of favorable evidence concerning poor personnel training was when the crime analyst in *Lynch v. Florida* admitted to not knowing how to interpret the results presented by the facial recognition software used to identify Lynch.[147] The analyst's lack of understanding the system indicates that she was never properly trained to evaluate the algorithm and account for possible error. A government study stated that when the operator of a facial recognition software has some personal qualification for facial identification, the system is more likely to lead to accurate results.[148] But if an analyst has no personal qualification to operate a system, it tends to undermine the quality of the results produced by that system and thus bolsters the case for misidentification. Poor personnel training is both material and favorable to a misidentification defense, and thus should qualify as *Brady* material.

2. Evidence of Police Overreliance on Facial Recognition Technology

Police misconduct during the investigation is favorable for the defendant. In *Kyles*, the police ignored a tip that the defendant had been framed, they disregarded evidence that supported this theory, and the prosecution never disclosed this information to the defendant.[149] Similarly, in the false arrest of Nijeer Parks based on a bad facial recognition search, the

[145] *Giglio*, 405 U.S. at 154-55 ("the Government's case depended almost entirely on Taliento's testimony; without it there could have been no indictment and no evidence to carry the case to the jury. Taliento's credibility as a witness was therefore an important issue in the case").

[146] *See Brady*, 83 U.S. at 87.

[147] Amici Curiae Brief of ACLU et al., *supra* note 5, at 20.

[148] *See* P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PROC. NAT'L ACAD. SCI'S. 6172 (June 12, 2018), https://www.pnas.org/content/pnas/115/24/6171.full.pdf [https://perma.cc/FXH2-4VVY].

[149] *See* Kyles v. Whitley, 514 U.S. 419, 420 (1995).

police skipped vital steps in the investigatory process, leading to the detention of Mr. Parks. The police obtained a search warrant, interrogated, and jailed Parks for ten days without taking any further precautions to confirm that he was the correct suspect. The culmination of evidence showing a lack of diligence taken by the police, coupled with overreliance on one fallible identification is much like the faulty investigation described in *Kyles*. Under *Brady*, the court evaluates the net value of favorable evidence to the defendant and decides whether its disclosure would have undermined the outcome of the case.[150] If Parks' case would have gone to trial, the evidence describing the lack of diligence taken by the police after obtaining a false match would have been both material and favorable to his defense.

B. *Evidence of Poor Algorithmic Quality Constitutes* *Brady* *Material*

Prosecutors should be required to disclose the use of facial recognition as *Brady* material where the system was the only identification mechanism the witness relied on to identify a suspect. When facial recognition technology has matched a Black, brown, or female defendant, it may be enough to satisfy both the "material" and "favorable" *Brady* elements. Given the aforementioned empirical evidence that facial recognition systems are disproportionately unreliable at identifying minorities and women, those defendants are entitled to access information about the algorithm used to identify them, especially when it is the only evidence on which the government and police relied.

Usually only the police and prosecution know when facial recognition technology has been used to identify a defendant.[151] This fact is especially problematic when a match by a facial recognition software is the sole basis on which the police rest their identification; if the algorithm was flawed, the defendant has no way of knowing why they were identified. Further, the defendant then has no way of challenging it in court with evidence unless it has been disclosed under *Brady*.

1. The Name of the Algorithm

The name of the algorithm used to identify a defendant is the first step in the discovery process that attorneys must take in order to reveal algorithmic flaws made in the development of the facial recognition software. Although the company name alone is not likely to be exculpatory to the defendant, it is the first piece of evidence necessary for a misidentification defense to cast doubt on the quality of the facial recognition technology used. Without the name of the company, an attorney may not be able to find any more evidence informing the quality of the technology.

[150] *Brady*, 83 U.S. at 87.

[151] Jackson, *supra* note 29, at 16.

The facial recognition error rates of companies such as Microsoft, Facebook and IBM have been published in academic studies.[152] If the name of the algorithm is disclosed, the defense could present evidence about that system to cast doubt on its accuracy towards people of color and women. If the defendant falls within a class of regularly misidentified people by that algorithm, this evidence would be "material to either guilt or punishment."[153] For example, if a Black defendant has been identified using "Amazon Rekognition," evidence of that company's history of misidentification of people of color would lead to a "reasonable probability" that the algorithm results may be wrong. This is the touchstone for *Brady* material.[154]

2. Other Matches Produced by the Algorithm

The other matches returned in a search is evidence that qualifies as *Brady* material. The other matches produced by an algorithm are exculpatory in nature because they cast doubt on the identification of the defendant as the suspect. When there are other possible suspects to a crime, the existence of those suspects serves to cast doubt on whether the defendant was correctly identified.[155] This can be likened to *Kyles*, where the government suppressed evidence of other suspects which may have changed the outcome of the case had they been admitted into evidence.[156]

The presence of other matches in the system works to contradict the reliability of the witness that identified the defendant. The admission of contradictory evidence satisfies the impeachment requirement of evidence that would constitute *Brady* material. Contradictory evidence would likely change the outcome of the case, and, thus, satisfies the "reasonable probability" prong for *Brady* evidence.

3. The Confidence Scores of Other Matches Produced

The confidence scores of the other matches should constitute *Brady* material if the scores are high because they could cast doubt on the positive identification of the defendant.[157] High confidence scores for other suspects that were ignored by police in the identification process undercuts the quality of the investigation that was conducted in identifying the defendant. If the defendant shapes their argument around misidentification, evidence that informs the method that police took to identify the defendant is material to the outcome of the case. A misidentification defense relies on the quality of the identification procedure, so when that procedure is called into question,

[152] Najibi, *supra* note 8.

[153] Brady v. Maryland, 373 U.S. 83, 87 (1963).

[154] *Kyles*, 514 U.S. at 420.

[155] *See id.* at 447.

[156] *Id.*

[157] OPEN TECHNOLOGY INSTITUTE ET AL., CIVIL RIGHTS CONCERNS REGARDING LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY 5, n.26 (2021), https://newamericadotorg.s3.amazonaws.com/documents/FINAL_Civil_Rights_Statement_of_Concerns_LE_Use_of_FRT_June_2021.pdf [https://perma.cc/BM8U-X8GW].

there is a reasonable probability that it can change the outcome of a case. The crux of these arguments lies in the question of whether the facial recognition software was the witness' sole reason for identifying the defendant as the suspect.

4. The Probe Photo Used to Conduct the Search

The probing photo would qualify as Brady material for two reasons: (1) if the probing photo used in a facial recognition system is of poor quality, or (2) if the probe image has defining characteristics that undermine comparison to the defendant.[158] Both of these scenarios make this evidence material to the case and possibly exculpatory.

As explained above, a poorly lit, positioned, or pixilated image run through a facial recognition search comes with a higher possibility of inaccuracy.[159] Evidence of a poor probe image is material to the defendant's misidentification case because it could serve to support the argument that a faulty search was committed. The quality of the search is an important issue in a case in which the police rely solely on the facial recognition search to identify a suspect.

The second reason the probe image could be *Brady* material is because that photo could create doubt among members of the jury regarding whether the defendant is in fact the correct suspect. The touchstone of materiality is a "reasonable probability" of a different result, and the adjective is important. A "reasonable probability" of a different result is accordingly shown when the government's evidentiary suppression undermines confidence in the outcome of the trial.[160] If a photo is shown to the jury that would cast doubt on whether the defendant is the correct suspect, there is a strong possibility that the outcome of the trial may change. If the probe photo does not favor the defendant, that piece of evidence would also be exculpatory towards the defendant, thereby rendering it *Brady* material.

C. Facial Recognition Ensures Fair Treatment: It Is Not a Governmental Burden

Because facial recognition is so widely used by police departments in the U.S., some would argue that automatic disclosure and access to the details of its usage may impose too much of a burden on the government. However, given that facial recognition in federal criminal proceedings and investigations is ungoverned by any law, there are no better safeguards to ensure fair treatment under this technology. Until this area is regulated, the courts need to protect defendants' constitutional rights to a fair trial. Some may argue that because the evidence may only be exculpatory for criminal

[158] ROGER RODRIGUEZ, FACIAL RECOGNITION: ART OR SCIENCE? 9, https://www.sheriffs.org/sites/default/files/Whitepaper%20Facial%20Recognition.pdf [https://perma.cc/XK97-TG62].

[159] Amici Curiae Brief of ACLU et al., *supra* note 5, at 5.

[160] *United States v. Bagley*, 473 U.S. 667, 678 (1985).

defendants of a specific race and/or gender, the need for disclosure to all defendants is not necessary. However, *Brady* material is assessed on factors within an individual case, and, thus, if the details of facial recognition are not relevant to a given defendant, then disclosure would not be required. This Note focuses on cases where the technology impacts the defendant negatively.

IV. CONCLUSION

In conclusion, use of facial recognition technology should be disclosed where the defendant could be exonerated given the nature of the facial recognition technology relied on by police. If Mr. Lynch was notified that the police solely relied on FACES to identify him during pre-trial discovery instead of eight days prior to his pretrial conference, he would have had a better opportunity to formulate his misidentification defense.

The purpose of the *Brady* rule is to ensure that defendants receive a fair trial and in order for a trial to be fair, they must have a chance to defend themselves based on any existing evidence that could aid their defense. If the prosecution withholds this evidence, a defendant will have no chance at a fair trial and could lose their liberty without ever receiving adequate due process. Due process is a constitutional right, and it should be treated with great importance. Until there are national standards set to improve the accuracy of facial recognition technology for all people, not just those that the technology does not negatively impact, defendants should have a right to access evidence regarding how that technology may have been the cause of police misidentification.

Building Blocks of Privacy: Why the Third-Party Doctrine Should Not Be Applied to Blockchain Transactions

Veronica Lark*

TABLE OF CONTENTS

[*] J.D., May 2022, The George Washington University Law School; B.A., English, May 2016, Lourdes University. I would like to thank Professor Ethan Lucarelli and Olivia Creser for their mentorship in the drafting this Note. Thank you as well to Professor Daniel Solove for his feedback on the privacy issues raised by my topic, and to Professor Douglas Pepe for his guidance concerning the technical aspects of this paper.

I. INTRODUCTION

In early 2018, twenty-three million users logged onto Coinbase, presumably to confirm how much Bitcoin had spiked in price or maybe to swap their Ethereum for Litecoin.[1] For months leading up to this, people were swarming to cryptocurrency exchanges like Coinbase to see "blockchain" in action. Many were told—by friends, acquaintances, their boss—a brief elevator pitch about cryptocurrency along the lines of: "cryptocurrency is the cash of the future!" or "blockchain works without any third party, so that means your finances are more secure, since no one can tell who you are based on the digits that get stamped into the blockchain." To the millions who signed up for a Coinbase account, cryptocurrency may have represented a libertarian solution to the encroachment of large financial institutions. To others, it was an opportunity to engage in criminal behavior, thinking that the blockchain could conceal it.

In the context of recent court decisions in which defendants claimed privacy rights for data records stored on the blockchain, consumers may be surprised to learn that cryptocurrency exchanges like Coinbase are not legally viewed any differently than other financial institutions and intermediaries.[2] When individuals transact with third-party entities, such as using a bank to wire money, courts have held that individuals lose any privacy interest in the data they have shared because (1) it was shared voluntarily, and sharing voluntarily means that the individual assumes the risk of the information being shared with the government, and (2) the individual does not own the business record.[3] This legal concept is known as the third-party doctrine. The result is that third parties like banks do not need to be presented with a search warrant before they turn over client records.[4] This legal reality extends into digital space, applying to those types of transactions conducted via credit card on third-party applications like Apple Pay and Venmo.[5]

Additionally, this legal reality implicates blockchain transactions.[6] However, there is a critical distinction between a blockchain and a third-party cryptocurrency exchange like Coinbase. A blockchain has no third-party intermediary—it is a digital ledger—in contrast with a cryptocurrency

[1] *See Global Number of Verified Coinbase Users from 1st Quarter of 2018 to 4th Quarter of 2020*, STATISTA (Mar. 2021), https://www.statista.com/statistics/803531/number-of-coinbase-users/ [https://perma.cc/9ETB-JE8L].

[2] *See* Zietzke v. United States, No. 19-cv-03761, 2020 WL 264394, at *13 (N.D. Cal. Jan. 17, 2020); United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020).

[3] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[4] *See Smith*, 442 U.S. at 745-46.

[5] *See generally* Dina Moussa, *Protecting Payment Privacy: Reconciling Financial Technology and The Fourth Amendment*, 1 GEO. L. TECHNOLOGY REV. 342, 344-45 (2017).

[6] *See generally Zietzke*, 2020 WL 264394 at *13; *Gratkowski*, 964 F.3d at 312-13.

exchange which serves essentially as a cryptocurrency brokerage.[7] Even though the blockchain and exchange are two distinct entities, law enforcement has successfully subpoenaed the Coinbase exchange with knowledge of recipient addresses: using this information to track down the accounts that sent cryptocurrency.[8] Cryptocurrency exchanges possess personal identification information for account holders, but this information does not carry over to a blockchain transaction;[9] at this point, this distinction does not prevent law enforcement from subpoenaing cryptocurrency exchanges when searching for account holders' information that may be connected to a given blockchain transaction even when the search is speculative and not based on probable cause.[10] In *U.S. v. Carpenter*, the Supreme Court recognized a privacy interest for a specific emerging technology, cell site location information (CSLI).[11] As another form of an emerging technology, blockchain should fit within the framework used by the Supreme Court in *Carpenter*. Even though the blockchain reveals cryptocurrency transactions to the public, the technology that allows for this revelation of data does not reveal the personally identifiable information shared with the cryptocurrency exchange: there is a distinction between the exchange's business records and the blockchain transaction.[12] The blockchain ledger is not a third-party intermediary, and, thus, any request issued to a cryptocurrency exchange to acquire accountholder information based on separate decentralized ledger transactions should require that law enforcement acquire a search warrant. Once law enforcement has identified a unique public address engaging in fraudulent or illegal transactions recorded in the blockchain ledger, this should require law enforcement to present a search warrant to a cryptocurrency exchange to obtain the records, since law enforcement does not yet have the requisite reasonable suspicion of a particular accountholder,

[7] *See What's the Difference Between Coinbase.com and Coinbase Wallet?*, COINBASE, https://help.coinbase.com/en/wallet/getting-started/what-s-the-difference-between-coinbase-com-and-wallet (last visited Oct. 20, 2021); *see also* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV., Jan.-Feb. 2017, https://hbr.org/2017/01/the-truth-about-blockchain [https://perma.cc/XV6G-7N66].

[8] *See Gratkowski,* 964 F.3d at 309.

[9] *See Data Privacy at Coinbase*, COINBASE, https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/what-is-the-gdpr (last visited Oct. 20, 2021); *see also What is a Transaction Hash/Hash ID?*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-a-transaction-hash-hash-id (last visited Oct. 20, 2021).

[10] *See Gratkowski*, 964 F.3d at 309.

[11] *E.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[12] *See Public and Private Keys*, BLOCKCHAIN.COM SUPPORT, (Dec. 29, 2021, 6:21 AM), https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys (an individual's address is "a shorter, representative form of the public key" which is visible in a blockchain transaction and can be "derived using a known algorithm").

and they will not know the accountholder's identity until the exchange turns over its relevant records.[13]

Part II lays out the factual background necessary to understand blockchain, cryptocurrency, and cryptocurrency exchanges. Part III assesses the origins of privacy law, the evolution of the third-party doctrine, and the application of the third-party doctrine in blockchain cases. Part IV proposes and analyzes why the distinction between blockchains and cryptocurrency exchanges is critical in third-party doctrine analysis. Part IV, Section A presents the basis for finding a privacy right in blockchain data in the context of *Carpenter*. Part IV, Section B looks at the distinction made between publicly revealed information and private information, and positions blockchain and cryptocurrency exchanges within this framework. Part IV, Section C proposes that law enforcement should be required to obtain a search warrant when seeking account information possessed by a cryptocurrency exchange. Part V presents potential solutions using both the court system and Congress, and also asserts why the blockchain/cryptocurrency exchange distinction does not overextend *Carpenter* and responds to potential issues concerning actors who will try to evade criminal liability based on the blockchain/cryptocurrency exchange distinction. Part VI concludes this analysis.

II. BLOCKCHAIN, CRYPTOCURRENCY, AND CRYPTOCURRENCY EXCHANGES

This section provides a basis for understanding the components of a blockchain such as the decentralization of the blockchain, the nature of the ledger, and how cryptocurrency fits into this system. This section also explains the anonymity and permanence of cryptocurrency transactions and how a public transaction effectuates these qualities. This section also explains the technical qualities of a cryptocurrency exchange and how an exchange exerts control over users.

A. A Blockchain Is a Decentralized Public Ledger Allowing for the Execution and Storage of Cryptocurrency Transactions

Blockchain is a decentralized network comprised of a system of computer node participants that record transactions on a shared, immutable

[13] *See id.*; *see also* Tyler G. Newby & Ana Razmazma, *An Untraceable Currency? Bitcoin Privacy Concerns*, FINTECH WKLY., (Apr. 7, 2018), https://fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns [https://perma.cc/TMX4-BQ6Z]; *Reasonable Suspicion*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/reasonable_suspicion ("Reasonable suspicion is used in determining the legality of a police officer's decision to perform a search." Law enforcement does not have reasonable suspicion that a given accountholder is connected to a crime; they just have information about the digits identifying a specific account) [https://perma.cc/Q4T8-XMH8].

ledger.[14] Blockchain technology does not require a centralized third party, like a bank, to complete and store transactions; all participants share ownership of records so that no one user has full control.[15] The blockchain ledger is distributed because multiple computer nodes have authority to update the record on the ledger; there is no centralized party in control.[16] The nodes are essentially a network of computers that compete to complete mathematical equations under a given consensus protocol, and the computer that does this this computation correctly, and the most quickly, posts the entry into the ledger, thus adding a new block to the chain.[17] The "blocks" added to the ledger per transaction are immutable, in that with time it becomes computationally and economically impractical to reverse transactions, unlike the ease with which a transaction can be reversed or refunded in the traditional sense of being able to cancel a payment on a credit card.[18] A more accessible analogy in understanding the blockchain would be to imagine a web of computers that all have access to the same Google spreadsheet, and whenever a transaction occurs, it is entered into the spreadsheet after each participant races to complete a computation that confirms the validity of the transaction on the shared spreadsheet.[19] The spreadsheet entry cannot be edited and it is visible to everyone with access.[20]

Key for the purposes of this Note's analysis is whether a blockchain is public, private, hybrid, or permissioned, which will determine how much information parties implicitly share with others as a result of a transaction.[21] These distinctions essentially determine how transactions are fulfilled by a consensus to post transactions to the ledger.[22] Consensus varies in these circumstances and essentially involves mathematical computing to allow for digital entry of a transaction.[23] These types of chains allow different levels of participation in consensus and access to the ledger, but consensus does not equal ownership.[24] A public blockchain allows any participating computer to help reach consensus of a transaction; private blockchains allow only a portion of the participating computers to be part of the consensus; a hybrid blockchain allows the same level of participation as a public blockchain, but there are designated nodes that are the only ones to input a block; a permissioned blockchain is even more restrictive than a private blockchain,

[14] *See* Ashley N. Longman, *The Future of Blockchain: As Technology Spreads, it May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 118-19 (2019).

[15] *See* Iansiti & Lakhani, *supra* note 7.

[16] *See* Brittany Manchisi, *What is Blockchain Technology?*, IBM: SUPPLY CHAIN & BLOCKCHAIN BLOG (July 31, 2018), https://www.ibm.com/blogs/blockchain/2018/07/what-is-blockchain-technology/ [https://perma.cc/C65D-2B8V].

[17] *See* Suyash Gupta & Mohammad Sadoghi, *Blockchain Transaction Processing*, *in* ENCYCLOPEDIA OF BIG DATA TECHNOLOGIES 2-3 (2018).

[18] *See* Zibin Zheng et al., *Blockchain Challenges and Opportunities: A Survey*, 14 INT'L J. WEB & GRID SERVS. 352, 357 (2018); *see also* Longman, *supra* note 14, at 119.

[19] *See* Zheng, *supra* note 18, at 354-55.

[20] *See id.*

[21] *See* Gupta & Sadoghi, *supra* note 17, at 3.

[22] *See id.*

[23] *See id.*

[24] *See id.* at 3-4.

and allows only a certain select group of computer nodes to participate in the consensus process.[25] Each node participant has its own copy of the ledger, which is constantly updated with new transaction entries; this distribution of the ledger makes it difficult for any one party to alter past data entries.[26] These different levels of permission and access are also wholly separate from the discussion of the cryptocurrency exchange: where transactions are buys and sells that are fulfilled by the cryptocurrency exchange and maintained in accounts owned by the exchange, and this transaction history and account information is accessible as business records.[27]

B. *Cryptocurrency Transactions Are Anonymous and Publicly Recorded in a Permanent Digital Ledger by Function of the Blockchain*

In cryptocurrency transactions, there are three components in a given entry input to the blockchain ledger: the transaction amount, the proof that the sender has the ability to send that amount, and the recipient's address.[28] Transactions occur on the blockchain through the use of a private and public key.[29] The private key is essentially a signature that is known only to the user that allows a cryptocurrency transaction to initiate; it allows a user to send cryptocurrency to another user.[30] The sender creates a transaction, signs the transaction, and broadcasts it "to the network for validation."[31] Nodes then "verif[y] that indeed your private key corresponds to the provided public key" and confirm the transaction.[32] The public key has a mathematical relationship to the private key, such that proof of ownership of the public key can be

[25] *See id.*

[26] *See* Longman, *supra* note 14, at 121-22.

[27] *See* Jake Frankenfield, *Bitcoin Exchange*, INVESTOPEDIA (Aug. 9, 2021), https://www.investopedia.com/terms/b/bitcoin-exchange.asp [https://perma.cc/V96D-SPAA]; *see also What's a Bitcoin Exchange?*, BITCOIN.COM https://www.bitcoin.com/get-started/how-bitcoin-exchange-works/#2 (describing the "custodial" nature of cryptocurrency transactions on exchange platforms like Coinbase) [https://perma.cc/2S9R-PERY].

[28] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

[29] *See* Zheng et al., *supra* note 18, at 356.

[30] *See* Jake Frankenfield, *Public Key*, INVESTOPEDIA (June 24, 2021), https://www.investopedia.com/terms/p/public-key.asp [https://perma.cc/GZR8-F9PC].

[31] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

[32] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

revealed without revealing the private key.[33] The public key is converted into hash code which is a visible public address entered as a component of the ledger entry.[34] The scrambled sender address combined with the recipient's public key allows the transaction to proceed, and the entry is added to the blockchain where it is visible to everyone with access.[35] In the realm of cryptocurrency exchanges, Coinbase is a broker and holds its own private keys and maintains a database allocating transactions to its users; as such, a Coinbase user does not possess actual private keys for use of transacting on the blockchain.[36]

Whether a user is using Coinbase or a decentralized blockchain directly, they are not relaying their identity during a transaction.[37] A cryptocurrency exchange functions like a stock or commodities market, and the exchange essentially fulfills a buy or sell order for a certain amount.[38] The transaction is also functionally anonymous between buyer and seller, but the cryptocurrency exchange is subject to Know Your Customer (KYC) laws that require the exchange to maintain personally identifiable information about its customers.[39] All that is traded is currency for currency: BTC for USD.[40] The operations are distinct from when users of an exchange then take their cryptocurrency holdings and transact them as payment for a good or service with a seller on a public blockchain.[41] This money can be transferred from the exchange held wallet to a seller, to a different exchange, or to a different type of wallet: online or offline where KYC laws might be different.[42]

C. A Cryptocurrency Exchange is a Third-Party Broker

A cryptocurrency exchange is an entity which issues exchange accounts to users who then buy and sell cryptocurrency on the blockchain using the exchange as a "broker" to make those trades.[43] A third-party operated cryptocurrency exchange is not the most ideal use case of blockchain

[33] *See* Jake Frankenfield, *Private Key*, INVESTOPEDIA (Nov. 27, 2021), https://www.investopedia.com/terms/p/private-key.asp [https://perma.cc/DWU6-3LJ7].

[34] *See* Frankenfield, *supra* note 30.

[35] *See* Longman, *supra* note 14, at 121.

[36] *See Data Privacy at Coinbase*, COINBASE, https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/what-is-the-gdpr (last visited Feb. 27, 2021); *What Is a Private Key?*, COINBASE, https://www.coinbase.com/learn/crypto-basics/what-is-a-private-key (last visited Apr. 3, 2021).

[37] *See* Frankenfield, *supra* note 30.

[38] *See generally What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[39] *See* Longman, *supra* note 14, at 120; *see also* Newby & Razmazma, *supra* note 13.

[40] *See generally What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[41] *See* Toshendra Kumar Sharma, *Five Differences Between an Exchange and a Blockchain*, BLOCKCHAIN COUNCIL, https://www.blockchain-council.org/blockchain/five-differences-between-an-exchange-and-a-blockchain/ [https://perma.cc/ERV9-PVTN].

[42] *See* Newby & Razmazma, *supra* note 13.

[43] *What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

technology.[44] Blockchain was designed to do away with third parties, but one needs technological wherewithal to transact on the blockchain without the help of an intermediary.[45] In this sense, exchanges fill that technological void, and help bring blockchain directly to consumers. Coinbase.com states that its role is as a "cryptocurrency brokerage where you buy or sell cryptocurrency in exchange for fiat currency."[46] While using the exchange, individuals can trade fiat currency like the USD for cryptocurrency or make trades between cryptocurrencies.[47] When an individual opens an account with an exchange, they share private data with the exchange, which implicitly links their personal account data to every transaction executed using the exchange.[48]

In addition, the user's public and private keys are not owned by the user, but by the cryptocurrency exchange.[49] Because of this lack of ownership, a user of an exchange account technically does not even own the cryptocurrency held on their account.[50] A cryptocurrency exchange can be one of many ways that cryptocurrency holders transact in cryptocurrency and keep their cryptocurrency holdings.[51] If someone holds their cryptocurrency on the exchange, the ownership interest is not clear since the exchanges are third-party intermediaries that maintain ownership of the wallet keys to users' private exchange accounts.[52] As financial institutions, cryptocurrency exchanges have responsibilities under the Bank Secrecy Act to collect certain forms of data, create reports on suspicious behavior, and to turn over suspicious information to law enforcement or the government.[53] Additionally, in order to access account data held by a cryptocurrency exchange, law enforcement only needs to obtain a court order or subpoena rather than a search warrant based on probable cause.[54]

[44] *See* Cassiopeia Services, *Challenges and Issues in Cryptocurrency Trading: Beyond the Controversies*, MEDIUM (Feb. 28, 2019), https://cassiopeiaservicesltd.medium.com/challenges-and-issues-in-cryptocurrency-trading-beyond-the-controversies-12bebb7c3849 (the centralization of risk in cryptocurrency exchanges works against the broader goals of decentralization).

[45] *See* United States v. Gratkowski, 964 F.3d 307, 312-13 (5th Cir. 2020).

[46] *What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[47] *See* Frankenfield, *supra* note 27; *see also* James Chen, *Fiat Money*, INVESTOPEDIA (Oct. 26, 2021), https://www.investopedia.com/terms/f/fiatmoney.asp (Fiat is currency that is backed by the issuing government rather than a physical commodity) [https://perma.cc/F6Z4-DH7R].

[48] *See* Longman, *supra* note 14, at 132-33.

[49] Cryptopedia Staff, *What Are Public and Private Keys?*, CRYPTOPEDIA, (Sept. 8, 2021), https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-where-are-my-private-keys [https://perma.cc/5TNT-2QTH].

[50] *See Gratkowski*, 964 F.3d at 312; *see* Cryptopedia Staff, *supra* note 49.

[51] *See generally* Paxful Team, *What Is a Paper Wallet?*, PAXFUL: BLOG (May 27, 2020), https://paxful.com/blog/bitcoin-paper-wallet/ [https://perma.cc/HBT3-PVHD].

[52] *See* Cryptopedia Staff, *supra* note 49.

[53] *See* Christopher Lloyd, *The Privacy Revolution Begins: Did* Carpenter *Just Give Bitcoin Users a Chance to Strike Down the Bank Secrecy Act?*, 88 GEO. WASH. L. REV. 204, 215-16 (2020).

[54] *Id.* at 217.

III. THE CHAIN OF PRIVACY LAW: FROM MAILBOXES TO CRYPTOCURRENCY EXCHANGES

This section describes the purpose of the Fourth Amendment, early Fourth Amendment case law, and how the third-party doctrine evolved when individuals claimed a privacy interest in data held by third parties. This section also presents the modern application of the third-party doctrine in emerging technology cases as well as recent case law assessing the third-party doctrine's application to cryptocurrency exchanges.

A. The Foundation of the Fourth Amendment and Evolution of the Third-Party Doctrine

The Fourth Amendment protects the rights of citizens to keep certain information private and away from the government.[55] Early Fourth Amendment jurisprudence drew distinctions between information that was voluntarily revealed to the public, and information that was kept private.[56] This evolution eventually created the standard conveyed in the third-party doctrine which limits privacy expectations when an individual voluntarily shares information with a third party.[57]

The Fourth Amendment is the grounding principle when determining circumstances under which the state can access private transactional information.[58] The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[59]

The Fourth Amendment was born out of a skepticism and dislike of the British government's use of the general warrant in obtaining access to houses, papers, and effects through search and seizure.[60] The general warrant required a low bar for access, and the result was "unreasonable searches and seizures."[61] The Fourth Amendment departed from this standard by requiring a "probable cause" showing before issuing a warrant.[62]

[55] *See* Ex parte Jackson, 96 U.S. 727, 733 (1877) (the information at issue being sealed letters).

[56] *See id.*

[57] *See* United States v. Miller, 425 U.S. 435, 443 (1976).

[58] *Id.* at 444.

[59] U.S. CONST. amend. IV.

[60] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[61] Paul Belonick, *Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 STAN. TECHNOLOGY L. REV. 114, 169 n.345 (2020).

[62] *Id.* at 180.

Early Fourth Amendment jurisprudence attempted to define how the amendment applied in settings involving searches and seizures.[63] In *Ex parte Jackson*, the Court articulated a standard for search and seizure when it came to letters, creating a distinction between content and envelope, specifically that the envelope contained address and directional information, and that content information was the letter within.[64] The content inside was protected from search and seizure, and the address information outside of the envelope did not have the same protections because it was necessary for transferring the letter.[65] Later on, *Katz v. U.S.* fleshed out the "unreasonable" element in the Fourth Amendment test by articulating a "reasonable expectation of privacy" in Fourth Amendment analysis, meaning that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[66] This expectation of privacy test affirms that there may be things revealed to the public in which one retains a privacy right.[67]

The development of the third-party doctrine followed *Katz* and was first articulated in *U.S. v. Miller*, a case concerning whether a bank client had a privacy interest in his checks used at a banking institution; the Court held that checks are "negotiable instruments" used in business, and the customer assumes the risk of having that information shared by engaging in the transaction.[68] The Court mentioned that:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to the Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[69]

This means that when conducting personal business with a bank, a client has no "expectation of privacy" in that data.[70]

[63] *See* Ex parte Jackson, 96 U.S. 727, 733 (1877); *see e.g.*, Belonick, *supra* note 61, at 151-53.

[64] *See Jackson*, 96 U.S. at 732-33.

[65] *See* DANIEL SOLOVE, NOTHING TO HIDE 94 (2011) (explaining generally how secrecy is equated with privacy and defining this as the "secrecy paradigm"); *see, e.g.*, Belonick, *supra* note 61, at 148-51 (Belonick presents the "content/noncontent" and "inside/outside" distinctions in relation to letters and more broadly that the "inside" and "content" of materials is where the privacy interest lies).

[66] Katz v. United States, 389 U.S. 347, 360-61 (1967).

[67] *See id.* at 351-52.

[68] United States v. Miller, 425 U.S. 435, 442-43 (1976).

[69] *Id.* at 443.

[70] *Id.* at 449.

Smith v. Maryland used this same "expectation of privacy" test in the context of pen registers.[71] Pen registers collect a record of the phone numbers being dialed between lines, but they are not able to pick up the content of the calls being tracked.[72] Phone companies maintain the records of these calls, so an individual does not have any real control over this data collection.[73] *Smith* held that because the content of the communications on the phone call was not at issue there is no expectation of privacy in the log of calls created by the pen register and thus a warrant was not needed for law enforcement to obtain the data.[74]

These two cases reaffirm the standard for third-party transactions specifying that there is no reasonable expectation of privacy in information voluntarily shared with a third party.[75] This logic has persisted even as third parties have become more abstract and exist only as banking apps and credit cards that appear only tangentially connected to the entities they proceed from.[76] Under this doctrine, the government or law enforcement has much more ease in acquiring information.[77] There is no need for a warrant showing probable cause, only a written request, a court order, or a subpoena—meaning that fewer limitations are placed on the government or law enforcement preventing them from searching and seizing data related to these consumer transactions.[78]

B. *There Is Mixed Treatment of Emerging Technologies Under the Third-Party Doctrine*

The third-party doctrine applies in the realm of credit cards: cases have held that that there is no reasonable expectation of privacy in a credit card number.[79] However, in the realm of developing technologies, the Supreme Court has applied the third-party doctrine and the Fourth Amendment warrant requirement with different results.[80] In *U.S. v. Jones*, a case concerning

[71] Smith v. Maryland, 442 U.S. 735, 740-41 (1979). A pen register is a "device or process that traces outgoing signals from a specific phone or computer to their destination . . . [and] produces a list of the phone numbers or Internet addresses contacted, but does not include substantive information transmitted by the signals." *Pen Register*, CORNELL L. SCH: LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/QF6Q-SVSG].

[72] *Smith*, 442 U.S. at 741.

[73] *Id.* at 742.

[74] *Id.* at 741, 745-46.

[75] *See generally id.*; *Miller*, 425 U.S. at 442-44.

[76] *See* United States. v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *11 (S.D. Fla. Oct. 24, 2009); United States v. DE L'Isle, 825 F.3d 426, 432 (8th Cir. 2016).

[77] *See* Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECHNOLOGY L. REV. 401, 402 (2015); Lloyd, *supra* note 53, at 217.

[78] Lloyd, *supra* note 53, at 217.

[79] *See Medina*, 2009 WL 3669636 at *11 ("the credit card holder voluntarily turns over his credit card number every time he uses the card"); *DE L'Isle*, 825 F.3d at 432 ("when the holder uses the card he 'knowingly disclose[s] the information on the magnetic strip of his credit card to a third party and cannot claim a reasonable expectation of privacy in it'").

[80] *See generally* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

whether the attachment of a GPS device on a vehicle constituted a search or seizure, Justice Sotomayor concurred that it might be time to reconsider the third-party doctrine since the digital age involves so much information-sharing with third parties.[81] Similarly, in *Kyllo v. U.S.*, when thermal heat imaging had been used to obtain a warrant to observe a potential illegal marijuana operation, the Court held that the warrant was improperly obtained as the home was a basic constitutionally protected area and that "advancing technology" that invades such a constitutionally protected area needs to be regarded carefully regardless of whether "intimate details" are revealed.[82]

In a recent Supreme Court case, *U.S. v. Carpenter*, the Court considered whether or not there was an expectation of privacy in cell site location information (CSLI) data revealing thousands of location points for a criminal defendant; the Court then assessed the third-party doctrine in connection with this data.[83] *Carpenter* assesses the privacy interest in CSLI data by looking at two different lines of case law: that of *Katz* and the "expectation of privacy in his physical location and movements" and one's "expectation of privacy in information voluntarily turned over to third parties."[84]

Carpenter hearkens back to *Miller* in order to make a distinction that the CSLI data was different than the "business records of the banks" at issue in *Miller*.[85] CSLI data reveals a cell phone's approximate position in relation to nearby cell phone towers, and, in this case, the location was revealed thousands of times and was acquired by law enforcement without a search warrant.[86] The technology at issue in *Carpenter* was the cell phone's periodic and innate attempts to establish signal connection by connecting to cell phone towers and the data trail created—CSLI data.[87] CSLI is data that is revealed about a cell phone's approximate position in relation to nearby cell phone towers; GPS data on a cell phone is even more specific, tracking location down to a 5–10-foot range.[88] This type of data implicates third-party cell phone companies or providers of GPS services.[89] This near-constant search for cell towers created a data trail identifying all of the towers that were near defendant's movements on the night the crime was committed.[90] The business records discussed in *Miller* are significantly different than the GPS-like tracking that occurred in *Carpenter*.[91] The *Carpenter* Court held that the tracking of someone's movements in this way without any voluntary action

[81] *Jones*, 565 U.S. at 417.

[82] Kyllo v. United States, 533 U.S. 27, 28 (2001).

[83] *Carpenter*, 138 S. Ct. at 2208-09.

[84] *Id.* at 2209-10, 2214-15.

[85] *Id.* at 2216.

[86] *Id.* at 2209, 2225.

[87] *Id.* at 2210.

[88] CELL PHONE LOCATION TRACKING, A NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (NACDL) PRIMER (2016) https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/U554-NREM].

[89] *Id.*

[90] *See Carpenter*, 138 S. Ct. at 2208-09.

[91] *See id.* at 2209 (CLSI data is "detailed, encyclopedic, and effortlessly compiled").

taken by the cell phone user seemed to be an overstretch of this "voluntary" element contained in the logic of the third-party doctrine.[92]

The *Carpenter* Court then assessed voluntary disclosure as it was described in *Smith*, in which bank records voluntarily shared between a bank client and the bank were considered business records.[93] A key touchstone for finding that the third-party doctrine applied in *Smith* was because of the client's voluntary handing over of information.[94] In *Carpenter*, the Court posited that while an individual may voluntarily use their cell phone, the cell phone user is not voluntarily relaying location data to third-party cell phone companies because it occurs involuntarily as a function of the technology.[95] The Court held that the third-party doctrine was over-extended when law enforcement acquired CSLI data without a warrant and connected the defendant to the crime.[96]

C. *Cryptocurrency Exchanges Are Third Parties in the Context of the Third-Party Doctrine*

Based on recent caselaw, cryptocurrency exchanges are third parties under the Fourth Amendment for purposes of the third-party doctrine. *Zietzke v. U.S.* is a blockchain case from the Northern District of California concerning personal information shared with the Coinbase cryptocurrency exchange that was tied to an accountholder who had inaccurately reported cryptocurrency gains on tax returns.[97] The *Zietzke* court held that consumers revealing information to Coinbase was comparable to the *Miller* holding concerning bank records, and thus, law enforcement rightfully did not need to obtain a warrant.[98]

U.S. v. Gratkowski presented a similar issue in which law enforcement subpoenaed Coinbase, and obtained access to Gratkowski's account without a warrant.[99] At issue was a blockchain in which a cluster of Bitcoin addresses were found to be connected with a child pornography website.[100] Federal agents recruited a service to analyze the cluster of addresses to identify specific ones connected with the website.[101] After identifying the implicated

[92] *Id.* at 2216-18 (*Carpenter* Court describing cell phones as practically a fixture of the human "anatomy").

[93] *Id.* at 2219-20.

[94] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[95] *Carpenter*, 138 S. Ct. at 2220.

[96] *Id.* at 2220, 2223 (While the Court described the holding as "narrow," the narrowness of this holding seemed to stem from the fact that cell phones are indispensable in modern society and that CSLI data is not voluntarily shared, but a virtue of the cell phone's operation. The narrowness of this holding likely would not preempt a similar logic being applied to other privacy-invasive technologies).

[97] Zietzke v. United States, No. 19-cv-03761-HSG (SK), 2020 WL 264394, at *1 (N.D. Cal. Jan. 17, 2020).

[98] *Id.* at *13 (because this information shared by Zietzke was "voluntarily exposed . . . to Coinbase for commercial purposes, he does not retain a reasonable expectation of privacy over this information").

[99] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

[100] *Id.*

[101] *Id.*

addresses, the agents served a "grand jury subpoena on Coinbase—rather than seeking and obtaining a warrant—for all information relating to the Coinbase customers whose accounts had sent Bitcoin to any of the addresses" included in the cluster.[102] The agents did not have any identifying information concerning the customers whose addresses they were seeking via subpoena.[103] However, the Fifth Circuit held that because "every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers" Gratkowski had no privacy interest.[104] In its analysis, the court stated that those people who interact on the blockchain have more privacy "than those who use other money-transfer means" because the blockchain provides more privacy than a bank.[105] However, this "privacy" seems more arbitrary than actual, considering that once law enforcement has the address of a blockchain user, the blockchain can be traced back to a cryptocurrency exchange, and the user seems to be treated no differently than "those who use other money-transfer means."[106]

Likewise, the *Gratkowski* court does not apply *Carpenter*, noting that Coinbase records are "limited" and do not create the same potential for constant surveillance as do the CSLI data; as well as the fact that transacting on Coinbase requires an "affirmative act" from users, more akin to that which was at issue in *Miller*.[107] To further flesh out what expectation of privacy users have in their data on Coinbase, the court assesses Coinbase in light of *Miller* and the requirements that Coinbase must follow under the Bank Secrecy Act.[108] The key distinction that the Fifth Circuit leaves us with is that people who choose Coinbase (a third-party money transmitter), rather than just going directly to the blockchain without an intermediary, end up sacrificing their privacy in the same way that consumers sacrifice their privacy interest when transacting with a bank.[109]

IV. A NECESSARY DISTINCTION: THE PROBLEM OF CONFLATING THE PUBLIC BLOCKCHAIN WITH THIRD-PARTY CRYPTOCURRENCY EXCHANGES.

As courts are presented with issues concerning the third-party doctrine's application to blockchain transactional data, there is a need to recognize the distinction between the blockchain and a cryptocurrency exchange. Part IV, Section A assesses why *Carpenter* can be looked at as establishing a new precedent concerning how courts examine the third-party

[102] *Id.*

[103] *No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds*, JONES DAY, (June 2020) https://www.jonesday.com/en/insights/2020/07/no-search-warrant-required-for-records-of-bitcoin-transactions-the-fifth-circuit-holds [https://perma.cc/KNV7-LYC9].

[104] *Gratkowski*, 964 F.3d at 312.

[105] *Id.*

[106] *See id.*

[107] *Id.* at 312.

[108] *Id.*

[109] *Id.* at 312-13.

doctrine's application in emerging technology cases. Section B identifies the issue with conflating the public ledger blockchain transactions as a public revelation of identity and proposes how a cryptocurrency exchange is distinct and should be approached by law enforcement with this in mind. Finally, Section C expands on Section B by discussing specific case law and recommends why the search warrant should be required.

A. Cryptocurrency Exchanges Are Third Parties, but Carpenter Sets New Precedent for Finding a Privacy Interest when Emerging Technologies Involve Third-Party Transactions

Under the third-party doctrine, cryptocurrency exchange users do not currently have a recognized privacy right to their stored data because the exchanges are viewed as money transmitters.[110] However, the two case lines presented in *Carpenter* provide a basis for recognizing an independent privacy interest in blockchain data. This section asserts that the logic of *Carpenter* justifies finding a privacy interest in blockchain data even while cryptocurrency exchanges are considered third parties.

The *Carpenter* Court stated that it keeps "[f]ounding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools."[111] As evidenced in *Gratkowski*, blockchain transactions require innovative surveillance tools to uncover malicious behavior.[112] Law enforcement cannot simply open up a blockchain ledger and do a quick "Control+F" search to find a public key; this requires cryptography and careful analysis of the blockchain to discern information such as the transaction ID, IP address, or geographic locational data for a suspect's Virtual Asset Service Provider.[113] The catalogues of information that can be dredged up in blockchain transactions are not unlike the CSLI data in *Carpenter* or law enforcement's use of a heat detector in *Kyllo* to uncover marijuana possession.[114] In *Kyllo* and *Carpenter*, these intrusions were held as violations of a person's reasonable expectation of privacy.[115]

In *Carpenter*, the court focused on how the reasonable expectation of privacy in CSLI data was at "the intersection of two lines of cases . . . [One] set . . . addresses a person's expectation of privacy in his physical location

[110] *Money Transmitter Licensing for U.S. Crypto Companies*, KELMAN LAW, (July 13, 2020), https://kelman.law/insights/money-transmitter-licensing-for-u-s-crypto-companies/ (describing the regulation of cryptocurrency exchanges as money transmitters) [https://perma.cc/KD76-5JRS]; Lloyd, *supra* note 53, at 214-15 (noting the potential for *Carpenter* to effect blockchain regulation).

[111] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[112] *See Gratkowski*, 964 F.3d at 309.

[113] Lucas Ropek, *Cryptocurrency Tracer Could Give Cops an Edge on Cybercrime*, GOV'T TECHNOLOGY, (Sept. 22, 2020), https://www.govtech.com/security/cryptocurrency-tracer-could-give-cops-an-edge-on-cybercrime.html (a virtual asset provider is "the forum through which cryptocurrency can be translated into actual cash") [https://perma.cc/9QP3-AZYH].

[114] *See Carpenter*, 138 S. Ct. at 2216-17; Kyllo v. United States, 533 U.S. 27, 34-35 (2001); *see, e.g.*, Longman, *supra* note 14, at 132.

[115] *See Carpenter*, 138 S. Ct. at 2216-17; *Kyllo*, 533 U.S. at 34-35.

and movements" while the other asserts that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[116] Concerning the expectation of privacy in physical location and movements, the CSLI data is "detailed, encyclopedic, and effortlessly compiled."[117] While *Carpenter* was, by its terms, "a narrow decision," the Court's logic acknowledged how new challenges presented by developing technologies invite caution about the rigid application of the third-party doctrine; these limitations of the third-party doctrine cannot reasonably be confined to CSLI data.[118] The tracking of physical movements may be troubling, but equally troubling is the tracking and ability to trace any data movement that reveals intimate content about the nature of transactions that individuals engage in.[119] On the blockchain, each transaction reveals a user's public key, and the public ledger reveals the chronological history of the user's transactions.[120] In creating an exception for CSLI data, the Court in *Carpenter* was focused on the fact that the "individual continuously reveals his location to his wireless carrier implicat[ing] the third-party principle of *Smith* and *Miller*."[121] This same logic could be applied to blockchain transactions completed through cryptocurrency exchanges because even while a cryptocurrency exchange maintains and owns the public and private keys associated with accounts hosted by their service, this continuous stream of data transactions listed on the blockchain is not the same as a bank possessing transaction history from individual clients.[122] A cryptocurrency exchange is essentially a public marketplace; it only facilitates what people can do by themselves if they remove themselves to a decentralized blockchain.[123] This distinct separation between the entity of the blockchain and the cryptocurrency exchange suggests that courts acknowledge that there is a separate privacy interest in blockchain data that is reflected by the lack of ownership in what is publicly viewable on the ledger and what is owned by the third-party cryptocurrency exchange.

Additionally, the *Carpenter* Court addresses the voluntariness of data sharing.[124] The two main points addressed are (1) how cell phones are pervasive and are essentially anatomical extensions in the modern world, and (2) that the cell phone's ability to connect to a cell tower does not require any

[116] *Carpenter*, 138 S. Ct. at 2214-16 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)).

[117] *Id.*

[118] *Id.* at 2214, 2220.

[119] Longman, *supra* note 14, at 132.

[120] Rui Zhang, et al., *Security and Privacy on Blockchain*, 52 ASS'N FOR COMPUTING MACHINERY COMPUTING SURVS. 51:2-3 (July 2019) (the "consensus procedure . . . enforced by the network . . . controls . . . the admission of new blocks into the block chain" and ensures the validity of each block).

[121] *Carpenter*, 138 S. Ct. at 2209.

[122] *See* Frankenfield, *supra* note 27; *see also What's a Bitcoin Exchange?*, *supra* note 27 (describing the "custodial" nature of cryptocurrency transactions on exchange platforms like Coinbase).

[123] *See* Frankenfield, *supra* note 27; *see What's a Bitcoin Exchange?*, *supra* note 27.

[124] *Carpenter*, 138 S. Ct. at 2220.

voluntary action from the user.[125] Certainly, blockchain technology is not so pervasive that it is a "feature of human anatomy."[126] However, the verification of a transaction requires no affirmative act on behalf of the user: it is a function of the program.[127] This "voluntariness" factor that the Court weighs is conspicuously absent from a blockchain transaction; courts assessing claims that blockchain follow a *Carpenter* analysis should not so easily dismiss *Carpenter*'s application based on the fact that the data being shared is financial in nature and that the blockchain is not as ubiquitous as a cell phone.[128] The reality is that once one consents to use a cryptocurrency exchange to transact, there is no voluntariness in the data sharing at all: it is required for individuals to submit to KYC protocols and share personally identifiable information with the platform in order to even open an account.[129]

The holding of *Carpenter* states that a warrant requiring probable cause was required to obtain CSLI records.[130] The Court's analysis should not be read to exclude a scenario in which blockchain technology appropriately fits within the Fourth Amendment's protection even while a cryptocurrency exchange is a third party. Even if not explicitly fleshed out in the opinion, the canon of construction concerning avoidance of absurd results in assessing advancing technology appears to undergird the logic of the opinion, and this principle is what should guide future courts in analyzing blockchain technology in these circumstances.[131] In *Carpenter*, there is a focus on the Court's role to preserve the Fourth Amendment's protection where technology is advancing. If the Court is ready to protect the public location of individuals as CSLI data under the Fourth Amendment, the issue of whether to consider the time-stamped, immutable blockchain transactional data as worthy of protection is ripe for consideration as well.

B. Why the Ledger's Transparency Does Not Negate the Privacy of Actors Using a Third-Party Exchange

Blockchain promises to deliver privacy while remaining transparent.[132] Privacy law is largely governed by a framework that relies on the concealment of information in order to maintain privacy, a concept that does not seem to line up with the transparency of the blockchain.[133] This premise that secrecy and privacy are one and the same arises frequently in the application of the third-party doctrine.[134] The hallmark case, *Smith*, talks about the concept of secrecy in privacy analysis: "it is too much to believe that telephone

[125] *Id.* at 2218, 2220.

[126] *Id.* at 2218.

[127] Zhang, et al., *supra* note 120, at 51:3.

[128] *See* United States v. Gratkowski, 964 F.3d 307, 312-13 (5th Cir. 2020).

[129] *See What Is AML/KYC in Crypto?*, SYGNA: BLOG , https://www.sygna.io/blog/what-is-aml-kyc-in-crypto/ [https://perma.cc/4JS9-49YH].

[130] *E.g.*, *Carpenter*, 138 S. Ct. at 2221.

[131] *Id.* at 2214, 2216-17.

[132] *See* Longman, *supra* note 14, at 118-19; *see also* Belonick, *supra* note 61, at 118-19.

[133] SOLOVE, *supra* note 65, at 94; *see also* Belonick, *supra* note 61, at 114-15.

[134] Belonick, *supra* note 61, at 122.

subscribers . . . harbor any general expectation that the numbers they dial will remain secret."[135] Some have questioned why someone with nothing to hide would be worried about their privacy on the blockchain where everything is recorded publicly. The answer should be clear: privacy's end goal does not have to be secrecy, and with blockchain, secrecy is not the end goal.[136] Blockchain's end goal is to "remove secrecy while maintaining privacy."[137]

There is a need to acknowledge that public ledger blockchain transactions are not a public revelation of identity; identity remains secret when the transaction is posted. A cryptocurrency exchange possesses private information obtained by KYC—information which is distinct from the public revelations on the blockchain ledger, and it should be approached by law enforcement with this in mind. By changing the conversation in this way, we are simply looking back to the foundation of Fourth Amendment law.[138] Early Americans wanted to secure their possessions from unfair intrusion.[139] These possessions were enumerated in the provision, but that provision did not include an exemption for those papers and records that were shared with others.[140] In the blockchain, the identity of individuals is concealed—the transactions only reveal the addresses of the users.[141] Paul Belonick describes this as a content/noncontent distinction and compares blockchain transactions to phone call records in a pen register; he describes how, traditionally, a pen register would record the phone number of a caller (the phone number being noncontent information), but that none of the contents of the call are recorded in the register. [142] Conversely, the blockchain reveals the contents of the transaction on the blockchain, without fully disclosing the content of the identity of the user who posted the transaction.[143] In *Katz*, the pen register case, the Court held that the individual standing in the phone booth had a reasonable expectation of privacy in the content of his conversation.[144] This content distinction should remain important in Fourth Amendment analysis and should be the basis for finding a privacy interest in the hidden content of a user's identity.[145]

We have been willing to recognize privacy interests in things exposed to the public based on a reasonable expectation of privacy.[146] The fact that law enforcement relies on the third-party doctrine to access content information at a lower standard than a search warrant is worrisome, as the Fourth Amendment has been neutered of any real meaning in an age that depends on third-party transactions.[147] If content truly is the basis of

[135] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[136] Belonick, *supra* note 61, at 153.

[137] Longman, *supra* note 14, at 127.

[138] Belonick, *supra* note 61, at 158.

[139] *Id.*

[140] *Id.* at 158, 166.

[141] Longman, *supra* note 14, at 122.

[142] *See* Belonick, *supra* note 61, at 152.

[143] *See id.* at 153.

[144] Katz v. United States, 389 U.S. 347, 353 (1964).

[145] Belonick, *supra* note 61, at 151-53.

[146] *Katz*, 389 U.S. at 351, 360-61.

[147] United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring).

protection, then blockchain data should be assessed with this standard.[148] This standard would not mean that we ignore the fact that the public ledger contains public key information that can be identified, but it does mean that we recognize that no investigator is going to be able to independently find out the user's identity when presented with just a string of digits. When an investigator has identified a public key, law enforcement should then be required to obtain a search warrant, because at that specific moment in time, they have no lead on identity. The only identity that should be searched for when presenting a cryptocurrency exchange with a search warrant is the identity associated with that public key.

C. Law Enforcement Should Need Search Warrant to Obtain Personal Information Held by a Cryptocurrency Exchange

The blockchain, unlike banks and phone companies, is not a third-party intermediary, and the transactions are not part of the course of business of a cryptocurrency exchange: it is a ledger establishing a public record of transactions. At issue in *Miller* were bank records, and the Court held that because these records were property of the bank, Miller had no privacy interest.[149] At issue in *Smith* was the expectation of privacy in the phone numbers dialed and traced by the pen register.[150] The phone company, possessing records of the phone calls placed by those using the service, is a third party who has "legitimate business purposes" in maintaining this data, just like the bank in *Miller*.[151]

In *Miller*, the bank was subpoenaed based on a tip that two individuals were connected to an illegal distillery trade, and, in *Smith*, the police did not get a warrant or court order, but merely requested the phone company install a pen register. [152] In either scenario, under the third-party doctrine, the third parties were not issued a warrant, but still turned over information in their possession: in the first case, there was no need for a warrant because there was no Fourth Amendment interest in the data, in the second case, the Court held that there was no content information, thus no Fourth Amendment violation in obtaining the records.[153]

On the surface, the fact pattern in *Gratkowski* resembles that of *Miller*. However, what is at issue in *Gratkowski* is that federal law enforcement was able to identify a cluster of likely addresses that comprised a pornography website, but had no leads on any customers.[154] Because there was no requirement for a search warrant, it did not matter whether the evidence that the officers had collected regarding the cluster of addresses was enough to establish probable cause that certain addresses were associated with a known pornography website: all they needed was a subpoena to obtain the

[148] *See* Belonick, *supra* note 61, at 151-53.

[149] United States v. Miller, 425 U.S. 435, 439-40 (1976).

[150] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[151] *Id.* at 742-44.

[152] *See Miller*, 425 U.S. at 435-37; *Smith*, 442 U.S. at 735.

[153] *See Miller*, 425 U.S. at 435-37; *Smith*, 442 U.S. at 735.

[154] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

cryptocurrency exchange account information of unknown addresses who had transacted with the address cluster.[155] If a search warrant had been the standard, they should have identified the public key addresses beforehand to see if Coinbase had public keys associated with any publicly available transaction information rather that subpoenaing Coinbase for account holder information and implicating an unknown amount of Coinbase customers in their search.[156]

Coinbase is a third party which owned at least one account address implicated in trading with a cluster of addresses associated with a criminal website.[157] The application of the third-party doctrine may make sense here if the forensic investigation into the address cluster had actually revealed that the address belonged to Gratkowski, because then law enforcement would be seeking information for an identified customer that Coinbase could confirm. However, even if Gratkowski was an "identified" customer, the forensic investigation by law enforcement only reveals the address, giving no information about customer identity. Gratkowski's account address was revealed during the investigation, but by operating under a subpoena, the evidence concerning the website cluster of addresses was treated akin to a general warrant to access Coinbase records for associated addresses and customer information.[158] In the opinion, the court makes the distinction between a third-party exchange like Coinbase and the blockchain.[159] The court also acknowledged that "users have the option to maintain a high level of privacy by transacting without a third-party intermediary," but the court does not question whether the subpoena was constitutional when law enforcement had no reason to suspect Coinbase accounts had an association with the criminal cluster of addresses prior to Coinbase's acquiescence to the subpoena request.[160] The forensic analysis directed at the blockchain to obtain data about whether certain addresses were part of a suspected child porn trafficking site and the use of that analysis to obtain data that incriminated previously unsuspected individuals reveals how this distinction between the blockchain and the exchange is eroded in *Gratkowski*.[161] The erosion of this distinction appears to be an expansion of the third-party doctrine beyond its prior bounds.[162]

Gratkowski acknowledges that the blockchain ledger is public; the fact that anyone can log on and view the transactions on the Bitcoin ledger may

[155] *Id.*; *see also Probable Cause*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/probable_cause (probable cause can be established when there is "reasonable basis for believing that a crime may have been committed…or when evidence of the crime is present in the place to be searched.") [https://perma.cc/7XSS-J3L9].

[156] *See Gratkowski*, 964 F.3d at 309.

[157] *Gratkowski*, 964 F. 3d at 309.

[158] *Id.*

[159] *Id.* at 309 ("to conduct Bitcoin transactions, Bitcoin users must either download Bitcoin's specialized software or use a virtual currency exchange, such as the one used here, called Coinbase").

[160] *Id.* at 312-13 (this could be accomplished by using software to transact on the blockchain without an exchange, but activity requires sophisticated "technical expertise").

[161] *Id.* at 312-13.

[162] *Id.*

seem to make it redundant to require a search warrant to view what is in plain sight.[163] But these transactions do not relay identity in the way that they reveal public keys.[164] This is evidenced by the fact that law enforcement needed to subpoena Coinbase to even find out which addresses they possessed had transacted with the website.[165] This extensive search for accounts and seizure of information is much different than subpoenaing a bank for a known suspect's bank records or tracing the phone calls of a known suspect with a pen register.[166] The blockchain may contain a recipient's address, but it does not directly reveal any content information about the sender or recipient.[167] Before subpoenaing Coinbase, there was no reasonable suspicion of any individuals in particular; law enforcement should be required to establish probable cause and obtain a warrant to search an exchange service, otherwise this type of search too closely resembles the general warrant, the rejection of which was a key motivator to the drafters of the Fourth Amendment.[168]

The lens of early Fourth Amendment jurisprudence offers further insight into this concern. *Ex parte Jackson* created the logical and theoretical distinction between envelope and content.[169] The court held that the envelope had no privacy interest because it was exposed to the public strictly for the transmission of data.[170] The content inside the envelope retained a privacy interest because it was enclosed from view; the government could not just take any envelope, open it up, and discern its contents.[171] This distinction was a logical extension to protect Americans from general warrants.[172]

If we apply this same logic to the blockchain, we can think of the public keys on the blockchain as equivalent to an address on an envelope.[173] The block in the ledger reveals addresses that engaged in the transaction, but does not establish identity.[174] Conversely, in *Ex parte Jackson*, the address did identify the individual but was also non-content information.[175] Likewise, in the early third-party doctrine cases, the pen register and bank records automatically could be tied to the party who owned the phone number or the

[163] *Id.* at 312.

[164] Longman, *supra* note 14, at 123.

[165] *Gratkowski,* 964 F.3d at 309.

[166] *See* United States v. Miller, 425 U.S. 435, 437 (1976); Smith v. Maryland, 442 U.S. 735, 735 (1979).

[167] Longman, *supra* note 14, at 123; Belonick, *supra* note 61, at 153.

[168] Belonick, *supra* note 61, at 151-53, 170.

[169] *Id.* at 151-53.

[170] *See* Ex parte Jackson, 96 U.S. 727, 732-33 (1877).

[171] *See id.*; *see also* Belonick, *supra* note 61, at 151.

[172] *See* Belonick, *supra* note 61, at 151-52, 162; *Jackson*, 96 U.S. at 732-33.

[173] Belonick, *supra* note 61, at 153, 160-61 ("like a physical address, directing the transaction to a recipient"; it would not make sense to require law enforcement to "avert their gazes" from this observable data); *see also* Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393, 1429-1430 (2017) ("if an encryption key qualifies as content information, then its seizure will typically require a warrant; not so if it is non-content").

[174] Belonick, *supra* note 61, at 153.

[175] *Jackson*, 96 U.S. at 732-33.

bank account, respectively.[176] These distinctions reveal that while blockchain wasn't anticipated by the Fourth Amendment, it still operates within the logic of what the Fourth Amendment was designed to protect.[177] As mentioned by Paul Belonick, this "non-content" data of digits in a blockchain transaction may still preserve a privacy right simply because it cannot be so easily connected to an individual without cryptographic analysis.[178] Subpoenas based on evidence of a collection of addresses should not be the basis to seek out every unknown user who may have transacted with a suspect entity; allowing for this standard as it was established in *Gratkowski* sets a dangerous precedent that diverts from traditional Fourth Amendment jurisprudence.

V. COURTS OR CONGRESS SHOULD RECOGNIZE A PRIVACY INTEREST IN BLOCKCHAIN TRANSACTIONS

This section first presents proposed solutions to the problems enumerated above and then assesses the counterarguments that logically flow from this analysis and proposes solutions.

A. Later Court or Congressional Developments Provide Future Opportunities to Distinguish Exchanges from Blockchain

Blockchain technology should be understood as an advancement in technology that needs to be examined with the same care as technologies in the family of cases that have followed *Miller* and *Smith*.[179] Blockchain transactions are comprised of address information: the identity information possessed by exchanges should not be accessible without probable cause and a warrant since the blockchain does not record this identity information in the public ledger.[180] Formalization of this principle could be achieved either through the courts or by federal legislative action.

1. Courts Should Look at Blockchain as an Emerging Technology, Distinct from Online Banking Apps and Cell Phones

The technical and fact-specific realities of blockchain's function lend themselves easily to comparison with technologies that have been held as too invasive and intrusive to stand without a warrant. It will be critical to

[176] *See* United States v. Miller, 425 U.S. 435, 437 (1976); Smith v. Maryland, 442 U.S. 735, 735 (1979).

[177] Belonick, *supra* note 61, at 151-53.

[178] *Id.* at 153.

[179] *See* Kyllo v. United States*,* 533 U.S. 27, 35 (2001) (the court resists an approach that "would leave the homeowner at the mercy of advancing technology"); United States v. Jones, 565 U.S. 400, 430-31 (2012) (Alito, J., concurring) (court looks at the reasonable person's expectation of privacy in using new GPS technology); Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (the court talks about the "infallible" memory of the technology at issue in assessing the potential privacy right).

[180] Belonick, *supra* note 61, at 153.

distinguish blockchain from instances of new technologies that have fallen under the third-party doctrine. In *Carpenter*, the Supreme Court found that CSLI data was equally if not more intrusive than the GPS data at issue in *Jones*, when the Supreme Court held that attaching a GPS to a suspect's vehicle violated his right to privacy in his movements; but even more noteworthy was that this type of data was held to not be subject to the third-party doctrine even though it was owned by a third party.[181] If it could be shown that blockchain data is more akin to the content-envelope issue, then it could be argued that the third-party doctrine may not apply even if a third-party exchange claims ownership of the address and public/private keys.[182]

2. Congress Needs to Assess the Gaps Created by the Emergence of New Technology with Legislation Like it Did with the 1978 Right to Financial Privacy Act

In response to the holding in *Miller*, Congress passed the Right to Financial Privacy Act of 1978, which requires "a subpoena, a summons, a search warrant, or the customer's written consent, or . . . the government [to] submit[] a formal written request."[183] This was an attempt to fill the gap in Fourth Amendment protections effectuated by passage of the Bank Secrecy Act and the result of the *Miller* case.[184] Congress is similarly aware of privacy concerns that are only amplified by the free reign given third parties in the digital age.[185] Congress is in the position to reassess the reach of the third-party doctrine in light of the role that third parties play in the digital world, as noted in *Jones*.[186] Such a solution from Congress could be to pass a law that requires law enforcement to establish probable cause concerning implicated addresses before obtaining consumer records from a cryptocurrency exchange.

B. Blockchain Threats to Established Fourth Amendment Jurisprudence and Protecting Privacy in the Face of Criminal Activity

The following two sections assess concerns about whether blockchain threatens to expand *Carpenter*'s supposedly narrow holding, as well as

[181] *Carpenter*, 138 S. Ct. at 2217, 2220.

[182] *E.g.*, Belonick, *supra* note 61, at 151-53.

[183] Longman, *supra* note 14, at 115 (citing *Duncan*, 813 F.2d 1135, 1337 (4th Cir. 1987)).

[184] Longman, *supra* note 14, at 115; Lloyd, *supra* note 53, at 218.

[185] Cameron F. Kerry & John B. Morris, Jr., *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS INST., (Dec. 8, 2020), https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/ [https://perma.cc/45WT-NMSM].

[186] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

broader worries about the effects on criminal prosecution in the cryptocurrency space.

1. *Carpenter* Accommodates Blockchain in Its Analysis: Blockchain Does Not Require Special Protection

While some might argue that the approach proposed in this Note would undermine established case law, this proposal does not apply a special protection or stretch *Carpenter*. Blockchain is a developing technology, just like the technologies assessed in *Carpenter*, *Jones*, and *Kyllo*.[187] As such, it should be recognized that obtaining records in the manner conducted in *Gratkowski* did not comport with typical probable cause requirements under the Fourth Amendment.[188] Law enforcement had no lead on any implicated identities which Coinbase was able to supply.[189] In situations like this, law enforcement should be required to identify individual account addresses in these transactions and use this information to present a search warrant to Coinbase. This two-step procedure would honor the distinction between the actual third-party exchange and the blockchain.

2. Criminals Do Not Evade Liability with this Proposal: The Third-Party Doctrine Should Not Reach Activity Outside a Third-Party's Possession

If we fear technology's negative use cases more than we prize protecting citizens' Fourth Amendment rights, we may risk putting up too many barriers for users to engage in innovations without fear of government overreach. In this regard, blockchain technology creates a space that is different than what was initially at issue when the Bank Secrecy Act was passed and when the third-party doctrine was applied to banks.[190] This legal regime predated the Internet and could not comprehend the digital economy of blockchain. This new world is ripe for a second look at the third-party doctrine, as evidenced in *Carpenter*.[191]

By adopting a willingness to see how third parties are implicated and involved in these transactions, it may open the door to a more honest interpretation and application of the Fourth Amendment in the modern era, as it is made more irrelevant in a world where every transaction seems to implicate a third party. Rather than allowing access of private information possessed by exchanges through a simple subpoena, court order, or written request, the distinction between blockchain and exchanges would be honored

[187] *See Kyllo*, 533 U.S. at 35; *Jones*, 565 U.S. at 430-31 (Alito, J., concurring); *Carpenter*, 138 S. Ct. at 2219.

[188] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

[189] *Id.*

[190] United States v. Miller, 425 U.S. 435, 442-43 (1976).

[191] *Carpenter*, 138 S. Ct. at 2224.

by requiring an actual warrant supported by probable cause for law enforcement seeking information about exchange users.

VI. CONCLUSION

The third-party doctrine was first asserted in the realm of early technological development with the telephone and in bank records. That era could not anticipate a tech innovation like blockchain technology and the role played by third-party intermediaries controlling data. The protections of the Fourth Amendment and the third-party doctrine are always being tested by the new technologies used to conduct surveillance and communicate. By assessing new technology in light of the Fourth Amendment's purpose, privacy can be protected in the digital age.

This paper has attempted to reveal the concerns raised by courts applying the third-party doctrine to blockchain transactions and to encourage dialogue considering the implications of this technology and why the solutions may not be that different than prior treatment of advancements like GPS and CSLI data. As more companies adopt blockchain, courts should be made aware of the distinction between the blockchain and a third-party exchange's ownership of an address and private data. Consumers should only lose their expectation of privacy in their account information if a properly acquired warrant is brought against an exchange.

Whose Lie Is It Anyway? Holding Social Media Sites Liable for Procedural Election Disinformation

Jadyn Marks*

TABLE OF CONTENTS

[*] Jadyn Marks, J.D., May 2022, The George Washington University Law School. I want to thank my parents for their unconditional love and support. I would also like to thank the FCLJ editorial board and members for their work during the editorial process.

I. INTRODUCTION

The 2020 presidential election was a rollercoaster for the American people. From Facebook providing an election information center notification on posts pertaining to the election,[1] to Twitter flagging tweets from then-President Donald Trump,[2] social media sites have developed and enacted different policies to prevent the spread of political misinformation and disinformation.[3] These sites have taken encouraging steps toward protecting foundational principles of American democracy, but standards that vary site-by-site are insufficient to curb the onslaught of misinformation and disinformation that users are exposed to on a daily basis. Exposure to false information about procedural aspects of elections is especially worrisome for American democracy. To help prevent the spread of procedural election disinformation, Congress should authorize the Federal Trade Commission to promulgate regulations to prevent paid procedural election disinformation from circulating on social media sites.

In 1996, Congress passed the Communications Decency Act. This Act includes section 230, which has been frequently discussed by politicians, federal representatives, and the media throughout 2020 and 2021.[4] Section 230(c)(1) provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[5] This provision essentially insulates service providers — including social media sites like Facebook and Twitter — from liability for third-party content, with some exceptions relating to criminal acts.[6]

While section 230 was more easily applicable in 1996 when the Internet was just beginning to develop, technological developments have now likely exceeded the bounds of what legislators imagined in 1996. Unfortunately, the legislation has not kept pace with the times, and as such, Internet Service Providers (ISPs) continue to be insulated from liability in questionable circumstances. One such circumstance is that many social media companies fail to meaningfully regulate procedural election advertising on their websites. This failure to regulate leads to the spread of disinformation and could have

[1] Guy Rosen, *Preparing for Election Day*, META (Oct. 7, 2020), https://about.fb.com/news/2020/10/preparing-for-election-day/ [https://perma.cc/8857-R7CH].

[2] *Trump Falsely Claims He Won the Election; Twitter Flags the Tweet*, CBS NEWS (Nov. 16, 2020, 3:42 PM), https://www.cbsnews.com/news/trump-tweet-claims-he-won-election-twitter-flags/ [https://perma.cc/W793-SVGB].

[3] Dawn Carla Nunziato, *Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation*, 19 FIRST AMEND. L. REV. 33, 33 (2020).

[4] William A. Sodeman, *Communications Decency Act*, BRITANNICA (Nov. 24, 2016), https://www.britannica.com/topic/Communications-Decency-Act [https://perma.cc/32GX-2HR5]; Taylor Hatmaker, *Trump Vetoes Major Defense Bill, Citing Section 230*, TECHCRUNCH (Dec. 23, 2020), https://techcrunch.com/2020/12/23/trump-ndaa-veto-section-230/ [https://perma.cc/2EKR-MHQ6].

[5] 47 U.S.C. § 230.

[6] *Id.*

long-lasting effects on American democracy by disenfranchising eligible voters.

Permitting the unchecked spread of procedural election disinformation prompts significant concerns both with the First Amendment and with notions of a free democracy. John Stuart Mill's theory of the free marketplace of ideas contemplates that having an open forum for speech will allow individuals to exchange information and ideas, and over time, society will filter out inaccurate information from this exchange.[7] While this "marketplace of ideas" theory applied easily in a time where people were openly exposed to a variety of information and ideas, this theory is limited by the modern marketplace of ideas of social media. Social media users tend to consume content they find interesting and agree with, creating an "echo chamber," wherein users may only be exposed to the ideas with which they agree.[8] This problem is further exacerbated by algorithms which suggest content based on other content users have consumed.[9]

Procedural election disinformation also affects America's notion of a free democracy by suppressing voters and rendering them misinformed.[10] Inaccurate information about polling places, where and how to properly register to vote and to check your voter registration status, and other procedural aspects of participating in elections amounts to voter suppression.[11] Further, citizens may cast their votes based on inaccurate information about candidates and their platforms.[12] For example, a study surrounding the 2016 Presidential election found that undecided voters were more likely to vote for Donald Trump after being exposed to fake news stories about Hillary Clinton.[13]

Social media sites have taken varied and admirable steps to curb the spread of political and election-related misinformation and disinformation. However, because the procedures and policies vary from company to company, and sometimes from state to state,[14] there is no uniform approach. This could lead to the information sneaking into users' feeds if they use

[7] David Schultz & David Hudson, *Marketplace of Ideas*, FREE SPEECH CTR. (June 2017), https://www.mtsu.edu/first-amendment/article/999/marketplace-of-ideas [https://perma.cc/QUU6-9RM3].

[8] Christopher Seneca, *How to Break Out of Your Social Media Echo Chamber*, WIRED (Sept. 17, 2020, 9:00 AM), https://www.wired.com/story/facebook-twitter-echo-chamber-confirmation-bias/ [https://perma.cc/LL9G-SFRU].

[9] *Id.*

[10] *See* Zachary Roth, *We Need a Truth-in-Advertising Commission — For Voters*, BRENNAN CTR. FOR JUST. (Oct. 16, 2019), https://www.brennancenter.org/our-work/analysis-opinion/we-need-truth-advertising-commission-voters [https://perma.cc/5MJY-MJ53].

[11] *See id.*

[12] *Id.*

[13] Aaron Blake, *A New Study Suggests Fake News Might Have Won Donald Trump the 2016 election*, WASH. POST. (Apr. 3, 2018), https://www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/ [https://perma.cc/RC64-BAZ3].

[14] Salvador Rodriguez, *Facebook to Reinstate Political Ad Ban in Georgia Following Senate Runoff Elections*, CNBC (Jan. 5, 2021), https://www.cnbc.com/2021/01/05/facebook-to-reinstate-political-ad-ban-in-georgia-following-senate-runoff-elections.html [https://perma.cc/SQ54-MWJ9].

multiple social media applications with different policies. For example, a user could take a screenshot of a political advertisement on Facebook and share it on Twitter.

To combat the difficulties created by and the worrying consequences resulting from allowing unregulated paid procedural election disinformation to be promulgated on social media sites, Congress should pass narrowly tailored and specific legislation authorizing the Federal Trade Commission (FTC) to promulgate rules regulating this area.

This statutory authorization must be narrowly and specifically written to include only regulation in the area of paid advertising regarding procedural aspects of elections. Once the FTC receives congressional authorization, it will be able to promulgate regulations as it sees fit. However, it may want to hold hearings to garner information about the existing procedures and approaches of different social media sites to determine the framework for its regulations. These regulations would be centered around the social media sites and would determine substantive guidelines and regulations for displaying ads concerning procedural election information, rather than focusing on the entities purchasing the ad space.

This Note will first define disinformation in Part II, Section A, and will explore the legal theories that provide a framework for regulation in this area in Section B. In Section C, this Note considers the current regulatory frameworks of two popular social media sites, Facebook and Twitter, compares their approaches, and explains why regulation of social media sites as "middlemen" is appropriate. Section C will also contrast Facebook and Twitter's approaches with those of Parler. Section D will then establish the FTC's jurisdiction in this area. In Part III, Section A, the Note will consider why delegation to the FTC is superior to Congress regulating the area itself through legislation; Section B will explain why regulation at the federal level is superior to regulation at the state level; Section C offers considerations concerning how debate over section 230 has made this area ripe for change; and Sections D and E consider alternative solutions and public policy. Finally, Section F explores how the FTC should proceed with regulating this space.

II. BACKGROUND

A. Defining Disinformation

Political misinformation and disinformation are popular topics, but each has a distinct meaning. Both misinformation and disinformation involve information that is false or out of context and is presented as factual.[15]

[15] Meira Gebel, *Misinformation vs. Disinformation: What to Know About Each Form of False Information, and How to Spot Them Online*, BUS. INSIDER (Jan. 15, 2021), https://www.businessinsider.com/misinformation-vs-disinformation [https://perma.cc/2DTC-J5CY].

However, disinformation is distinct in that it involves an intent to deceive.[16] Misinformation, by contrast, does not require an intent to deceive.[17]

B. *Two Legal Theories: The Marketplace of Ideas and Protecting Democracy*

There are two legal theories in First Amendment jurisprudence that support federal agency regulation of procedural information about elections. The first is John Stuart Mill's theory of the free marketplace of ideas.[18] Mill applied an economic analysis to speech and ideas, positing that information and ideas exist in a marketplace the same way that commercial products exist in a marketplace.[19] The competition of information and ideas in this marketplace naturally determines what ideas are true and acceptable, as the popular and widely accepted ideas will prevail over inaccurate ones.[20] Mill particularly believed that truth is better derived through this competitive marketplace than through any form of government censorship.[21]

The Supreme Court has come to favor Mill's marketplace of ideas theory in its First Amendment jurisprudence. In particular, the Supreme Court favors counterspeech as the most effective solution to harmful speech. Justice Oliver Wendell Holmes first brought Mill's theory to light in his dissent in *Abrams v. U.S.* In *Abrams*, the defendants published and distributed pamphlets supporting Russia and criticizing capitalism.[22] Notably, this was not at a time when the United States was at war with Russia.[23] The defendants were convicted on counts of conspiracy to incite, provoke, or encourage resistance against the United States and conspiracy to curtail production of war materials.[24] The Supreme Court affirmed the defendants' convictions and rejected their defense that the convictions violated the First Amendment.[25] In a now-famous dissent, Justice Holmes criticized the majority approach, emphasizing that the government interest in restricting speech is more important and justifiable in times of war.[26] He further proponed a major theory of First Amendment jurisprudence that the Supreme Court now favors — Mill's theory that the best way to come to the truth is for ideas to compete in a free marketplace, without any government censorship.[27]

Justice Holmes continued to emphasize this approach in his concurrence in *Whitney v. California*. In that case, the plaintiff attended a convention for the Socialist Party, and later sought to organize a California

[16] *Id.*

[17] *Id.*

[18] Schultz & Hudson, *supra* note 7.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Abrams v. United State, 250 U.S. 616, 618 (1919).

[23] *Id.* at 617-18.

[24] *Id.* at 617.

[25] *Id.* at 624.

[26] *Id.* at 626-27.

[27] *Id.* at 630.

branch of the Communist Labor Party.[28] She was then charged with and convicted of violating the California Criminal Syndicalism Act because she was a member of a group organized to advocate criminal syndicalism.[29] Criminal syndicalism laws were popular in the 1910s and 1920s during the Red Scare, and they outlawed advocating for radical political and economic changes through criminal or violent means.[30] The Supreme Court upheld the Act as constitutional and held that it was not an unreasonable or arbitrary exercise of the State police power.[31] In a concurrence by Justice Brandeis, joined by Justice Holmes, the justices once again espoused Mill's marketplace of ideas theory, especially the soon-to-become-popularized idea that counterspeech is the most effective remedy to harmful speech.[32]

Mill contemplated this theory in his book, *On Liberty*, which was published in 1859.[33] While this theory has its merits, Mill clearly developed it before the existence of the Internet or modern social media. The development of social media, along with its algorithms, have created barriers to the truly free marketplace of ideas that Mill contemplated. During the era in which Mill developed his theory, one could be exposed to different viewpoints simply by walking outside—individuals could post fliers on doors, hand out pamphlets or handbills, or yell on a street corner. Of course, it is still possible to do these things today, but social media is a much more accessible and easy way to exchange information and ideas because individuals don't need to leave their house to do so. However, while social media makes information and ideas more accessible, algorithms make exposure to information and ideas that are different from one's own views and ideas more difficult. Social media algorithms keep track of the content you watch or engage with, and then recommend new content based on your record.[34] For example, if a user explores their personal Facebook profile's settings and ad preferences, they can see certain demographics that Facebook has pegged them as—including their political affiliation.[35] Thus, algorithms tend to lock social media users into an "echo chamber" in which they are more

[28] Whitney v. California, 274 U.S. 357, 363 (1927).

[29] *Id.* at 359-60.

[30] Dale Mineshima-Lowe, *Criminal Syndicalism Laws*, FREE SPEECH CTR. (2009), https://www.mtsu.edu/first-amendment/article/942/criminal-syndicalism-laws [https://perma.cc/BKC2-SQNH].

[31] Whitney, 274 U.S. at 372.

[32] *Id.* at 377-78.

[33] *See generally* JOHN STUART MILL, ON LIBERTY (1859).

[34] Audrey Hingle, *Misinfo Monday: Are Algorithms Feeding You Crap?*, MOZILLA (Aug. 10, 2020), https://foundation.mozilla.org/en/blog/misinfo-monday-are-algorithms-feeding-you-crap/?gclid=Cj0KCQiAjKqABhDLARIsABbJrGkDIZNX3aDo2gSJ4rdf4NskDPYs95i-qkWICdOskxx7o4l7tgiwobcaAqz3EALw_wcB [https://perma.cc/YMM7-3E6C].

[35] *How to Check what Facebook Thinks Your Political Views Are*, TRISTATEHOMEPAGE.COM (Apr. 3, 2018, 7:20 PM), https://www.tristatehomepage.com/news/how-to-check-what-facebook-thinks-your-political-views-are/ [https://perma.cc/EBM7-XN8B].

likely to be exposed to viewpoints in which they have expressed prior interest.[36]

Further, Mill's and Justice Holmes' solution of counterspeech is far less effective in the modern world of social media. In the 19th and 20th centuries, individuals could engage in counterspeech by any of the same methods discussed above to engage in speech. People could yell over each other, or post or pass out fliers and pamphlets to counter other fliers and pamphlets. However, social media algorithms make this solution less feasible. When algorithms tend to only recommend speech that aligns with an individual's viewpoints, counterspeech is more difficult to access because algorithms simply won't recommend speech with which users tend to disagree. Beyond that, even where social media sites expose individuals to counterspeech, it is arguably easier to disengage from that speech. When two parties who disagree with each other are having a civil discussion, walking away from that discussion with no explanation would likely be considered rude. However, if someone is consuming media with which they disagree on the Internet and decide they don't want to listen anymore, all they have to do is close the Internet tab or page.

The other First Amendment theory supporting federal agency regulation of election information explores the issue of procedural election disinformation from a democracy standpoint. The First Amendment at its root is about protecting the individual right to speak, and by proxy, is about protecting the ability to have one's voice heard in elections. Although the First Amendment does not directly protect voting itself, it protects activities adjacent to voting, including whether one spends money to support candidates, protesting in general, and signing petitions that allow initiatives to appear on ballots.[37] In order to exercise these First Amendment rights, it is imperative that individuals have accurate information about polling places, voter registration, and the current status of an election race.

Each of these procedural aspects of elections—polling places, registration, and the current status of election races—are important for democracy. Accessible and accurate information about polling places and voter registration makes the voting process easier for people. Up until an individual turns eighteen, they have never registered to vote and may have little to no familiarity with the voting process. Accurate and accessible information about the registration process and how citizens can vote in their respective states makes the process easier because individuals don't have to spend as much time looking up where to go and how to register. If individuals are instead exposed to disinformation about polling places and voter registration, they may decide the process is too laborious. Worse still, people

[36] Christina Pazzanese, *Danger in the Internet Echo Chamber*, HARV. L. TODAY (Mar. 24, 2017), https://today.law.harvard.edu/danger-internet-echo-chamber/ [https://perma.cc/GR5V-U8GC].

[37] Lata Nott, *The First Amendment Protects Activities Adjacent to Voting, But Stops Short of Voting Itself*, FREEDOM F. INST. (Feb. 27, 2020), https://www.freedomforuminstitute.org/2020/02/27/the-first-amendment-protects-activities-adjacent-to-voting-but-stops-short-of-voting-itself/ [https://perma.cc/H74X-K78Q].

may think they have properly registered and then are denied the ability to vote on Election Day or have their vote rejected during vote processing.

Further, it is important that individuals have accurate information about ongoing or called races, and how those races were called by different news outlets. The 2020 election was particularly intense, as Democrats anticipated a potential change of the party in the White House, as well as the possibility of gaining a majority in the Senate.[38] The process was further intensified as several key states took days to count all of the votes, including a much-increased number of mail-in ballots due to COVID-19.[39] During the 2020 primaries, 50.3% of votes were cast absentee or by mail.[40] During the 2020 presidential election, 46% of votes were cast by mail.[41] Due to the combination of Trump's loss in the 2020 election and far-right conspiracy theories suggesting that mail-in ballots are not legitimate, there is now a right-wing movement insisting that Joe Biden fraudulently won the election, and that Donald Trump is the rightful President.[42]

Although this conspiracy theory initially seemed innocuous, especially as courts all over the country and even the Supreme Court rebuffed lawsuits challenging the election results, it has culminated into a very real threat.[43] On January 6, 2021, Americans lived through a jarring piece of history as a Trump rally went from unmasked crowds attending a speech during a global pandemic to breaking into the Capitol where Congress was in the process of certifying the election results.[44] The riot itself took five lives, and at least one

[38] Jacob Pramuk, *A Guide to 2020's Most Important Senate Races*, CNBC (Nov. 9, 2020), https://www.cnbc.com/guide/the-most-important-senate-races/ [https://perma.cc/6YJR-X3J9].

[39] Benjamin Swasey, *Election Night Viewer's Guide: Why You May Need to Be Patient*, NPR (Nov. 3, 2020), https://www.npr.org/2020/11/03/929740947/election-night-viewers-guide-why-you-may-need-to-be-patient [https://perma.cc/65JM-YKZ3].

[40] Drew DeSilver, *Mail-in Voting Became Much More Common in 2020 Primaries as COVID-19 Spread*, PEW RSCH. CTR. (Oct. 13, 2020), https://www.pewresearch.org/fact-tank/2020/10/13/mail-in-voting-became-much-more-common-in-2020-primaries-as-covid-19-spread/ [https://perma.cc/7U78-PN2V].

[41] CHARLES STEWART III, MIT ELECTION DATA + SCIENCE LAB, HOW WE VOTED IN 2020: A FIRST LOOK AT THE SURVEY OF THE PERFORMANCE OF AMERICAN ELECTIONS (2020), http://electionlab.mit.edu/sites/default/files/2020-12/How-we-voted-in-2020-v01.pdf [https://perma.cc/9KS4-A3PX].

[42] Abigail Censky, *How Misinformation Lit the Fire Under a Year of Political Chaos in Michigan*, NPR (Jan. 1, 2021), https://www.npr.org/2021/01/01/952528193/how-misinformation-lit-the-fire-under-a-year-of-political-chaos-in-michigan [https://perma.cc/TWQ9-GZWK].

[43] William Cummings et al., *By the Numbers: President Donald Trump's Failed Efforts to Overturn the Election*, USA TODAY NEWS (Jan. 6, 2021, 10:50 AM), https://www.usatoday.com/in-depth/news/politics/elections/2021/01/06/trumps-failed-efforts-overturn-election-numbers/4130307001/ [https://perma.cc/9KX2-KETF]; Tucker Higgins, *Supreme Court Refuses Quick Action on Last-Ditch Trump Election Lawsuits*, CNBC (Jan. 11, 2021, 3:53 PM), https://www.cnbc.com/2021/01/11/supreme-court-refuses-quick-action-on-trump-election-lawsuits.html [https://perma.cc/6TNA-UJ5Q].

[44] Robert O'Harrow Jr., *Rallies Ahead of Capitol Riot Were Planned by Established Washington Insiders*, WASH. POST (Jan. 17, 2021), https://www-washingtonpost-com.proxygw.wrlc.org/investigations/capitol-rally-organizers-before-riots/2021/01/16/tigations/capitol-rally-organizers-before-riots/2021/01/16/c5b40250-552d-11eb-a931-5b162d0d033d_story.html [https://perma.cc/TWQ9-GZWK].

member of Congress has claimed that she and other representatives were nearly killed.[45]

The prevalence of this conspiracy theory, fueled by former President Trump himself, has illustrated the deadly ramifications of allowing widespread disinformation. For example, the day after the Electoral College certified President Joe Biden's victory, Donald Trump tweeted: "Tremendous evidence pouring in on voter fraud. There has never been anything like this in our Country!"[46] The "evidence" that the former President was referring to was rejected by every court in which he brought suits relating to the election. However, then-President Trump's efforts to undermine the election results began far prior to the Electoral College's certification—as early as May 2020, Trump was making claims about potential voter fraud.[47] The issue is further exacerbated by taking into account that social media sites profit off the purchase of advertising, whether or not it is accurate. Social media sites should not be permitted to profit from the purveyance of disinformation, especially when this disinformation has deadly ramifications.

C. *Exploring Facebook and Twitter's Approaches to Regulating Political Advertising and Why They Should Be Held Accountable*

Although social media sites are considered the "middlemen" when it comes to advertising, they still have a moral and ethical responsibility to take action against procedural election advertising.[48] Social media sites have played a large role in expanding access to information on the Internet, but allowing this expanded access to go entirely unchecked permits and even promotes widespread disinformation.[49] Beyond this, some social media sites have engaged in anticompetitive behaviors, making it easier for them to govern as they see fit with no marketplace pressures.[50]

These social media sites actually profit from the prevalence of misinformation on their platforms. U.S. House Representative David

[45] Jack Healy, *These Are the 5 People Who Died in the Capitol Riot*, N.Y. TIMES (Feb. 22. 2021), https://www.nytimes.com/2021/01/11/us/who-died-in-capitol-building-attack.html [https://perma.cc/U9EL-PQZQ]; Barbara Sprunt, *'Many Of Us Narrowly Escaped Death': Rep. Ocasio-Cortez Recounts Capitol Insurrection*, NPR (Jan. 13, 2021), https://www.npr.org/sections/trump-impeachment-effort-live-updates/2021/01/13/956398483/many-of-us-narrowly-escaped-death-rep-ocasio-cortez-recounts-capitol-insurrectio [https://perma.cc/3KHU-8EP5].

[46] CBSLA Staff, *Trump Tweets About Voter Fraud After Biden Electoral College Victory*, CBS L.A. (Dec. 15, 2020, 4:19 PM), https://losangeles.cbslocal.com/2020/12/15/trump-tweets-about-voter-fraud-after-biden-electoral-college-victory/.

[47] *Trump Makes Unsubstantiated Claim that Mail-in Ballots Will Lead to Voter Fraud*, TWITTER (May 26, 2020), https://twitter.com/i/events/1265330601034256384?lang=en [https://perma.cc/3YU3-FSGF].

[48] Brian Stauffer, *Social Media's Moral Reckoning: Changing the Terms of Engagement with Silicon Valley*, HUM. RTS. WATCH (2019), https://www.hrw.org/world-report/2019/country-chapters/global-6# [https://perma.cc/L2L6-GGBT].

[49] *Id.*

[50] *Id.*

Cicilline, who is leading an antitrust subcommittee investigation of tech giants, has emphasized that allowing the promulgation of misinformation and disinformation is actually a business decision which profits the companies.[51] Essentially, engagement drives profits, so removing the misinformation and disinformation that are producing engagement cuts down on the companies' profits.[52] House Speaker Nancy Pelosi has described social media sites' business model as one that "capture[s] your time and attention, even if it's at the expense of the truth."[53] Social media sites not only make money by selling ads, but by tracking users and selling their information and data.[54] With less engagement, there is less information and data available to sell.[55]

Although the federal government has the option of going after those who purchase advertising space and use it for nefarious purposes, providing the middlemen with an incentive to restrict this information will reduce the amount of disinformation that is actually disseminated. This may be analogized to selling a product in a store that does not contain the appropriate warning labels—if a person purchases a product and is injured by it, the person would likely try to hold both the store distributing the product and the creator of the product liable, even though the store only serves as the middleman. This is an aspect of tort law referred to as products liability, in which a party injured by a product may attempt to hold any parties involved in the "chain of manufacture" liable for their injury.[56] This approach encourages distributors, the "middlemen" of products, to take care in selecting which products to carry and to err on the side of not carrying products that could open them up to liability. In the same manner, permitting liability for social media sites that do not take action to prevent the spread of disinformation would encourage them to develop more stringent policies to insulate themselves from liability.

"Traditional media" such as broadcast television have developed norms for political advertising, but these norms have not transferred to new forms of media such as social media.[57] For example, cable networks have developed norms around fact-checking political ads for inaccuracies, and may refuse to air ads for that reason.[58] Two such ads, which CNN refused to air, were later

[51] Tatyana Hopkins, *Social Media Companies Profiting from Misinformation*, GW TODAY (June 19, 2020), https://gwtoday.gwu.edu/social-media-companies-profiting-misinformation [https://perma.cc/NB6F-ZEPX].

[52] *Id.*

[53] *Id.*

[54] Chirag Shah, *It's Not Just a Social Media Problem — How Search Engines Spread Misinformation*, CONVERSATION (Mar. 10, 2021), https://theconversation.com/its-not-just-a-social-media-problem-how-search-engines-spread-misinformation-152155 [https://perma.cc/G9PN-JKCW].

[55] *Id.*

[56] *Products Liability*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/products_liability [https://perma.cc/Y8FM-ZSD6].

[57] Amber Herrle, *Regulating fact from fiction: Disinformation in political advertising*, BROOKINGS INST. (Dec. 20, 2019), https://www.brookings.edu/blog/fixgov/2019/12/20/regulating-fact-from-fiction-disinformation-in-political-advertising/ [https://perma.cc/M322-G28P].

[58] *Id.*

featured on Facebook.[59] The ads in question denounced the House Democrats' impeachment inquiry as a coup.[60]

Social media sites have taken somewhat different approaches in attempting to regulate political advertising. Twitter has taken an extreme approach when compared to other websites such as Facebook—it has globally banned the paid promotion of political content.[61] This means that while political candidates are permitted to have accounts and tweet on them—which are expressly labeled with their candidacy—they may not pay for their content to be promoted.[62] The ban extends to any political content, defined as referencing "a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive, or judicial outcome."[63]

1. Twitter's Policies

Over a year before the 2020 election, Twitter's CEO, Jack Dorsey, announced that Twitter was banning political advertising altogether.[64] This policy prohibits ads of any type by candidates, political parties, elected government officials, or appointed government officials.[65] When it comes to the 2020 Presidential election, Twitter also took steps to combat disinformation by users, even though the content wasn't promoted through the site.[66] This highlights an important distinction in approaches—some sites are more hesitant than others to regulate content that users post that is not paid for. However, Twitter is willing to engage in regulation of user-generated content. On its blog, Twitter provided a lengthy explanation of the steps and policies it was putting into place in anticipation of the 2020 election.[67] The most significant step Twitter took was to flag tweets that violated its Civic Integrity Policy.[68] Further, tweets with misleading information from U.S. political figures were flagged with a warning that users had to tap or click before being able to view the tweet.[69] In addition, Twitter requires that users

[59] *Id.*

[60] Michael M. Grynbaum & Tiffany Hsu, *CNN Rejects 2 Trump Campaign Ads, Citing Inaccuracies*, N.Y. TIMES (Oct. 3, 2019), https://www.nytimes.com/2019/10/03/business/media/cnn-trump-campaign-ad.html [https://perma.cc/8NJZ-CBUX].

[61] *Political Content*, TWITTER, https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html [https://perma.cc/BEB5-DTPH].

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] Kate Conger, *How Twitter Policed Trump During the Election*, N.Y. TIMES (Nov. 6, 2020), https://www.nytimes.com/2020/11/06/technology/trump-twitter-labels-election.html [https://perma.cc/SME9-BTLE].

[67] Vijaya Gadde & Kayvon Beykpour, *Additional Steps We're Taking Ahead of the 2020 US Election*, TWITTER: BLOG (Nov. 2, 2020), https://blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html [https://perma.cc/7WQG-VUDH].

[68] *Id.*

[69] *Id.*

who are also U.S. election candidates have an election label on their Twitter profile "contain[ing] information about the office the candidate is running for, the state the office is located in, and (when applicable) the district number."[70] Twitter's specific election policy, focused on election integrity, is called the Civic Integrity Policy.[71] Labeled January 2021, the policy states:

> You may not use Twitter's services for the purpose of manipulating or interfering in elections or other civic processes. This includes posting or sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process. In addition, we may label and reduce the visibility of Tweets containing false or misleading information about civic processes in order to provide additional context.[72]

Twitter reserves the right to flag or remove tweets in violation of this policy.[73] The Civic Integrity Policy had previously been updated prior to the 2020 election, in anticipation of the potential purveyance of misinformation on Twitter's platform.[74]

Although the policy may seem extreme, it may have paid off in terms of slowing the spread of disinformation. The Election Integrity Partnership, which "support[s] real-time information exchange between the research community, election officials, government agencies, civil society organizations, and social media platforms," performed an analysis on one of then-President Trump's tweets.[75] Before Twitter labeled the former president's tweet with a misinformation notification that users had to click through, it was engaged with (shared or replied to) 827 times per minute.[76] After the label, engagement dropped approximately 82% to engagements occurring 151 times per minute.[77] Nonetheless, a group dedicated to

[70] *About Election Labels on Twitter*, TWITTER: HELP CTR., https://help.twitter.com/en/using-twitter/election-labels [https://perma.cc/9K8U-AX7W].

[71] *Civic Integrity Policy*, TWITTER: HELP CTR., https://help.twitter.com/en/rules-and-policies/election-integrity-policy [https://perma.cc/Q929-WKSE].

[72] *Id.*

[73] *Id.*

[74] Ry Crist, *Twitter Lays Out Plan to Protect the Election from False or Misleading Tweets*, CNET (Sept. 10, 2020, 10:59 AM), https://www.cnet.com/news/twitter-lays-out-its-plan-to-protect-the-election-from-false-or-misleading-tweets/ [https://perma.cc/X8AH-LP4V].

[75] ELECTION INTEGRITY P'SHIP, THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION (2021), https://www.eipartnership.net/ [https://perma.cc/XM4W-AWFN]; Kellen Browning, *After Twitter Labels Trump's Tweet About Pennsylvania, Its Spread Slows*, N.Y. TIMES (Nov. 3, 2020, 2:15 PM), https://www.nytimes.com/2020/11/03/technology/after-twitter-labels-trumps-tweet-about-pennsylvania-its-spread-slows.html [https://perma.cc/8A59-G7MF].

[76] Kellen Browning, *After Twitter Labels Trump's Tweet About Pennsylvania, Its Spread Slows*, N.Y. TIMES (Nov. 3, 2020, 2:15 PM), https://www.nytimes.com/2020/11/03/technology/after-twitter-labels-trumps-tweet-about-pennsylvania-its-spread-slows.html [https://perma.cc/K3DH-RWWQ].

[77] *Id.*

combating misinformation says that Twitter's policies would be more effective if decisions about whether and how to flag a tweet were made more quickly.[78]

Finally, following the January 6th, 2021 Capitol riots, Twitter chose to de-platform then-President Trump for inciting violence.[79] CEO Jack Dorsey made the call, announcing that the former President would be banned permanently from Twitter on the Friday following the riots.[80]

2. Facebook's Policies

Facebook has taken a different and arguably more hands-off approach. However, Facebook's approach is still surprising considering Mark Zuckerberg's previous stance on regulating political speech. In October 2019, Zuckerberg gave a speech at Georgetown University, emphasizing his belief in Facebook as a proponent of free speech.[81] This speech came after Senator and then-presidential candidate Elizabeth Warren accused Zuckerberg of making Facebook a disinformation-for-profit service.[82] In particular, Zuckerberg emphasized that "greater progress requires confronting ideas that challenge us," invoking historical figures such as Frederick Douglass and Dr. Martin Luther King Jr., as well as First Amendment freedoms of speech and expression.[83]

Facebook's policies surrounding the 2020 election have seemed to backpedal from Zuckerberg's October 2019 stance. These policies are primarily focused on ads surrounding procedural aspects of elections, including the promotion of reliable election results and stopping voter interference and fraud.[84] Facebook has provided a Voting Information Center (VIC), which the Bipartisan Policy Center has supplemented with facts about voting, including voting by mail.[85] The VIC served as a source of information for election results, showing the status of the presidential, U.S. Senate, U.S. House, and gubernatorial races.[86] It also provided information on voter registration and the ability for users to check their registration.[87] These

[78] *Id.*

[79] Dylan Byers, *How Facebook and Twitter Decided to Take Down Trump's Accounts*, NBC NEWS (Jan. 14, 2021, 5:01 PM), https://www.nbcnews.com/tech/tech-news/how-facebook-twitter-decided-take-down-trump-s-accounts-n1254317 [https://perma.cc/4YKU-XHQ7].

[80] *Id.*

[81] Cecilia Kang & Mike Isaac, *Defiant Zuckerberg Says Facebook Won't Police Political Speech*, N.Y. TIMES (Oct. 21, 2019), https://www.nytimes.com/2019/10/17/business/zuckerberg-facebook-free-speech.html [https://perma.cc/6BU6-WNZD].

[82] Elizabeth Warren (@ewarren), TWITTER (Oct. 12, 2019, 10:01 AM), https://twitter.com/ewarren/status/1183019880867680256 [https://perma.cc/UT3S-GJER].

[83] *See* Kang & Isaac, *supra* note 81.

[84] FACEBOOK, FACEBOOK'S POLICIES FOR ELECTIONS AND VOTING: WHAT YOU NEED TO KNOW (2020), https://about.fb.com/wp-content/uploads/2020/10/Facebooks-Policies-for-Elections-and-Voting.pdf [https://perma.cc/S7GZ-KNBJ].

[85] *Id.*

[86] *Id.*

[87] *Id.*

procedures seemed to be aimed at combating claims that voting by mail is not a legitimate means of voting and that voting in person would cause people to contract COVID-19. Facebook also committed to removing ads by candidates or parties declaring a premature victory, and labeling posts from presidential candidates.[88] These labels noted that vote counting was still in progress and a winner had not yet been declared.[89]

Facebook has distinguished between procedural and substantive political ads in its policies based on its approach to the different types of ads. While ads promoting candidates were previously largely unrestricted, Facebook has expressly prohibited "explicit and implicit misrepresentation of the dates, locations, times and methods for voting or voter registration," as well as "misrepresentation of who can vote, qualifications for voting, whether a vote will be counted, and what information and/or materials must be provided in order to vote."[90] Ads of this sort are procedural because they concern voter registration and polling places. Thus, Facebook approaches them differently than ads oriented toward promoting a specific candidate or cause.

Facebook further instituted the policy that in the week leading up to the November 3, 2020 election, it would not permit any new political ads.[91] However, this policy was criticized for not having much of an effect because users are still able to see political ads generally, and, at the time the policy was instituted, millions of Americans had already cast their votes due to the early voting and mail-in ballot procedures instituted in several states due to the COVID-19 pandemic.[92] Therefore, the policy did not do much to protect those who had already voted, which was not an insignificant number of people.

On November 3, 2020, Facebook took the more drastic step of implementing a gag rule on "ads about social issues, politics or elections."[93] The company also implemented a policy restricting the content of certain ads, including ads claiming widespread voter fraud, ads with premature claims of election victory, ads that delegitimize lawful methods of voting or vote-counting as illegal, and ads that delegitimize an election as fraudulent "because the result can't be determined on the final day of voting and/or before ballots received after the final day of voting are lawfully counted."[94] Ads of this type were expressly prohibited.[95] Additionally, Facebook banned

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *See* Steve Kovach, *Facebook's Ban on New Political Ads Won't Change Anything*, CNBC (Sept. 3, 2020, 3:44 PM), https://www.cnbc.com/2020/09/03/facebooks-ban-on-new-political-ads-wont-change-anything.html [https://perma.cc/L943-5MHC].

[92] *See id.*

[93] *What to Know About Facebook Advertising Around the Election,* FACEBOOK (Oct. 26, 2020), https://www.facebook.com/business/news/facebook-ads-restriction-2020-us-election [https://perma.cc/S9KE-T2L9].

[94] *Information on Prohibited Ads Related to Voting and Ads About Social Issues, Elections*, META, https://www.facebook.com/business/help/253606115684173.

[95] *Id.*

ads regarding the Georgia runoff election starting on January 6, 2021.[96] Until March 3, 2021, Facebook had not yet announced when the ban would be lifted.[97] On that day, Facebook announced that the ban would be lifted starting on March 4, 2021.[98]

In terms of content moderation, Facebook has taken fewer steps than Twitter. While both social media sites have some form of flagging available for false or misleading information about elections, the only posts that Facebook agreed to take down were those expressly stating that if an individual goes to a polling place, they will contract COVID-19.[99] Other user-generated content that was not purchased, but involved false or misleading information regarding election procedures, remained on the website with flags of some sort.[100]

Finally, Facebook also chose to ban then-President Trump in light of the January 6th Capitol riots.[101] The Facebook Oversight Board reviewed the ban in May 2021, and upheld it, but added that the case should be re-reviewed in six months.[102] Not only that, Facebook has gone further, banning the "voice of Trump" from its platform.[103] Lara Trump posted a video in which she interviewed the former President, and the platform took the video down, explaining that it would remove "further content posted in the voice of Donald Trump."[104]

3. Parler's Policies

Parler is a smaller social media site that entered the spotlight in early 2020.[105] Its popularity grew throughout 2020 as conservative media stars joined and promoted the social media platform.[106] Audiences migrated to the site from Facebook and Twitter, interested in the lack of "censorship" occurring on Parler in comparison to other sites.[107] However, this perceived lack of censorship led to Parler's partial demise—after the January 6th Capitol riots, the site was removed from Google and Apple application stores, and

[96] Elena Schneider, *Facebook Lifts Political Ad Ban*, POLITICO (Mar. 3, 2021, 2:15 PM), https://www.politico.com/news/2021/03/03/facebook-lifts-political-ad-ban-473368 [https://perma.cc/C4T2-44EE].

[97] *See* Rodriguez, *supra* note 14.

[98] *See* Schneider, *supra* note 96.

[99] Steve Kovach, *Facebook to Ban New Political Ads in Week Before Presidential Election*, CNBC (Sept. 3, 2020), https://www.cnbc.com/2020/09/03/facebook-to-ban-political-ads-in-week-before-presidential-election.html [https://perma.cc/UP6Q-UPND].

[100] *Id.*

[101] *See* Byers, *supra* note 79.

[102] Mike Isaac, *Facebook Oversight Board Upholds Social Network's Ban of Trump*, N.Y. TIMES (Oct. 21, 2021), https://www.nytimes.com/2021/05/05/technology/facebook-trump-ban-upheld.html [https://perma.cc/J4GD-HX63].

[103] *Facebook Bans 'Voice of Trump' From Platform*, BBC NEWS (Apr. 1, 2021), https://www.bbc.com/news/world-us-canada-56598862 [https://perma.cc/F5U7-KVA6].

[104] *Id.*

[105] David Strom, *The Rise and Fall of Parler*, AVAST (Jan. 11, 2021), https://blog.avast.com/the-rise-and-fall-of-parler-avast [https://perma.cc/E5KR-FKDC].

[106] *Id.*

[107] *Id.*

Amazon revoked its server access.[108] Parler came back online on February 15, 2021.[109]

Parler's Community Guidelines, last updated on November 2, 2021, contain two pages enumerating Parler's two guiding principles in removing content.[110] The first principle is that Parler will remove content that indicates use of Parler as a tool for a crime, civil tort, or other unlawful act.[111] The second is that users may not post spam or use bots.[112] As compared with Facebook and Twitter's policies, these community guidelines are highly underdeveloped.

Some at Parler have apparently pushed for content moderation, but this has not been fruitful—former CEO John Matze was terminated on January 29, 2021, allegedly due to his push for stronger content moderation.[113] This isn't surprising, given that Parler prides itself on being a free speech platform free of censorship.[114]

4. Comparisons

Each of Facebook's and Twitter's procedures have their challenges, and neither is a flawless approach to the issue. Twitter's blanket ban on political ads may level the playing field in terms of preventing candidates with more money from having larger platforms, but the number of followers and algorithms also come into play and may disadvantage new and smaller challenging candidates who do not yet have firm support.[115] Further, Twitter has ventured into user content moderation, a solution that the Federal Government would want to stay away from to avoid First Amendment implications.[116] Regulation of individual users' speech on social media sites is largely new territory, and mandating that social media sites regulate individual users would be a broad overhaul of the way social media sites currently operate and would very likely violate the First Amendment. Finally, in contrast to Facebook, Twitter did not provide links to a VIC, which is a helpful tool that makes reliable information about elections more accessible. This procedure would have helped in combatting disinformation and allowing users to be more informed about voting generally.

Facebook's approach to political advertising seems like a more feasible model for the Federal Government to orient its own regulations around. First,

[108] *Id.*

[109] Stephanie Mlot, *Parler Is Back Online and 'Open to Americans of All Viewpoints'*, PCMAG (Feb. 16, 2021), https://www.pcmag.com/news/parler-is-back-online-and-open-to-americans-of-all-viewpoints [https://perma.cc/A4DJ-CP42].

[110] *Community Guidelines*, PARLER (Feb. 14, 2021), https://legal.parler.com/documents/guidelines.pdf [https://perma.cc/H5RB-BHU5].

[111] *Id.*

[112] *Id.*

[113] Michael Kan, *Parler CEO Fired Over Content Moderation Push*, PCMAG (Feb. 4, 2021), https://www.pcmag.com/news/parler-ceo-fired-over-content-moderation-push [https://perma.cc/D4VS-ZKUD].

[114] *About Parler*, PARLER, https://parler.com/main.php (last visited Nov. 27, 2021).

[115] *See Political Content*, *supra* note 61.

[116] *See Civil Integrity Policy*, *supra* note 72.

Facebook has expressly banned procedural election disinformation, which has extremely important implications for democracy.[117] The protection of social media users from procedural election disinformation allows them greater accessibility to accurate information, which will likely lead to more votes successfully being cast and counted and will likely help prevent voter disenfranchisement. Second, Facebook has made a distinction between procedural election advertising and other political advertising about candidates, previously applying fewer restrictions to the latter.[118] This sets a precedent for that same distinction in federal regulations, making them more likely to withstand a First Amendment legal challenge because they are oriented around facts that may be proven as true or false, rather than speech of a political nature which the First Amendment was designed to protect.[119] The only Facebook policy that federal agencies would likely want to avoid implementing would be Facebook's blanket ban on any ads concerning political and social issues for four months after the election.[120] This policy, if applied by a federal agency, would almost certainly violate the First Amendment as an unconstitutional government restriction on protected speech.[121]

D. The Federal Trade Commission Has Jurisdiction in this Area Because There Is Precedent for Regulation of Information and the Information at Issue Here Is Not Political Speech

At first glance, one might think that this type of information should not be regulated at all, because it involves politics in some capacity, which is the crux of First Amendment jurisprudence. If it is regulated, one might think that either the Federal Communications Commission (FCC) or the Federal Election Commission (FEC) are best suited for the job. However, these two government agencies have extremely limited jurisdiction in this area. Further, significant barriers exist to creating a new agency dedicated to this particular area of regulation. As such, the job of regulating procedural election information is best suited to the Federal Trade Commission (FTC), despite the information's pseudo-political nature.

The FCC is not the right federal agency to regulate this type of content because it has limited jurisdiction in this area. The FCC's primary focus is "regulat[ing] interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S.

[117] *See Information on Prohibited Ads Related to Voting and Ads About Social Issues, Elections*, *supra* note 94.

[118] *See* FACEBOOK, *supra* note 84.

[119] Ellada Gamreklidze, *Political Speech Protection and the Supreme Court of the United States*, NAT'L COMMC'N ASS'N (Oct. 1, 2015), https://www.natcom.org/communication-currents/political-speech-protection-and-supreme-court-united-states [https://perma.cc/2D5Z-NW82].

[120] *See What to Know About Facebook Advertising Around the Election*, *supra* note 93.

[121] *See* Gamreklidze, *supra* note 119.

territories."[122] The FCC does regulate some areas of political advertising, but its regulations are limited to broadcast stations, cable television, and direct broadcast satellite service.[123] As such, the FCC is primarily focused on communications infrastructure, rather than any form of content moderation, user-generated or purchased.[124] The only potential exception here is section 230, but this Act does not actually grant the FCC any authority over ISPs.[125] The issue of FCC jurisdiction regarding section 230 was brought into question in 2020, after the National Telecommunications and Information Administration submitted a petition for rulemaking with the FCC, seeking clarification of the provisions of section 230.[126] The petition garnered over 1,000 comments in response, many of which expressed brief support for the petition filed at the direction of then-President Donald Trump.[127] However, many trade associations and think tanks also provided comments on the petition, insisting that the FCC does not have the ability or jurisdiction to interpret § 230.[128] Although section 230 is tangentially related to procedural election information, these responses illustrate how this type of information is likely not within the FCC's jurisdiction to regulate.

The FEC similarly has virtually no authority to regulate procedural election information. The FEC's focus is on campaign finance law, including public disclosure of the funds that candidates raise.[129] The FEC was initially created to "administer such reform efforts as limiting campaign contributions, facilitating disclosure of campaign contributions and overseeing public funding of presidential elections."[130] Because the FEC is focused so narrowly on campaign finance, it is unlikely it would feasibly have jurisdiction in this area.

The FTC is the most likely of these three agencies to have jurisdiction in this area. The Federal Trade Commission Act of 1914 empowers the FTC to "prevent unfair methods of competition and unfair acts or practices in or affecting commerce."[131] Since its inception in 1914, assorted Congressional

[122] *What We Do*, FCC, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/AT6T-NEBC].

[123] *Statutes and Rules on Candidate Appearances & Advertising*, FCC , https://www.fcc.gov/media/policy/statutes-and-rules-candidate-appearances-advertising [https://perma.cc/RRR4-G2JB].

[124] Devin Coldewey, *Who Regulates Social Media? Good Question!*, TECHCRUNCH (Oct. 19, 2020), https://techcrunch.com/2020/10/19/who-regulates-social-media/ [https://perma.cc/9523-3XNY].

[125] *Id.*

[126] Petition for Rulemaking of the Nat'l Telecomms. & Info. Admin. at 15-16, Section 230 of the Commc'ns. Decency Act of 1934, RM-11862 (Aug. 3, 2020) [hereinafter Petition],

[127] Josh Turner et al., *230 Petition Commenters Question FCC Authority, Argue NTIA Proposal Unconstitutional, Bad for Tech*, WILEY: CONNECT (Sept. 4, 2020), https://www.wileyconnect.com/home/2020/9/4/230-petition-commenters-question-fcc-authority-argue-ntia-proposal-unconstitutional-bad-for-tech [https://perma.cc/HK53-MNUY].

[128] *Id.*

[129] *Mission and History*, FED. ELECTIONS COMM'N, https://www.fec.gov/about/mission-and-history/ [https://perma.cc/PH3M-SWVL].

[130] *Federal Election Commission Regulates Presidential Campaigns,* U.S. EMBASSY IN NOR., https://no.usembassy.gov/education-culture/about-the-usa/us-elections/federal-election-commission-regulates-presidential-campaigns/ [https://perma.cc/DC6L-5BM3].

[131] 15 U.S.C. § 45.

statutes have delegated authority to the FTC in varying capacities, especially in the areas of promoting competition and consumer protection.[132] The FTC's power has historically included regulation of advertising, as illustrated in its Truth in Advertising laws.[133] This type of regulation has typically excluded political advertising.[134]

However, the FTC's regulation exception for political advertising is understood to involve ads purchased by candidates encouraging individuals to vote for them and expressing their stances or policies.[135] Political speech in this context involves ideas, opinions, stances, and perspectives.[136] This information is different in nature from procedural election information including polling places, registration information, and the status of election races because the latter is factual information. Procedural information about elections is either true or false, whereas the political advertising exempt from FTC regulation is "political speech" of the nature that the First Amendment is meant to protect.

The Supreme Court has distinguished advertising and commercial speech as distinct from political speech. In *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, the defendants were convicted of violating a Virginia statute that deemed pharmacists guilty of unprofessional conduct for publishing advertisements for drugs available exclusively by prescription.[137] This statute effectively prevented pharmacists from disseminating any pricing information, making a competitive market more difficult.[138] The Supreme Court struck down the statute, holding that although commercial speech is protected by the First Amendment, it does not have the same value as political speech and thus may be subject to some regulation.[139]

Not only that, but the FTC's existence has also illustrated that the Court does not consider the two types of speech to be the same. If commercial and political speech were of the same caliber, the FTC would not be able to regulate commercial speech in any capacity, as this regulation would be seen as a violation of the First Amendment. Therefore, Supreme Court jurisprudence has illustrated that even when speech affords some First Amendment protections, that does not necessarily mean that it is exempt from regulations entirely.[140]

[132] *Statutes Enforced or Administered by the Commission,* FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes [https://perma.cc/B4BF-YDN7].

[133] *See Truth In Advertising*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/truth-advertising [https://perma.cc/CUV2-SNSX].

[134] Liza Lucas, *VERIFY: No, Truth In Advertising Laws Do Not Apply to Political Ads*, WCNC (Oct. 23, 2020), https://www.wcnc.com/article/news/verify/political-ads-truth-in-advertising-laws-election-2020/85-a9b12c2b-c3c7-4284-9f8e-e0e89dc47f85 [https://perma.cc/WZ5U-JCES].

[135] *Id.*

[136] *Id.*

[137] Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 748-50 (1975).

[138] *Id.* at 752-54.

[139] *Id.* at 770-71.

[140] *Id.*

Considering these categories of speech, the question then becomes under which category procedural information about elections is a better fit. This type of information could be political speech because it relates to elections and therefore is inherently political. However, in its policies, Facebook has distinguished procedural election information from political speech that it has previously chosen not to regulate, indicating that it does not view procedural election information as political speech.[141] This approach reflects the notion that procedural election information is separate and distinct from political speech that expresses viewpoints or encourages an information consumer to vote for or against a specific candidate or issue.

However, commercial speech typically "does no more than propose a commercial transaction."[142] Procedural election information is not well-suited to fit under this category either, because it does not advertise a transaction. Most likely, procedural information about elections falls into neither category, but nonetheless falls under the jurisdiction of the FTC due to its regulation in tangentially related areas and the fact that procedural election information can be easily verified as accurate or rejected as misleading.

The FTC engages in regulation in a broad array of categories, encompassed by a theme of protecting consumers and promoting competition.[143] The FTC regulates not only products themselves, but the advertisement of these products and advertising in general.[144] Many statutes that delegate authority to the FTC do not necessarily regulate specific products, but rather regulate or involve the FTC in regulating information about products.[145]

The Sober Truth on Preventing Underage Drinking Act (STOP Act) is a prime example of FTC involvement in regulating information.[146] This Act established the "Interagency Coordinating Committee on the Prevention of Underage Drinking, of which the FTC is a member."[147] This Act is part of a government initiative to reduce underage drinking in the name of public health.[148] The Committee is tasked with policy and program development.[149] The FTC in particular is tasked with measuring underage exposure to messages about alcohol in advertising and "the entertainment media."[150] The FTC's power in this area is to make a report not only concerning for-profit advertising, but how alcohol and underage drinking are portrayed in the media.[151] This approach illustrates that the FTC's jurisdiction may extend beyond mere regulation of for-profit advertising to include reports and analysis of information and exposure to media that goes beyond strictly advertising.

[141] *See* FACEBOOK, *supra* note 84.

[142] *See Va. State Bd. of Pharmacy*, 425 U.S. at 760-763.

[143] *See Truth In Advertising*, *supra* note 133.

[144] *See id.*

[145] *See id.*

[146] 42 U.S.C. § 290bb-25b.

[147] *Id.* § 290bb-25b(c).

[148] *Id.* § 290bb-25b.

[149] *Id.* § 290bb-25b(c)(1)(D).

[150] *Id.* § 290bb-25b(c)(1)(F).

[151] *Id.* § 290bb-25b(c)(1)(F).

Another example of the FTC regulating information is the Protecting Children in the 21st Century Act.[152] This Act tasks the FTC with "encourag[ing] best practices for internet safety and facilitat[ing] access to awareness and education campaigns."[153] In so doing, the FTC is required to submit a report to Congress about the activities it has carried out under the Act.[154] This delegation is different from the STOP Act because it empowers the FTC more extensively, as it has the ability to engage in education campaigns and promulgate best practices.[155] As such, it illustrates that the FTC can do more than merely research and report on areas of information regulation—it may actually be able to engage in some form of regulation.

Based on Congress' ability to delegate some form of regulation of information in these areas, it is similarly feasible for Congress to narrowly and specifically delegate regulation of procedural election information advertised on social media sites. The scope of this delegation would have to be very narrow so as to not invoke First Amendment protections or the nondelegation doctrine. These potential challenges are explored in Part III below.

III. ANALYSIS

A. *Potential Legal Challenges*

1. Delegation to the FTC Will Help Insulate Regulations from Judicial Scrutiny Under the *Chevron* Doctrine

Delegation to the FTC is a superior legal solution than legislation for two reasons. First, the Supreme Court is more hesitant to get involved in regulations that have been delegated to an agency than in legislation regulating a certain area, as long as the delegation is not itself unconstitutional. Second, delegation allows the FTC, which is better equipped and in a better position to promulgate these regulations, to consult the social media sites they will be regulating and develop best practices based in part on these consultations.

Generally speaking, delegations of authority to federal agencies are upheld as long as the legislature includes an "intelligible principle" for the delegation.[156] The "intelligible principle" doctrine was mostly famously discussed in *Whitman v. American Trucking Associations, Inc*. In that case, legislation required the Environmental Protection Agency (EPA) to promulgate air quality standards.[157] The plaintiffs brought suit because they didn't like the standards the EPA promulgated, so they challenged the

[152] 15 U.S.C. §§ 6552-6553.

[153] *Id.* § 6552.

[154] *Id.* § 6553.

[155] *Id.* § 6552.

[156] Whitman v. Am. Trucking Ass'ns., 531 U.S. 457, 457-58 (2001).

[157] *Id.* at 457.

congressional delegation of authority as unconstitutional.[158] The Court determined that there was an intelligible principle in the statute delegating authority because there were limits on the EPA's authority.[159] The Supreme Court has rarely found that there is not an intelligible principle in a statute delegating authority—it will generally only find lack of an intelligible principle where there is no guidance or where authority conferred is very broad and with little justification.[160]

As long as the delegation is constitutional, the Supreme Court would likely uphold the agency action under *Chevron* deference.[161] *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.* was a Supreme Court case also involving the EPA in which the plaintiffs challenged the EPA's construction of a statute as unconstitutional.[162] The Court declined to hold that either the delegation or the EPA's construction of the statute was impermissible.[163] Here, the Court afforded significant deference to federal agency interpretation of a delegating statute, and noted that an agency's interpretation need not be the best interpretation, merely that the interpretation be permissible under the statute.[164] In particular, the Court noted that agencies are in the best position to interpret statutes that delegate authority, because they have resources and subject matter expertise.[165]

Some states have seen success in instituting legislation in this area. As of 2014, twenty-seven states prohibited misrepresentation in some form within campaign advertising.[166] The categories of false statements or misrepresentation in these laws includes incumbency, endorsements, voter information, veteran status, false statements, and other prohibitions.[167] However, in four of those states, legislation in these areas has been struck down as unconstitutional.[168] This does not bode well for Congress if it seeks to legislate in this area rather than delegating the task to a federal agency. Further, Congress does not really have the resources to regulate this area itself, and would at a minimum have to delegate the task of enforcement to an agency. Because it does not have subject matter expertise in the area, it may as well delegate the development of regulations to an agency instead.

[158] *Id.* at 457-59.

[159] *Id.* at 458-59.

[160] *Id.* at 474.

[161] Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 838 (1984).

[162] *Id.* at 837-38.

[163] *Id.*

[164] *Id.* at 843.

[165] *Id.* at 865-66.

[166] Mark Listes & Wendy Underhill, *Campaign Fair Practice Laws (Is There a Right to Lie?)*, NAT'L CONF. OF STATE LEGISLATURES (Oct. 29, 2014), https://www.ncsl.org/research/elections-and-campaigns/campaign-fair-practice-laws-is-there-a-right-to-lie.aspx [https://perma.cc/MNH4-K95E].

[167] *Id.*

[168] Matt Vasilogambros, *Political Candidates Don't Always Tell the Truth (And You Can't Make Them)*, PEW CHARITABLE TRUST (Mar. 21, 2019), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/03/21/political-candidates-dont-always-tell-the-truth [https://perma.cc/5WC5-4NDH].

Therefore, under the intelligible principle standard, *Chevron* deference, and general principles of administrative law, the FTC is best suited to promulgate regulations in this area.

2. First Amendment Jurisprudence in this Area Is Unclear

If a litigant chose to go after the substance of the regulations, rather than Congress' authority to delegate or the FTC's jurisdiction in this area, it is unclear how it would play out given Supreme Court First Amendment precedent. Major considerations include whether social media sites are analyzed as public forums and the nature of the speech at issue.

Public forums are public or government-owned spaces in which speech generally may not be regulated.[169] Supreme Court precedent indicates that public forums are not created where the activity at issue is commercial in nature or where the forum is not open to indiscriminate public use.[170] Under this doctrine, it is unlikely that advertising space on social media sites constitutes a public forum. First, the decision to purchase advertising, even for procedural election information, is commercial in nature. In *Lehman v. City of Shaker Heights*, the Supreme Court in a plurality opinion held that a government-owned form of transit with advertising space available for purchase was not a public forum, because the activity at issue was commercial in nature.[171] The Court reasoned that the city was engaged in commerce and had chosen to limit advertising in a viewpoint-neutral way by not permitting any political advertising.[172] Second, the purchase of advertising is not open to indiscriminate public use, because users wishing to purchase advertising have to go through processes to make the purchases, including following both FTC and individual website regulations and policies.[173] Even explicit political advertising space purchased on Facebook requires disclaimers and a certification process.

However, there is an argument to be made that social media sites generally are considered public forums, since the public has access to them unless they are permanently banned for misuse. Despite this, the most convincing argument for a social media site to not be considered a public forum is that social media sites are not owned by the government—they are owned by private companies and thus are private entities. In some cases, government actors may create public forums on a social media site with a

[169] David L. Hudson Jr., *Public Forum Doctrine*, FREE SPEECH CTR. (Jan. 8, 2020), https://www.mtsu.edu/first-amendment/article/824/public-forum-doctrine [https://perma.cc/7DTK-YWVB].

[170] Lehman v. City of Shaker Heights, 418 U.S. 298, 301-303 (1973); Perry Educators' Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 47 (1983).

[171] *Lehman*, 418 U.S. at 303.

[172] *Id.* at 304.

[173] *Facebook Advertising Policies*, FACEBOOK, https://www.facebook.com/policies/ads/ (last accessed Feb. 2, 2022) [https://perma.cc/AZ4Z-M2WK].

specific profile page,[174] but generally speaking, social media sites likely would not be considered a public forum.

Further, it is unclear whether the nature of the speech here would be found to be political, commercial, or neither.[175] The Court has expressed that commercial speech "does no more than propose a transaction."[176] Within First Amendment jurisprudence, the Court has not expressly defined political speech. However, as discussed above, social media sites have distinguished political advertising from procedural election information, making it more likely that this distinction will become more widely accepted. Whether the Court views procedural election disinformation as high or low value speech may bear on how it chooses to analyze agency regulations.

Despite these confusions, this regulation would likely be considered content-based, because it regulates the content of the speech—procedural election information. Content-based regulations are reviewed under strict scrutiny, requiring a statute to be narrowly tailored to advance a compelling government interest.[177]

If the language of the statute clearly delineated that the FTC may promulgate regulations specifically in the area of procedural election information, this would more likely fulfill the narrowly tailored element of strict scrutiny, or perhaps not invoke strict scrutiny if the Court were to find that this is not the type of high value speech that the First Amendment protects absolutely. After all, false information about election results, polling places, and how to register to vote are low value when compared with the high value speech of political opinions and stances candidates express in advertisements about their candidacy.

The government has a compelling interest in promoting fair access to voting, as well as promulgating accurate information about elections. This interest is essential to democratic governance, so the Court would be inclined to find a compelling government interest here.

However, it is unclear how exactly the Supreme Court would perform analysis in the present case because the proposed legislation is to delegate to the FTC, which would subsequently promulgate regulations. Because of the level of insulation that delegation to the FTC provides, it is unclear whether the Court would choose to evaluate the content of the regulations, and if the Court did choose to evaluate, the means by which it would do so.

B. Federal Regulation Is Superior to State Regulation Because It Provides Uniformity

Although the states could individually regulate procedural election advertisements, it makes more sense to regulate at the federal level, at least

[174] Knight First Amend. Inst. v. Trump, 953 F.3d 216, 218 (2d Cir. 2020).

[175] *See supra* text accompanying notes 137-42.

[176] *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 760-763 (1975).

[177] Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 799 (2011).

advertisements regarding federal elections, to promote uniformity and to ease the burden on social media sites.

First, uniformity in how to approach procedural disinformation is highly important. If different states have different standards or procedures for how they regulate this information, disinformation could still easily be promulgated if residents of one state share screenshots or provide information via word of mouth. Further, the varying standards could cause even more confusion than the initial disinformation. For example, if one state mandates that social media sites "flag" inaccurate election information while another mandates that they remove it entirely, there would be confusion about this disparity among users of different states if they communicate amongst each other. The difference in approaches may foster distrust in regulations and undermine the entire effort if people don't believe the regulations are accurate.

Further, adhering to state-by-state regulations would place a significant burden on social media sites, because having a different approach in each state would be more difficult to adopt than a uniform approach. As a result, social media sites would likely end up adapting the strictest state's regulations, which would result in uniformity anyways. However, this would make a potentially overbroad approach the norm, running the risk of depriving social media users of information they should be able to freely view and interact with.

At a minimum, there should be uniformity in procedural advertising regulations for federal elections which concern citizens of every state. Disinformation about an election at the state level is not as harmful to individuals who do not vote in or have no personal ties to a particular state. However, federal elections concern all U.S. citizens. If one state is permitting disinformation about which candidate was chosen in a federal election, and another is not, the conflicting information across state lines would wreak havoc and cause more confusion. This would also undermine the intention of the regulations by causing social media users to distrust the inconsistencies in the regulations and thus to distrust election results generally.

C. Section 230 of the Communications Decency Act Has Opened the Door for Regulations in this Area

Section 230 of the Communications Decency Act protects Internet Service Providers (ISPs) from liability for content that its users post.[178] Throughout most of 2020, section 230 was a hot-button topic in the news, as then-President Trump and Democrats alike called for either reform or repeal of the legislation.[179] The primary argument for amending, reforming, or repealing the legislation is that its protections are overbroad, allowing ISPs to

[178] 47 U.S.C. § 230.

[179] Anshu Siripurapu, *Trump and Section 230: What to Know*, COUNCIL ON FOREIGN RELS. (Dec. 2, 2020), https://www.cfr.org/in-brief/trump-and-section-230-what-know [https://perma.cc/ED6R-UCWU].

do virtually whatever they like in terms of regulating content and advertising without facing any liability.[180]

Whatever the future of section 230 may be, it has brought about a larger conversation about the overprotected and anticompetitive nature of Big Tech, and the different ways in which this level of control might be harmful. Given the current climate surrounding section 230 and Big Tech's power, the public likely would not view a specific and narrow delegation as contemplated in this Note as very controversial in comparison to a sweeping repeal of section 230.

D. Creating A New Agency Is an Inefficient and Inferior Solution

Creating a new agency to regulate this area would likely be more trouble than it is worth, especially considering that there is already an agency that could be regulating this area. First, Congress would have to write an organic statute that creates the new agency and delegates specific powers to that agency. While this legislation would be more likely to pass with Democrats taking control of both the House and the Senate, it may still face challenges—it will likely be scrutinized more strictly because it is regulation of information that is adjacent to political advertising. Further, the Democrats in the Senate hold a razor-thin majority, as each party holds 50 seats, rendering Vice President Kamala Harris the tie-breaking vote if every representative votes down their party lines.[181] If even one Democrat or Vice President Harris chose to break ranks, the legislation to create a new agency would not pass.

Second, even if Congress were successfully able to create this new agency, it would face difficulties in getting started. The prevention of disinformation on social media during and approaching elections is an omnipresent and ongoing issue that requires a shifting approach, as Facebook has illustrated with its choice to ban all political advertising starting on November 4.[182] The new agency would be diving in headfirst and building itself from the ground up at the same time, and that level of multitasking would likely make the agency ineffective at the start. Further, even if the agency were created the day after the 2020 election, it likely would not be fully functional by the time 2022 mid-term elections rolled around.

Delegating this authority to an already-existing agency is superior. As discussed above, the FTC does not only regulate commercial advertising, but also participates in the regulation of information in certain expressly delegated instances.[183] Narrowly expanding the areas in which the FTC has been delegated jurisdiction to include regulation of procedural election

[180] Alan Rozenshtein, *Section 230 and the Supreme Court: Is Too Late Worse Than Never?* LAWFARE (Oct. 20, 2020), https://www.lawfareblog.com/section-230-and-supreme-court-is-too-late-worse-than-never [https://perma.cc/93AM-RDXY].

[181] Emma Hinchliffe, *Kamala Harris Could Make Even More History - as the Senate's Tiebreaker*, FORTUNE (Jan. 20, 2021), https://fortune.com/2021/01/20/kamala-harris-vp-senate-tiebreaker-biden/ [https://perma.cc/C24V-LGFV].

[182] *See What to Know About Facebook Advertising Around the Election*, *supra* note 93.

[183] *See supra* text accompanying notes 143-55.

information is a much more feasible solution than creating an entirely new agency exclusively for that purpose.

Additionally, the FTC has existed for over 100 years.[184] It has had time to develop and build up agency infrastructure and is thus equipped to take on additional responsibilities. Further, it has already begun to engage in some form of regulation involving information and the Internet, so it won't be venturing into entirely unexplored areas.[185] These elements of the FTC indicate that it is ready to take on the new challenge of regulating procedural election information with little additional burden.

E. Public Policy Calls for Regulations in this Area

The tumultuous 2020 election and the state of United States politics since then have illustrated that there is a public interest in regulation in this area. The promulgation of procedural election misinformation disenfranchises voters, creates mistrust in media generally, and emboldens those who create or share misinformation in any form.

First, procedural election misinformation disenfranchises voters. Those who have inaccurate information about registration or polling places may end up not voting because they think it's too much of a hassle, accidentally show up at the wrong polling place and are turned away, or do not realize they have not been registered to vote by the deadline and are turned away. These possibilities create barriers for citizens interested in voting and may lead to them giving up on having their vote counted in the election.

Second, procedural election misinformation creates distrust in media generally. Whenever someone views an advertisement containing misinformation and is able to identify it as misinformation, they may become distrustful of other advertising on that social media site or media in general. This distrust makes it difficult for users to trust actual reliable information, which in turn may also lead to voter disenfranchisement.

Finally, seeing misinformation being successfully promulgated may embolden those who create misinformation or who profit from it to continue to do so, thus furthering the problem.

F. How the FTC Should Proceed with Regulations

A legislative delegation of authority to the FTC regarding procedural election information is likely to withstand legal challenges.[186] As discussed above, the statute will need to be narrowly and specifically drawn such that the FTC's jurisdiction is restricted to procedural election information, including information about polling places, how to register to vote, and the ongoing status of election races. The statute will be more likely to withstand scrutiny if it specifically enumerates these three categories and uses limiting

[184] *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/G3ZT-TPM5].

[185] *See supra* text accompanying notes 143-55.

[186] *See supra* text accompanying notes 156-76.

language, rather than using ambiguous language that is open to significant FTC interpretation.

The statute will also need to specify the context of regulating advertisements paid for and featured on social media sites, rather than regulation of any user-posted content. Although it may seem obvious that federal agencies should not tread in the arena of regulating user-generated, unpaid content, this specification will also help to shield both the legislation and the agency from significant First Amendment challenges. This way, the legislation and the agency are less likely to face legitimate legal First Amendment scrutiny claiming government regulation of speech that should remain unregulated.

Assuming this delegation withstands legal challenges, the statute would likely follow the approach of other statutes delegating authority to the FTC to allow it to promulgate regulations as it sees fit. Typically, this would mean that the FTC is not required to engage in informal notice-and-comment rulemaking that other federal agencies such as the FCC perform.[187] However, perhaps a better approach would be either for the FTC to voluntarily conduct hearings, or the statute to mandate that the FTC conduct hearings. During these hearings, social media site representatives could explain their current approaches in regulating procedural election information. This way, the FTC could use their input in promulgating the regulations that all the social media sites would be following, thereby lessening the burden that these sites will face in making adjustments to the federal regulations.

If the statute were to take the latter approach in requiring hearings, the FTC would likely take the approach of informal notice-and-comment rulemaking. This would help to insulate the legislation and agency action from legal claims by the social media sites themselves—they could claim that they deserve a say in an area that substantially affects part of the way they operate, and therefore should be afforded due process.

Ideally, after either voluntary or legislatively mandated hearings, the FTC would choose to regulate this area of disinformation in an approach similar to the one Facebook has taken. These regulations should focus on three areas: removal of disinformation advertising, flagging misleading (but not expressly false) advertising, and temporal limitations.

First, the FTC should implement a zero-tolerance policy for expressly inaccurate procedural election information. This would mandate that social media sites scrutinize advertising relating to procedural aspects of elections and decline to display those that contain expressly inaccurate information. By mandating this review, procedural election disinformation is less likely to even enter the information stratosphere, causing less harm. Both Facebook and Twitter have already taken this approach, as Facebook had banned procedural election disinformation before its blanket ban on political advertising, and Twitter also has a blanket ban on political advertising.[188]

[187] *Rulemaking Process*, FCC, https://www.fcc.gov/about-fcc/rulemaking-process [https://perma.cc/7S6W-CJS8].

[188] *See* TWITTER, *supra* note 61; Byers, *supra* note 79.

Second, the FTC should mandate that advertising that is not expressly inaccurate, but is misleading, should be flagged as such. This way, users would get a visual notification that the source they are relying on may not be accurate, and that they should check other sources. The flagged content could also provide a link leading to an election center, such as Facebook has done, but this should be left to the discretion of social media sites as to what information they wish to include.

Finally, there should be temporal limitations. While this will be a prevalent issue as long as free elections exist in the United States, elections are not constantly going on. The FTC should limit its regulation in this area to registration deadlines and leading up to and immediately following elections. These are the times when accurate procedural election information is most imperative and disinformation is most dangerous.

While the above areas should be promulgated as regulations that social media sites must follow, the FTC should also release reports on further best practices, providing recommendations for other actions that social media sites could take. These best practices could include providing an election information center of the nature Facebook provided.

These solutions most closely follow the approach that Facebook has taken.[189] While Twitter's approach works as they are a private company, it is not a feasible model to follow as a federal agency. A global, blanket ban on paid political content would almost certainly go beyond the scope of the statute delegating authority and would further fail to withstand a First Amendment challenge.

IV. CONCLUSION

Regulation of paid procedural election information will help to prevent the spread of disinformation and begin the process of restoring the American's people's trust in fair and accurate elections. Citizens have the right to accurate information about the voting process, and the proposed solution will not significantly harm Big Tech companies like Facebook and Twitter, who already engage in both advertising and user content moderation.[190] The potential First Amendment harms—which may or may not be explored should the regulations or the delegation itself face legal challenges—are minimal when compared with the benefits of preventing false procedural election information from being spread, especially when this spread of false information has proven to be deadly.[191] Ultimately, this legislation and the subsequent FTC regulations will protect the American people and begin to restore some of the equilibrium and trust that has been lost over the 2020 election process.

[189] *See supra* text accompanying notes 81-104.

[190] *See supra* text accompanying notes 64-104.

[191] *See supra* text accompanying notes 156-76.

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

FCC v. Prometheus Radio Project

Micah Leval

141 S. CT. 1150 (2021)

In *FCC v. Prometheus Radio Project*, the Supreme Court reversed the judgement of the Third Circuit, holding that the FCC's decision to repeal two of its media ownership rules and modify a third ownership rule was not arbitrary and capricious under the Administrative Procedure Act (APA).[1] Prometheus Radio Project (Prometheus) argued that, due to the FCC's reliance on flawed data, the FCC incorrectly concluded that the proposed rule changes would not have a negative impact on women and minority media ownership.[2] However, the FCC acknowledged that it was not working with a complete set of data, and that when the FCC requested additional data from outside parties to help fill the gaps, no data was provided.[3] Additionally, although Prometheus argued that the FCC ignored two studies regarding the negative impact of past rule changes on female and minority ownership, the Court found that the FCC had considered these studies but it had a different interpretation of the studies than what Prometheus had argued.[4] In light of the totality of the FCC's reasoning, the Supreme Court held that the FCC's decision to modify its media ownership rules was not arbitrary and capricious under the APA.[5]

I. BACKGROUND

The Communications Act of 1934 directs the FCC to regulate broadcast media "as public convenience, interest, or necessity requires."[6] In doing so, the 1934 Act grants the FCC power to promulgate rules related to broadcast media ownership that "limit the number of radio stations, television stations, and newspapers that a single entity may own in a given market."[7] Traditionally, the goal of these FCC media ownership rules has been to "promote competition, localism, and viewpoint diversity," including diversity with respect to women and minorities.[8] Pursuant to the Telecommunications Act of 1996, the FCC must conduct a review of its ownership rules every four

[1] FCC v. Prometheus Radio Project, 141 S. Ct. 1150, 1154-55 (2021).
[2] *Id.* at 1159.
[3] *Id.*
[4] *Id.*
[5] *Id.* at 1155.
[6] *Id.* (citing 47 U.S.C. §303).
[7] *Id.*
[8] *Id.*

years and abrogate or modify any rules that are "no longer in the public interest."[9]

In 2017, the FCC issued an order concluding that three of its media ownership rules "no longer served the public interest," and, therefore, needed to be abrogated or modified.[10] Two of the three rules, the Newspaper/Broadcast Cross-Ownership Rule and Radio/Television Cross-Ownership Rule, were repealed in their entirety.[11] The Newspaper/Broadcast Cross-Ownership Rule prohibited an entity from owning both a daily newspaper and either a radio or television broadcast company in the same market.[12] The Radio/Television Cross-Ownership Rule limited the amount of radio and television stations an entity can own in any given market.[13] The third rule implicated by the 2017 Order—the Local Television Ownership Rule, which limits the number of local television stations an entity can own in a single market—was amended rather than repealed.[14]

In coming to these decisions, the FCC "considered the effects of the rules on competition, localism, viewpoint diversity, and minority and female ownership of broadcast media outlets."[15] The FCC reasoned that, given the ever-evolving methods through which people consume information, including the rise of popular online alternatives to print, broadcast, and radio,[16] "the three rules were no longer necessary to promote competition, localism, and viewpoint diversity, and . . . changing the rules was not likely to harm minority and female ownership."[17]

Prometheus Radio Project, a non-profit advocacy organization, filed suit arguing that the FCC's decision to modify the ownership rules was arbitrary and capricious under the APA.[18] Prometheus took issue with the FCC's conclusion that the rule modifications would have only a "minimal effect" on minority and female media ownership.[19] Agreeing with Prometheus, the Third Circuit vacated the FCC's 2017 Order modifying its media ownership rules.[20] On petition from the FCC, the Supreme Court granted certiorari.[21]

II. ANALYSIS

In *Motor Vehicle Manufacturers Ass'n v. State Farm*, the Supreme Court held that, to pass muster under arbitrary and capricious review, the

[9] *Id.* at 1155-56.

[10] *Id.* at 1154.

[11] *Id.* at 1157.

[12] *Id.* at 1155.

[13] *Id.*

[14] *Id.* at 1155, 1157.

[15] *Id.* at 1154.

[16] *See id.* at 1157.

[17] *Id.* at 1154.

[18] *Id.* at 1155.

[19] *See id.* at 1153, 1157 (quoting Prometheus Radio Project v. FCC, 939 F.3d 567, 584 (3d Cir. 2019), *rev'd*, 141 S. Ct. 1150 (2021)).

[20] *Id.* at 1155.

[21] *Id.* at 1157.

agency must examine the data presented to it, "reasonably consider[] the relevant issues, and reasonably explain[] the decision."[22] *State Farm* also made clear that arbitrary and capricious review is highly deferential to the agency, explaining that "the scope of review under the 'arbitrary and capricious' standard is narrow and a court is not to substitute its judgment for that of the agency."[23]

With respect to the potential impact that the rule modifications would have on women and minority ownership, the FCC noted that, despite inviting public comment on the matter, the only comments received were those suggesting that the rule modifications would have a *positive* effect on women and minority ownership—none that forecasted a negative effect.[24] Prometheus argued that the data relied upon by the FCC was "materially incomplete," thus rendering the FCC's decision arbitrary and capricious.[25] However, the Court reasoned that because no additional data was presented to the FCC upon request, the FCC acted reasonably in relying on the only data it had received.[26] As the Court noted, agencies are not required to supplement a sparse record with studies of their own.[27]

Additionally, Prometheus argued that two separate studies submitted to the FCC proved that past reforms to media ownership rules had harmed female and minority ownership, and the FCC acted arbitrarily and capriciously in ignoring this data.[28] However, the Court determined that the FCC did not actually ignore those two studies.[29] Rather, the FCC engaged with both studies and concluded that they actually suggested a "long-term *increase* in minority ownership after the Local Television Ownership and Local Radio Ownership Rules were relaxed."[30] In other words, Prometheus and the FCC simply interpreted the studies differently.[31] In offering its own reasonable interpretation of the studies, albeit a different interpretation from that of Prometheus, the Court found that the FCC's decision was not arbitrary and capricious.[32]

Accordingly, the Supreme Court reversed the judgment of the Third Circuit.[33]

[22] *Id.* at 1158 (citing Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983)).

[23] *State Farm*, 463 U.S. at 43.

[24] *Prometheus*, 141 S. Ct. at 1158.

[25] *Id.* at 1159.

[26] *Id.*

[27] *See id.* at 1160 (citing FCC v. Fox Television Stations, Inc., 556 U.S. 502, 518-20 (2009)).

[28] *See id.* at 1159.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *See id.* at 1160.

[33] *Id.* at 1161.

III. CONCURRENCE (J. THOMAS)

Justice Clarence Thomas wrote separately to note an alternative reason for reversal. Justice Thomas argued that by requiring the FCC to consider female and minority diversity in its consideration of media ownership rules, the Third Circuit imposed an impermissible procedural requirement onto the FCC.[34]

Justice Thomas noted that the Telecommunications Act of 1996 does not require the FCC to consider female and minority diversity with respect to media ownership; the 1996 Act only requires the FCC to determine whether its media ownership rules still further the public interest.[35] Therefore, given that "courts have no authority to impose 'judge-made procedure[s]' on agencies," the Third Circuit improperly required the FCC to take female and minority ownership into account—both in this case and in other challenges to the FCC's media ownership rules dating back to 2004.[36]

Prometheus argued that "because an agency cannot 'depart from a prior policy *sub silentio*,'" the fact that the FCC previously considered minority ownership required the FCC to either do so too in the present case, or alternatively, expressly depart from that prior policy.[37] Although Justice Thomas noted that the FCC has considered female and minority diversity in its past decisions, he noted that these considerations are not "policy goals in and of themselves, but . . . proxies for viewpoint diversity."[38] Therefore, Justice Thomas concluded that the Third Circuit erred in past cases by faulting the FCC for not considering female and minority diversity when modifying its ownership rules.[39]

IV. CONCLUSION

For the forgoing reasons, the Supreme Court reversed the judgement of the Third Circuit, holding that the FCC's actions were not arbitrary and capricious under the Administrative Procedure Act (APA).[40]

[34] *Id.*

[35] *Id.*

[36] *Id.* (quoting Perez v. Mortg. Bankers Ass'n, 575 U.S. 92, 102 (2015)).

[37] *Id.* (quoting *Fox Television Stations*, 556 U.S. at 515).

[38] *Id.* at 1162.

[39] *Id.* at 1163.

[40] *Id.* at 1154-55.

NetChoice, LLC v. Paxton

Thompson J. Hangen

2021 WL 5755120 (W.D. TEX. 2021)

Plaintiffs NetChoice, LLC (NetChoice) and Computer & Communications Industry Association (CCIA) challenge Texas House Bill 20 (HB 20) on multiple grounds.[1] NetChoice and CCIA brought a motion for a preliminary injunction,[2] and the State of Texas, represented by the Attorney General of Texas, Ken Paxton, brought a motion to dismiss for lack of standing.[3] NetChoice and CCIA also brought a motion to strike an expert report attached to the state's opposition.[4] Judge Robert L. Pitman of the United States District Court for the Western District of Texas granted the plaintiffs' motion for preliminary injunction, dismissed the plaintiffs' motion to strike an expert report as moot, and dismissed the State's motion to dismiss.[5]

I. BACKGROUND

Texas House Bill 20, signed into law on September 9, 2021, is designed to prevent social media users from "censorship" by social media platforms.[6] Specifically, section 7 of HB 20 makes it unlawful for social media platforms to censor users and their speech based on: "(1) the viewpoint of the user or another person; (2) the viewpoint represented in the user's expression; or (3) a user's geographic location in [Texas]."[7] Section 2 of HB 20 requires social media platforms to publish "acceptable use policies," establish an accessible complaints system, and produce a biannual "transparency report."[8] The bill applies to companies "(1) with more than fifty million active users in the United States in a calendar month, (2) that is open to the public, (3) allows users to create an account, and (4) enables users to communicate with each other for the primary purpose of posting information, comments, messages, or images."[9] HB 20 provides a right to private action under section 7 for users who have been improperly "censored," and also authorizes the Attorney General of Texas to bring an action "to enjoin a violation or potential

[1] NetChoice, LLC v. Paxton, No. 1:21-CV-840-RP, 2021 WL 5755120, at *2 (W.D. Tex. Dec. 1, 2021).
[2] *Id.*
[3] *Id.* at *3.
[4] *Id.*
[5] *Id.* at *15.
[6] *Id.* at *1.
[7] *Id.* (citing TEX. CIV. PRAC. & REM. CODE ANN. § 143A.002 (West 2021)).
[8] *Id.* at *2.
[9] *See Id.* at *1 (internal quotation marks omitted).

violation" of HB 20 or for failure to comply with the requirements of section 2.[10]

Plaintiffs Netchoice, LLC (NetChoice) and Computer & Communication Industry Association (CCIA) are trade associations who have members who operate social media platforms that would be affected by HB 20.[11] NetChoice and CCIA challenged HB 20, alleging that it violates the First Amendment, Commerce Clause, Full Faith and Credit Clause, and the Fourteenth Amendment's Due Process and Equal Protection clauses.[12] NetChoice and CCIA also alleged that HB 20 is preempted under the Supremacy Clause because of the Communications Decency Act, and that HB 20 should be found void for vagueness.[13] NetChoice and CCIA moved for preliminary injunction to enjoin state enforcement of sections 2 and 7 of HB 20 against NetChoice, CCIA, and their members.[14] Shortly thereafter, Texas filed a motion to dismiss for lack of standing.[15] NetChoice and CCIA also filed a motion to strike an expert report attached to the State's opposition to the motion for a preliminary injunction.[16]

II. ANALYSIS

The court denied the State's motion to dismiss, rejecting the argument that NetChoice and CCIA lacked either associational or organizational standing.[17] The court described that an association may assert the standing of their own members when three elements are met: "(1) its members would otherwise have standing to sue in their own right, (2) the interests at stake are germane to the organization's purpose, and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit."[18] The court addressed each element in turn. In holding that the members of plaintiff organizations otherwise have standing to sue, the court was satisfied that the plaintiffs had alleged sufficient threat of prosecution and economic harms to members operating social media platforms, either of which would support standing.[19] The second element was undisputed by the State, and was therefore not addressed by the court in detail.[20] The court found that it could address the threshold question of whether a social media platform is a common carrier without the individual participation of association members, which fulfilled the third element needed to determine that the

[10] *Id.* at *2.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.* at *3.

[16] *Id.*

[17] *Id.* at *3, *6, *15.

[18] *Id.* at *4 (quoting Tex. Ass'n of Mfrs. v. U.S. Consumer Prod. Safety Comm'n, 989 F.3d 368, 377 (5th Cir. 2021) (internal quotation marks omitted)).

[19] *Id.* at *4-5.

[20] *Id.* at *5.

plaintiffs have associational standing.[21] The court also addressed the issue of the plaintiffs' organizational standing on behalf of members.[22] The plaintiffs alleged in their complaint that they have already incurred costs to address compliance with and implications of HB 20, which was found to be sufficient for organizational standing.[23] Accordingly, the defendant's motion to dismiss was denied.[24]

The court granted the plaintiffs' motion for preliminary injunction, enjoining the Texas Attorney General from enforcing sections 2 and 7 of HB 20 until judgement in this case is entered.[25] Success on the motion for preliminary injunction rested on a determination that HB 20 "compels private social media platforms to disseminate third-party content and interferes with their editorial discretion over their platforms."[26] As a preliminary matter, the court addressed whether social media platforms have a First Amendment right to exercise editorial discretion.[27] In citing a number of cases, the court demonstrated that newspapers have the First Amendment right to moderate content, which extends to social media platforms moderating content disseminated on their platforms: "private companies that use editorial judgement to choose whether to publish content—and, if they do publish content, use editorial judgment to choose what they want to publish—cannot be compelled by the government to publish other content."[28] This editorial judgement is applicable to social media platforms because of the variety of content moderation that exists: screening, moderation, and curation of content, both by persons and algorithms employed by social media platforms.[29] The court found that this editorial discretion is explicitly considered in HB 20, which recognizes that social media platforms engage in curation of content, moderation of content and users, and search and ranking of content by algorithms or other procedures.[30]

The court continued to find that HB 20 violates the First Amendment right to exercise editorial discretion by prohibiting content moderation based on "viewpoint."[31] Not only would HB 20 restrict platforms in expressing agreement or disagreement with content, but the threat of lawsuits under section 7 would "chill[] the social media platforms' speech rights."[32] "Burdensome" public disclosures mandated by section 2 would furthermore chill protected speech by platforms and "force elements of civil society to speak when they would otherwise have refrained."[33] Finally, the court held

[21] *Id.* at *5.

[22] *Id.* at *6.

[23] *Id.*

[24] *Id.* at *6, *15.

[25] *Id.* at *15.

[26] *Id.* at *6 (internal quotation marks omitted).

[27] *Id.*

[28] *Id.* at *7.

[29] *Id.* at *7-8.

[30] *Id.* at *8.

[31] *Id.* at *9.

[32] *Id.* at *9-10.

[33] *Id.* at *11.

that HB 20 would discriminate based on content and speaker due to the limited exceptions found in section 7.[34] The record demonstrates that a legislative purpose in establishing a fifty million monthly user limit was to specifically target large social media companies viewed as "biased against conservative views," further supporting a conclusion that HB 20 would discriminate based on content.[35]

In addressing other reasons put forth by the plaintiffs to support a preliminary injunction, the court rejected arguments from the plaintiffs that HB 20 is unconstitutionally vague.[36] The court found that HB 20 fails on struct scrutiny and intermediate scrutiny, rejecting defendant's arguments that state interests in free and unobstructed use of public forums and providing individual citizens effective protection against discriminatory practices were sufficiently served by such a broad bill imposing serious consequences for privately owned platforms.[37]

The court dismissed the plaintiffs' motion to strike an expert report as moot, because it was not relied on by the court in reaching a decision on the motion for preliminary injunction or motion to dismiss.[38]

III. CONCLUSION

The District Court for the Western District of Texas denied the state's motion to dismiss and granted the plaintiffs' motion for preliminary injunction.[39] The court then dismissed as moot the plaintiffs' motion to strike without prejudice.[40] The decision has been appealed to the Fifth Circuit Court of Appeals as of December 7, 2021.[41]

[34] *Id.*

[35] *Id.*

[36] *Id.* at *12-13.

[37] *Id.* at *13-14.

[38] *Id.* at *3.

[39] *Id.* at *15.

[40] *Id.*

[41] *Id.*

AT&T Services, Inc., v. FCC

Courtland D. Ingraham

21 F.4TH 841 (D.C. CIR. 2021)

In *AT&T Services, Inc., v. FCC*, the D.C. Circuit denied the AT&T petition to review the FCC's 2020 Flexible Use Order (Order), which opened the 6 GHz band of spectrum to unlicensed users, and held that the petitioners did not overcome judicial deference to the FCC's conclusion that the Order would protect against a "significant risk of harmful interference."[1] The court dismissed all but one petition challenging the Order, finding that their petitions failed to bring into doubt the Order's thoroughness in preventing harmful interference,[2] and wholly mischaracterized the FCC's goals.[3] The court remanded the petition brought by the National Association of Broadcasters (NAB), and held that the FCC failed to reserve some of the 6GHz band exclusively for mobile licensees, as NAB had requested.[4]

I. BACKGROUND

Under the Communications Act of 1934, the FCC is mandated to encourage a more expansive and efficient use of spectrum.[5] The FCC has historically reserved the 6 GHz band "for licensed users that support a variety of critical services."[6] Many of these devices use spectrum to support critical functions ranging from public safety and transportation to energy, telecommunications, and broadcasting including 911 dispatch, railroad train movements, oil and gas pipelines, electric grid management, long distance telephone service, and connectivity to news vans and broadcast cameras.[7] The Order extended the 6 GHz band to unlicensed indoor low-power devices to meet a near sixfold increase in demand for broadband connectivity spurred by the rise in devices that use Wi-Fi and Bluetooth technology.[8] Further, in an effort to protect licensed users from potential interference, the Order required that routers must: (1) operate at power levels below 5 dbm/Mhz, (2) "use a 'contention-based' protocol," and (3) "remain indoors."[9] The Order also

[1] AT&T Servs., Inc., v. FCC, 21 F.4th 841, 843 (D.C. Cir. 2021); Unlicensed Use of the 6 GHz Band: Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz, *Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd 3852, para. 5 (2020) [hereinafter *Order*].

[2] *AT&T*, 21 F.4th at 843.

[3] *Id.* at 846.

[4] *Id.* at 843 (citing *Order*, *supra* note 1 at para. 7).

[5] *Id.* at 844 (citing 47 U.S.C. §303(g)) (outlining the powers and duties of the Commission).

[6] *AT&T*, 21 F.4th at 843.

[7] *Id.*

[8] *Id.* at 845; *see Order*, *supra* note 1, at para. 2.

[9] *AT&T*, 21 F.4th at 845.

discouraged the use of outdoor routers to minimize the likelihood of interference with licensees by prohibiting outdoor routers from being made weather-resistant or battery-equipped and by requiring that they have integrated antennas.[10]

II. ANALYSIS

In response to the FCC's Order, several private sector parties filed a joint petition arguing that the Order was arbitrary and capricious and claimed that the FCC understated the harmful interference that may result from giving unlicensed users access to the 6 GHz band.[11] Further, the petitioners claimed that in doing so, the FCC overstepped its authority under both the Communications Act of 1934 and the Administrative Procedure Act (APA).[12] The court consolidated six challenges to the Order into one decision, addressing both jointly- and individually-petitioned causes.[13]

The court rejected most of the petitions and held that they did not meet the threshold to show that the Order was arbitrary and capricious under *Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Insurance Co.*[14] The court emphasized that the FCC was owed "the greatest deference by a reviewing court" and must only exhibit "a modicum of reasoned analysis" in its policymaking for a regulation to be upheld.[15] The court further justified giving the FCC heightened deference because it acted reasonably in areas within its discretion and expertise.[16]

A. Joint Petitions

The court dismissed the joint petitions because they mischaracterized the FCC's goals in claiming that the Order understated the risk of interference that unlicensed users may cause on the 6 GHz band.[17] Further, the court disagreed with the petitioners' claim that the FCC had violated the APA by failing to explain their decision to "not require low-power devices to use an AFC system."[18] The court also accepted the FCC's determination that if harmful interference ever occurred, that the FCC's Enforcement Bureau would investigate, issue enforcement actions if necessary, and if the

[10] *Id.*; *Order*, *supra* note 1at para. 107.

[11] *AT&T*, 21 F.4th at 846.

[12] *Id.* at 843.

[13] *Id.* at 841.

[14] *Id.* at 845-46, 851, 852, 854 (citing Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)) (holding that in order for a challenger to demonstrate an agency regulation is arbitrary and capricious, they must show the "agency 'relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise'").

[15] *Id.* at 846 (citing Mobile Relay Assocs. v. FCC, 457 F.3d 1, 8 (D.C. Cir. 2006)).

[16] *Id.* at 851 (citing *EarthLink, Inc. v. FCC*, 462 F.3d 1, 12 (D.C. Cir. 2006)).

[17] *Id.* at 846.

[18] *Id.* at 847.

Enforcement Bureau were unequipped to handle an issue that victims may then petition the FCC for relief.[19]

1. CableLabs and AT&T Studies

The court held the FCC acted within its authority under the APA because it adequately addressed the risk of harmful interference by substantiating the Order with intensive data analysis.[20] The court generally found that the FCC responded adequately to technical challenges brought forward by the petitioners because the Order was heavily justified by a study conducted by Cable Television Laboratories (CableLabs) that evaluated several scenarios where harmful interference could occur.[21] The CableLabs study simulated how towers in New York City could hypothetically be impacted by introducing 1.2 billion unlicensed routers to the 6 GHz band of spectrum and it found no scenarios resulting in harmful interference.[22] The D.C. Circuit rejected the petitioners' assertion that the FCC should have publicly released the CableLabs datasets owing to the court's longtime practice of giving "considerable deference" to the FCC's expertise in "highly technical questions."[23] To dispute the accuracy of the CableLabs report, AT&T submitted an independently prepared study during the Notice and Comment period which simulated six worst-case scenarios that all showed the possibility of harmful interference from clutter loss.[24] The court found that the AT&T study did not raise sufficient doubt concerning the FCC's judgement and expertise that would merit the court denying the FCC deference.[25] The FCC adequately addressed AT&T's concerns because they incorporated the AT&T study into the Order by modifying the study's methodology to fit more realistic circumstances and moved forward with the Order when they found only one in six scenarios resulting in harmful interference.[26]

2. Harmful Interference Concerns

Petitioners also challenged the Order's requirements that routers must: (1) operate below 5 dbm/Mhz, (2) "use a 'contention-based' protocol," and (3) "remain indoors."[27] Regarding the power limit requirement, the court decided that the FCC's conclusion was well-founded.[28] While petitioners

[19] *Id.* at 851; *see Order*, *supra* note 1, at para. 149.

[20] *AT&T*, 21 F.4th at 846-48, 851.

[21] *Id.* at 847; *see Order*, *supra* note 1, at paras. 117-18.

[22] *AT&T*, 21 F.4th at 847.

[23] *Id.* at 848 (citing Am. Radio Relay League, Inc. v. FCC, 524 F.3d 227, 233 (D.C. Cir. 2008)).

[24] *Id.* at 849. The court defined "clutter loss" as "signal attenuation caused by terrain, trees, and other structures." *Id.*

[25] *Id.*

[26] *Id.*; *see Order*, *supra* note 1, at paras. 123-32.

[27] *AT&T*, 21 F.4th at 845.

[28] *Id.* at 850-51.

claimed that the Order's "contention-based" protocol offered licensees no protection against interference, the court rejected this assertion as a mischaracterization because the FCC never claimed that towers would be fully protected by such requirements.[29] The court also suggested that the FCC fully acknowledged petitioner's concerns about indoor devices causing interference when brought outside, and that by making outdoor router use impractical, the FCC promoted their goal to minimize the risk of harmful interference.[30] Lastly, the court dismissed petitioner's claim that the Order failed to offer a protocol for detecting and turning off harmfully interfering devices by again referring to the FCC's Enforcement Bureau as the proper venue for relief, should such a situation arise.[31]

B. Individual Petitions

The D.C. Circuit also heard and addressed individual petitions that challenged the Order brought by APCO International (APCO), electric utilities entities, and NAB.[32]

APCO's concerns, delivered on behalf of public safety operators, (1) claimed the Order did not acknowledge potential interference with 911 operators and AFC systems, (2) challenged the Order's regulation of unlicensed standard-power devices, and (3) characterized the FCC's enforcement authority as inadequate to address their concerns.[33] The court dismissed these challenges, noting that the FCC adequately considered APCO's concerns about harmful interference and that APCO failed to identify where the Order fell short in doing so.[34] The Order's requirement that unlicensed standard-power devices must consult a centralized AFC system before transmitting was found to be a sufficient demonstration of the FCC's predictive judgement to prevent harmful interference.[35] Lastly, the D.C. Circuit found APCO's concerns were inadequate for the court to question the FCC's Enforcement Bureau's competence to investigate interference issues, should they arise.[36]

Electric utility companies brought forward concerns that the FCC unreasonably dismissed Southern and Critical Infrastructure Industry studies submitted by Southern Company Services to contrast the CableLabs study.[37] Although the D.C. Circuit found that the FCC mischaracterized how the Southern and Critical Infrastructure Industry studies treated clutter loss, they ultimately held the FCC fulfilled its duty to respond to their comments in the Order.[38]

[29] *Id.* at 850.

[30] *Id.*; *see Order*, *supra* note 1, at paras. 105-08.

[31] *AT&T*, 21 F.4th at 851 (citing EarthLink, Inc. v. FCC, 462 F.3d 1, 12 (D.C. Cir. 2006)); *see Order*, *supra* note 1, at para. 149.

[32] *AT&T*, 21 F.4th at 845.

[33] *Id.* at 851-52.

[34] *Id.* (citing Mozilla Corp. v. FCC, 940 F.3d 1, 59 (D.C. Cir. 2019).

[35] *Id.* at 852.

[36] *Id.*

[37] *Id.* at 852-53.

[38] *Id.* at 853 (citing *Order*, *supra* note 1, at para. 138 n.364).

Lastly, the court addressed NAB's petition to vacate the Order because the FCC failed to address its concerns that the Order's restrictions on indoor low-power routers offered insufficient protection to mobile licensees.[39] The court ruled in favor of this petition only with regard to complaints that NAB expressed about interference in the 2.4 GHz band, and it remanded the issue to the FCC for a response.[40] The court further held this was a remand without vacatur, both relying on factors established in *Allied-Signal, Inc. v. Nuclear Regulatory Commission* and under the rationale that vacating the Order would be much more disruptive than leaving it in place.[41]

III. CONCLUSION

Ultimately, the D.C. Circuit upheld the Order and dismissed most of the petitioners' challenges because they failed to meet *State Farm*'s high standards for holding an agency regulation to be arbitrary and capricious.[42] Only NAB's comments about interference in the 2.4 GHz were remanded to the FCC for further consideration.[43]

[39] *Id.*

[40] *Id.* at 853-54.

[41] *Id.* (citing Allied-Signal, Inc. v. U.S. Nuclear Regul. Comm'n, 988 F.2d 146, 150-51 (D.C. Cir. 1993)) (holding that "the decision whether to vacate depends on the seriousness of the order's deficiencies and the disruptive consequences of an interim change that may itself be changed." *Allied-Signal*, 988 F.2d 150-51).

[42] *AT&T*, 21 F.4th at 854 (citing Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)).

[43] *Id.*

Colon v. Twitter, Inc.

Rebecca Roberts

14 F.4TH 1213 (11TH CIR. 2021)

In *Colon v. Twitter, Inc.*,[1] the United States Court of Appeals for the Eleventh Circuit affirmed the district court's decision to dismiss the plaintiffs' claims for aiding and abetting under the Anti-Terrorism Act (ATA), and affirmed its decision to dismiss the plaintiffs' claims for negligent infliction of emotional distress and wrongful death under Florida state law.[2] The court determined that the plaintiffs were unable to show that the Pulse massacre was an act of "international terrorism" associated with ISIS as defined by the Anti-Terrorism Act.[3] The court also held that the plaintiffs failed to demonstrate "proximate cause," as was required by both state law claims.[4]

I. BACKGROUND

In 2004, ISIS was designated as a foreign terrorist organization (FTO), in accordance with 8 U.S.C. § 1189.[5] Its stated goal is to use social media sites —like Twitter, Facebook, and Google (YouTube)—to "assist in carrying out [its] terrorist attacks throughout the world."[6] These social media postings often include violent videos, propaganda, messages, and solicitations for donations.[7]

Omar Mateen was a security guard from Fort Pierce, Florida.[8] On June 12, 2016, Mr. Mateen armed himself with a semi-automatic pistol and rifle, and opened fire at Pulse, an LGBT nightclub in Orlando, Florida—killing forty-nine people and injuring fifty-three others.[9] During the attack, he made a 9-1-1 call where he pledged allegiance to ISIS and declared himself an "Islamic soldier."[10] Mr. Mateen was ultimately killed by police during a standoff.[11] After the Pulse shooting, ISIS claimed responsibility for it, issuing a statement identifying Mr. Mateen as an "Islamic State fighter" and a "soldier of the Caliphate."[12] Following a thorough investigation, the FBI concluded

[1] *Colon v. Twitter, Inc.*, 14 F.4th 1213 (11th Cir. 2021).
[2] *Id.* at 1228.
[3] *Id.* at 1216.
[4] *Id.*
[5] *Id.* at 1218.
[6] *Id.*
[7] *Id.* at 1218-19.
[8] *Id.* at 1219.
[9] *Id.* at 1216.
[10] *Id.* at 1219.
[11] *Id.*
[12] *Id.*

that, prior to his attack at Pulse, Mr. Mateen had been self-radicalized through ISIS's postings on Twitter, Facebook, and YouTube.[13]

Plaintiffs are a blend of some of the injured parties and the estates of some of the victims from the Pulse nightclub shooting.[14] Their three claims against Facebook, Twitter, and Google (YouTube) include an allegation that the social media companies aided and abetted Mr. Mateen in violation of the ATA, as well as allegations of negligent infliction of emotional distress and wrongful death under Florida state law.[15] This lawsuit was filed after an unsuccessful lawsuit in Michigan by the estates of other victims from the same shooting and against the same companies.[16] However, the present Florida lawsuit was also unsuccessful, as the ATA claim and the Florida state-law claims were dismissed with prejudice by the district court under Rule 12(b)(6) of the Federal Rules of Civil Procedure.[17] The plaintiffs only appealed the dismissal of those three claims.[18]

II. ANALYSIS

The Eleventh Circuit performed a plenary review of the district court's dismissal order of: (1) the ATA aiding and abetting claim, (2) the Florida state law claim of negligent infliction of emotional distress, and (3) the Florida state law claim of wrongful death.[19]

Turning first to the ATA claim, the plaintiffs must first show that an act of "international terrorism" was "committed, planned, or authorized" by a foreign terrorist organization.[20] After showing that, a further analysis would be necessary to identify whether aiding and abetting liability under the ATA could be asserted.[21] However, the court found that the Pulse shooting was *not* an instance of "international terrorism," as defined by the ATA, nor was it "committed, planned, or authorized" by ISIS.[22] Therefore, a further analysis of aiding and abetting liability was not performed.[23]

The court acknowledged that the definition of international terrorism varies depending on context and situation.[24] However, because the ATA clearly defines the term "international terrorism," such an explicit definition should be followed closely.[25] The ATA definition of "international terrorism"

[13] *Id.* at 1219.
[14] *Id.* at 1216.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.* at 1217.
[19] *Id.*
[20] *Id.* at 1219.
[21] *Id.*
[22] *Id.* at 1222.
[23] *Id.* at 1218.
[24] *Id.* at 1217.
[25] *Id.* at 1218.

has three requirements that must be satisfied.[26] Focusing on the third element, requiring that the act in question either "occur primarily outside the territorial jurisdiction of the United States" or "transcend national boundaries," the court found that the Pulse shooting did neither, and, thus, did not meet the definitional requirements of "international terrorism."[27]

First, the shooting occurred in Orlando, Florida, which is within the territorial jurisdiction of the United States.[28] However, the plaintiffs alleged that the Pulse shooting was an activity that transcended national boundaries "in terms of the means by which [it was] accomplished, the persons [it] appear[ed] to be intended to intimidate or coerce, or the locale in which the[] perpetrators operate[d] or s[ought] asylum," as defined in the ATA.[29] As Mr. Mateen was radicalized via the Internet while living in Florida, and then committed mass murder while also in Florida, the means by which the Pulse shooting was accomplished did not transcend national boundaries.[30] While the plaintiffs argued that it was ISIS's social media use from outside of the United States that transcended national boundaries, it was Mr. Mateen's conduct, and not that of the Internet, which was the means by which he carried out his deadly acts.[31] Likewise, the court found that the "persons . . . intended to intimidate or coerce" did not transcend national boundaries, as an attack in the United States justifiably terrorized its citizens and residents.[32] And finally, as discussed previously, Mr. Mateen (the lone perpetrator) operated and acted within Florida and as such, did not "transcend national boundaries" since Florida is located within the national boundaries of the United States.[33]

While ISIS *did* take credit for the shooting after the fact, the court was not persuaded that this subsequent act transcended national boundaries "in terms of the means by which they [were] accomplished."[34] Nor did the court find that ISIS "committed, planned, or authorized" the shooting, as required by the ATA.[35] The court agreed with the Sixth Circuit's finding, during the previous Michigan lawsuit, that Mr. Mateen's self-radicalization did not indicate that ISIS "committed, planned, or authorized" the Pulse shooting, only that it approved of Mr. Mateen's actions after the shooting had already occurred.[36]

As for the two Florida state law claims, the court agreed with the district court's finding that the plaintiffs had not shown proximate cause to raise

[26] *Id.* at 1217. The first two elements of international terrorism require activities that "…(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State…" and "…(B) appear intended … (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping…" *Id.*

[27] *Id.* at 1220.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.* at 1220-21.

[32] *Id.* at 1221.

[33] *Id.* at 1220.

[34] *Id.*

[35] *Id.* at 1222.

[36] *Id.*

either one.[37] The plaintiffs had mistakenly relied on establishing proximate cause under the ATA, failing to address how Florida state law should address instances of third-party proximate cause, as found in this case.[38] The court performed a cursory analysis, identifying the lack of precedence and clarity in instances of third-party proximate cause, especially within Florida state law.[39] However, the court chose not to perform a more thorough search into relevant case law without input from the parties involved, and held that by failing to cite critical and applicable case law, the plaintiffs failed to show proximate cause in this case.[40]

III. CONCLUSION

For the foregoing reasons, the court affirmed the district court's decision to dismiss plaintiffs' claims of aiding and abetting in violation of the ATA and negligent infliction of emotional distress and wrongful death claims under Florida state law.[41]

[37] *Id.* at 1227.
[38] *Id.* at 1224.
[39] *Id.* at 1224-27.
[40] *Id.* at 1227.
[41] *Id.* at 1228.

Mahanoy Area School District v. B.L.

Julia Dacy

141 S. CT. 2038 (2021)

I. INTRODUCTION

Mahanoy Area School District v. B.L. deals with the First Amendment right to free speech as it applies to public school students.[1] This issue was most notably addressed in the Supreme Court case, *Tinker v. Des Moines* in which the Court found that schools have an interest in regulating student speech that "materially disrupts classwork."[2] In *Mahanoy*, the Supreme Court granted certiorari to decide whether the school district's decision to punish a student for comments posted on Snapchat outside of school hours and off of school grounds violated her First Amendment right to free speech.[3]

II. BACKGROUND

B.L.—then a minor—was a freshman student at Mahanoy Area High School.[4] At the end of the school year, B.L. tried out for the school's cheerleading squad and a private softball team.[5] She failed to make the varsity squad but was instead offered a spot on the junior varsity team.[6] Additionally, B.L. was not given the softball position for which she had hoped.[7] That weekend, B.L. expressed her frustration with the situation.[8] While visiting a local convenience store, B.L. posted two Snapchat images criticizing the coaches' decisions.[9] The first image showed B.L. and her friend raising their middle fingers, and the caption read "F**k school f**k softball f**k cheer f**k everything."[10] The second image's caption read, "[l]ove how me and [another student] get told we need a year of [junior varsity] before we make varsity but tha[t] doesn't matter to anyone else?"[11]

The images were posted to B.L.'s Snapchat story which was viewable by about 250 people for twenty-four hours.[12] During that time, at least one other student at the school took photos of B.L.'s posts and shared them with

[1] Mahanoy Area Sch. Dist. v. B.L. *ex rel.* Levy, 141 S. Ct. 2038 (2021).

[2] *Id.* at 2044 (citing Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 513 (1969)).

[3] Mahanoy, 141 S. Ct. at 2044.

[4] *See id.* at 2043.

[5] *See id.*

[6] *See id.*

[7] *See id.*

[8] *See id.*

[9] *See id.*

[10] *See id.*

[11] *See id.*

[12] *See id.*

the cheerleading squad.[13] One of the students showed the images to her mother who was a cheerleading coach at the school.[14] The situation garnered some attention and two coaches reported having to take several minutes during an algebra class they taught to address the issue.[15] Eventually, the coaches consulted school administrators who determined that "the posts used profanity in connection with a school-sponsored activity" which warranted a suspension from the cheerleading squad.[16]

At issue in this case is the applicability of the *Tinker* standard to off-campus speech.[17] In *Tinker*, the Supreme Court held that student speech that "materially disrupts" the school day is not fully protected by the constitutional right to free speech.[18] Here, B.L.'s speech occurred off-campus and on a weekend when school was not in session.[19]

B.L. challenged the suspension in Federal District Court, claiming that the school had no constitutional authority to punish her for off-campus speech.[20] The district court agreed and granted a temporary restraining order and a preliminary injunction ordering the school to allow B.L. to rejoin the cheerleading team.[21] The district court found that the Snapchats had not caused a substantial disruption to the school day that would have justified the district's actions under *Tinker*.[22] The Third Circuit affirmed this decision but concluded that the *Tinker* standard did not apply here to B.L.'s off-campus speech.[23]

III. Analysis

The Supreme Court granted certiorari to address *Tinker's* applicability to off-campus speech.[24] The Court rejected the Third Circuit's argument that schools have no regulatory interest in or authority to punish off-campus speech—acknowledging instead that schools have a regulatory interest in certain off-campus speech such as that which constitutes bullying or is expressed using school computers.[25] The Court identified three factors that should be considered when evaluating a school's regulation of student speech.[26] The first factor asks whether the school is standing *in loco parentis*, meaning in place of the student's parents.[27] The second factor considers whether regulating the student's off-campus speech would amount to regulation of "all the speech a student utters during a full twenty-four-hour

[13] *See id.*

[14] *See id.*

[15] *See id.*

[16] *See id.*

[17] *See id.* at 2044.

[18] *See id.* at 2040.

[19] *See id. at* 2043.

[20] *See id.* at 2043-44.

[21] *See id.* at 2044

[22] *See id.* at 2044.

[23] *See id.* at 2044.

[24] *See id.* at 2044.

[25] *See id.* at 2045.

[26] *See id.* at 2046.

[27] *See id.*

day," thus completely preventing a student from ever engaging in that type of speech.[28] This means that courts must be hesitant to permit regulations of off-campus speech—particularly when the speech is political or religious in nature—that could entirely restrict a student's ability to engage in that form of expression.[29] The third factor emphasizes that public schools are meant to be "nurseries of democracy" and have an interest in fostering even unpopular speech.[30]

In applying these factors to this case, the Court found that Mahanoy Area High School did not stand *in loco parentis* when B.L. posted the Snapchat messages from an off-campus location on a weekend.[31] As such, while the school claimed an interest in promoting good manners, this cannot overcome B.L.'s right to freedom of expression since the administration had no authority over her behavior at the time.[32] Additionally, the Supreme Court, agreeing with the district court, decided that the alleged class distraction lasted only a few minutes and did not cause a significant enough decline in school morale to constitute a substantial disruption.[33] This does not meet *Tinker's* high standard for regulation of student speech, which requires that such a prohibition be based on more than a fear of discomfort with a particular view.[34] Finally, the Court warned against dismissing the seriousness of this case simply because of the frivolous nature of the facts, noting that, "sometimes it is necessary to protect the superfluous in order to preserve the necessary."[35]

IV. CONCLUSION

In sum, the Supreme Court affirmed the judgment of the Third Circuit, yet it disagreed with the lower court's reasoning that the *Tinker* standard did not apply to this off-campus speech.[36] Instead, the Supreme Court considered several factors—including whether the school stood *in loco* parentis, if the school would be regulating all of a student's speech in a day, and whether the school has an interest in protecting unpopular opinions—to determine if *Tinker* applies in off-campus settings.[37] While the Court declined to state exact principles for regulating off-campus speech, it acknowledged that the leeway given to public schools to punish student speech is "diminished" in these situations.[38] Ultimately, the Court decided that Mahanoy Area School District violated B.L.'s First Amendment rights.[39]

[28] *Id.* at 2046.
[29] *See id.*
[30] *See id.*
[31] *See id.* at 2047.
[32] *See id.*
[33] *See id.* at 2047-48.
[34] *See id.* at 2048.
[35] *Id.*
[36] *See id.*
[37] *See id.* at 2046.
[38] *See id.*
[39] *Id.* at 2048.

V. CONCURRENCE (J. ALITO)

Justice Samuel Alito authored a concurring opinion agreeing with the majority's decision that the *Tinker* standard can apply to some instances of off-campus student speech.[40] However, he placed greater emphasis on the role of parents in making choices for their children and the distinction between private and public schools.[41] Alito noted that, while parents implicitly delegate *some* control over their child to a public school, they do not give the school complete authority to regulate what a student says at all times.[42]

VI. DISSENT (J. THOMAS)

Justice Clarence Thomas argued that courts have historically given schools leeway to discipline students for a variety of off-campus speech.[43] Thomas explained that the Court failed to address its reasons for departing from this rule, and, as a result, he dissented.[44]

[40] *Id.* (Alito J., concurring).

[41] *See id.* at 2050-51.

[42] *See id.* at 2052.

[43] *See id.* at 2059 (Thomas, J., dissenting).

[44] *See id.* at 2061.

ACA Connects v. Bonta

Alexa Pappas

24 F.4TH 1233 (9TH CIR. 2022)

In *ACA Connects v. Bonta*, the Ninth Circuit affirmed a California district court's refusal to enjoin the enforcement of the California Internet Consumer Protection and Net Neutrality Act of 2018 (SB-822), which created net neutrality rules for broadband Internet services provided to customers in California.[1] California passed SB-822 in the wake of the FCC's reclassification of broadband services from Title II's highly regulated "telecommunications services" to Title I's much less regulated "information services" (Reclassification Order).[2] Appellant service providers claimed that this reclassification preempted California from enacting SB-822.[3] The Ninth Circuit found that the service providers were unlikely to prevail on their argument that the FCC's reclassification preempts states from enacting their own net neutrality protections since the FCC no longer has the authority to regulate in that field.[4]

I. BACKGROUND

In 2018, the FCC ordered a decrease in federal regulation of broadband services by changing the classification of "broadband [I]nternet access services" from "telecommunications services" in Title II of the Communications Act, to "information services" in Title I.[5] Under Title II, broadband services were subject to a "multitude of statutory restrictions and requirements."[6] However, after the decision to reclassify under Title I, the FCC may only "impose regulations ancillary or necessary to the effective performance of the FCC's specific statutory responsibilities."[7] Thus, this reclassification abandoned extensive federal regulations that safeguarded equal access to the Internet, in favor of a "light-touch information service framework" in order to encourage innovation and investment.[8]

Within the FCC's Reclassification Order was a statement of preemption, which asserted federal preemption over any state or local laws "inconsistent with the federal deregulatory approach" (Preemption

[1] ACA Connects v. Bonta, 24 F.4th 1233, 1248 (9th Cir. 2022); 2018 Cal. Stat. ch. 976.

[2] *Bonta*, 24 F.4th at 1236; *see* Restoring Internet Freedom, *Declaratory Ruling, Report and Order, and Order*, 33 FCC Rcd 311 (2018) [hereinafter *Reclassification Order*].

[3] *Bonta*, 24 F.4th at 1237.

[4] *Id.* at 1248.

[5] *Id.* at 1236; *Reclassification Order*, *supra* note 2, at para. 2.

[6] *Bonta*, 24 F.4th at 1238 (citing Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 975-76 (2005)).

[7] *Id.*

[8] *See id.* at 1236; *Reclassification Order*, *supra* note 2, at para. 2.

Directive).[9] Through this Preemption Directive, the FCC sought to ensure that costs associated with state and local compliance requirements would not keep broadband services from innovating and investing as intended with the FCC's "free market" approach.[10]

Considering this federal policy change and California's interest in preserving net neutrality for its citizens, California joined a group of plaintiffs challenging both the Reclassification Order and Preemptive Directive in *Mozilla Corp. v. FCC*, and, shortly thereafter, passed SB-822, which provided net neutrality regulations on broadband services for California customers.[11] The instant case arose when, while the *Mozilla* decision was pending, a group of industry trade associations representing communications service providers (service providers) petitioned for a preliminary injunction in the District Court for the Eastern District of California in order to prevent SB-822's enforcement.[12] With the consent of the parties, this action was stayed in anticipation of the *Mozilla* decision.[13]

In 2019, the D.C. Circuit in *Mozilla* ruled to uphold the Reclassification Order but vacate its Preemptive Directive.[14] In striking down the Preemptive Directive, *Mozilla* relied on the basic premise that a federal agency must have Congressional regulatory authority to be able to permissibly preempt state and local regulations.[15] Thus, the *Mozilla* court held that because the FCC terminated its ability to enact net neutrality regulations on broadband services through the reclassification, it simultaneously terminated its ability to preempt such state laws.[16]

After hearing both parties' takes on *Mozilla*'s effect on the instant case, the district court, in a ruling from the bench, denied the service providers' request for a preliminary injunction using the *Mozilla* rationale.[17] *Bonta* was the service providers' appeal to the Ninth Circuit.[18] Throughout the *Bonta* opinion, the Ninth Circuit stressed that *Mozilla*'s preemption rationale formed the basis of its decisions, especially since both parties agreed to stay the case until the *Mozilla* decision, and neither party challenged the validity of *Mozilla*'s holding.[19]

II. ANALYSIS

Appellant service providers proffered three arguments in defense of preemption.[20] First, they claimed that SB-822 is preempted because it conflicts with the purpose underlying the Reclassification Order.[21] Next, they

[9] *Bonta*, 24 F.4th at 1239 (quoting *Reclassification Order*, *supra* note 2 at para. 194).

[10] *Id.* at 1239.

[11] *Id.* at 1240.

[12] *Id.*

[13] *Id.*

[14] *Id.* at 1239 (citing Mozilla Corp. v. FCC, 940 F.3d 1, 74 (D.C. Cir. 2019)).

[15] *Id.* (citing *Mozilla*, 940 F.3d at 74-75).

[16] *Id.* (citing *Mozilla*, 940 F.3d at 74-76).

[17] *Id.* at 1240.

[18] *Id.*

[19] *Id.* at 1241; *see also id.* at 1236, 1237, 1239-42, 1244-46.

[20] *See Bonta*, 24 F.4th at 1237.

[21] *Id.*

argued that SB-822 conflicts with the purpose underlying the Communications Act itself: specifically, section 153(51) and section 332(c)(2).[22] Appellants grounded these first two arguments in conflict preemption.[23] Third, they claimed that SB-822 impermissibly touches on the FCC-occupied field of interstate communications services.[24] This final argument was based in the theory of field preemption.[25]

A. Conflict Preemption

1. Reclassification Order's Purpose

First, the service providers claimed that SB-822 is preempted because it conflicts with the purpose underlying the Reclassification Order.[26] This argument implied that the elimination of federal net neutrality regulation is what preempts state net neutrality regulation; that is, "the state regulation conflicts with the absence of federal regulation."[27] The Ninth Circuit found this argument to be flawed, however, because "an absence of federal regulation may preempt state law only if the federal agency has the statutory authority to regulate in the first place."[28]

The service providers urged the Ninth Circuit to rely on *Ray v. Atlantic Richfield Co.*, in which the Secretary of Transportation had broad Congressional authority to regulate the size and speed of vessels in Puget Sound.[29] When the Secretary allowed large tankers, the Supreme Court found that decision to have preemptive power since the Secretary had the authority to ban large tankers, but, simply chose not to.[30] The Ninth Circuit distinguished *Ray* from the present case, because in the present case, the FCC does not possess the regulatory authority held by the Secretary in *Ray* since the FCC terminated its regulatory authority over broadband services by issuing the Reclassification Order.[31] The service providers urged that the reclassification was merely "an exercise of discretion under the statute as to the appropriate classification of communications services," and not a termination of regulatory authority.[32] However, the Ninth Circuit pointed to language in the Reclassification Order that suggested the FCC intended for the reclassification to strip it of its regulatory authority: "[A]fter reclassification[, there is] no 'source[] of statutory authority that individually or in the aggregate' supports net neutrality conduct rules."[33]

[22] *Id.* (citing 47 U.S.C. §§ 153(51), 332(c)(2)).

[23] *Id.*

[24] *Id.* at 1246-47.

[25] *Id.* at 1237.

[26] *Id.*

[27] *Id.* at 1241.

[28] *Id.* (citing Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986); citing Ray v. Atl. Richfield Co., 435 U.S. 151, 178 (1978)).

[29] *Id.* (citing *Ray*, 435 U.S. at 174).

[30] *Id.* (citing *Ray*, 435 U.S. at 178).

[31] *Id.*

[32] *Id.* at 1242

[33] *Id.* (quoting *Reclassification Order*, *supra* note 2, at para. 267).

The service providers additionally claimed that because *Mozilla* upheld the FCC's policy judgment underpinning its reclassification decision, the FCC's policy in favor of less regulation was sufficient for conflict preemption.[34] However, the Supreme Court in *Louisiana Pub. Serv. Comm'n v. F.C.C.* expressly rejected this policy form of conflict preemption theory if the agency already has no regulatory authority; thus, the Ninth Circuit rejected this argument here.[35] The court also rejected service providers' "novel" reliance on *Chevron U.S.A., Inc. v. N.R.D.C.* to argue that because Congress delegates the power to interpret statutory ambiguities to agencies, the FCC's deregulation policy preference preempts the states.[36] Here, the court adopted *Mozilla*'s sentiment: "Nothing in *Chevron* goes that far."[37]

Thus, applying the *Louisiana* principle that "[w]ithout the power to act, a federal agency can not preempt," the Ninth Circuit found that because the FCC forfeited its power to impose net neutrality regulations on broadband services, the FCC could not preempt SB-822.[38]

2. Communications Act's Purpose

The service providers' second argument in defense of preemption was that SB-822 conflicts with the purpose underlying the Communications Act itself; specifically, section 153(51) and section 332(c)(2).[39] The service providers claimed that while these provisions clearly limit the FCC's regulatory authority, they also limit the states' authority to impose regulations on information services and private mobile services that could be imposed only on common carriers.[40] The Ninth Circuit dismissed this claim for three reasons.[41] First, because each provision makes clear that the extent to which they are relevant pertains only to "this chapter," they define and limit only the FCC's regulatory authority without touching the authority of the states.[42] Second, because of the other numerous express preemption provisions throughout the Communications Act, the court reasoned that Congress knows how to preempt state authority when it wants to and it did not implicitly do so in sections 153(51) or 332(c)(2).[43] Finally, the Ninth Circuit pointed to the Telecommunications Act's Savings Provision which makes clear that unless

[34] *Id.*

[35] *Id.* (citing Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374-75 (1986)).

[36] *Id.* at 1243 (citing Chevron U.S.A., Inc. v. Nat. Res. Def. Council, 467 U.S. 837, 842-44 (1984)).

[37] *Id.* (quoting Mozilla Corp. v. FCC, 940 F.3d 1, 84 (D.C. Cir. 2019)).

[38] *Id.* at 1242; *see also id.* at 1244 (discussing how *Mozilla*'s rationale is consistent with *Ray*, *Louisiana*, and the court's instant reasoning).

[39] *Id.* at 1245 (citing 47 U.S.C. §§ 153(51), 332(c)(2)). Section 153(51) defines "telecommunications carrier" and states that they "shall be treated as a common carrier *under this chapter* only to the extent that it is engaged in providing telecommunications services." *Id.* (quoting 47 U.S.C. § 153(51) (emphasis in original)). Section 332 states that "[a] person engaged in the provision of a service that is a private mobile service shall not, insofar as that person is so engaged, be treated as a common carrier for any purpose *under this chapter*." *Id.* (quoting 47 U.S.C. § 332(c)(2) (emphasis in original)).

[40] *Id.*

[41] *Id.* at 1237.

[42] *Id.* at 1245.

[43] *Id.* at 1246.

"expressly" stated, the Act does not "modify, impair, or supersede Federal, State, or local law."[44] Therefore, because neither section 153(51) nor section 332(c)(2) expressly say as much, the court found them to have no effect on the states' regulatory power.[45]

B. Field Preemption

The service providers' third argument in defense of preemption was that SB-822 impermissibly touches on the FCC's occupied field of interstate communications services.[46] Here, the court noted that the *Louisiana* Court found it impossible to exclude the states from impeding on the FCC's interstate regulatory field because of "the realities of technology and economics."[47] *Louisiana* held that rather than neatly dividing interstate and intrastate regulatory power between the FCC and the states, respectively, the Communications Act establishes "dual state and federal regulatory authority" for interstate communications services.[48] To hold otherwise would "misrepresent[] the statutory scheme."[49]

To further its finding that the Communications Act left room for state regulation of intrastate communications, the Ninth Circuit pointed to the fact that Maine, Nevada, and Minnesota require broadband providers to obtain consumers' permission before sharing their data.[50] Even within the Reclassification Order itself, the FCC recognized that in the field of interstate broadband services, the states have a role in policing fraud, taxation, and general commercial dealings, as well as enforcing fair business practices.[51] In addition, if Congress had intended for the Communications Act to preempt all state regulation of interstate communications, Congress would not have added an express preemption provision in section 253.[52] Thus, the Ninth Circuit agreed with the district court that the Communications Act likely does not preempt SB-822.[53]

C. Concurrence

Judge Wallace wrote a separate concurrence emphasizing the "little guidance" the Ninth Circuit's opinion provides since it is merely a review of

[44] *Id.* (quoting Telecommunications Act of 1996, Pub. L. No. 104-104, § 601(c)(1), 101 Stat. 56, 143 (1996), *reprinted in* 47 U.S.C. § 152 note).

[45] *Id.*

[46] *Id.*

[47] *Id.* at 1247 (quoting Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 360 (1986)).

[48] *Id.* (citing *Louisiana*, 476 U.S. at 360).

[49] *Id.* at 1248 (quoting *Louisiana*, 476 U.S. at 373-74).

[50] *Id.* (citing Me. Rev. Stat. Ann. § 9301 (2019); Minn. Stat. § 325M.01 (2021) et seq.; Nev. Rev. Stat. § 205.498 (2013)).

[51] *Id.* at 32-33 (citing *Reclassification Order*, *supra* note 2, at para. 196).

[52] *Id.* at 1248 (quoting 47 U.S.C. § 253(a) ("No State or local statute or regulation . . . may prohibit . . . the ability of any entity to provide any interstate or intrastate telecommunications service.") § 253(a).).

[53] *Bonta*, 24 F.4th at 1248.

an order denying a preliminary injunction, not an adjudication on the merits.[54] Judge Wallace cautioned the parties not to "read too much into" the court's holding, as it merely found that the FCC is not *likely* to prevail on the merits and came to such a finding without the "fully developed factual record" that a full trial would elicit.[55]

III. Conclusion

The Ninth Circuit affirmed the District Court for the District of Eastern California's order denying a preliminary injunction that would bar enforcement of SB-822.[56]

[54] *Id.* at 1248-49 (Wallace, J., concurring) (quoting Sports Form, Inc. v. United Press Int'l, Inc., 686 F.2d 750, 753 (9th Cir. 1982)).

[55] *Id.* (Wallace, J., concurring) (quoting Gregorio T. v. Wilson, 59 F.3d 1002, 1005 (9th Cir. 1995) and *Sports Form*, 686 F.2d at 753).

[56] *Id.* at 1248.