EDITOR'S NOTE

Welcome to the first issue of Volume 70 of the *Federal Communications Law Journal* ("*Journal*"), the official journal of the Federal Communications Bar Association. I am thankful to our GW Law team that has invested many valuable hours into piecing together a strong publication for this new volume. From cybersecurity, privacy, tax law, cloud computing, to the First Amendment, this issue covers a wide array of relevant topics in the field of telecommunications law.

We are honored to feature two practitioner articles in this issue. The first article is written by Jennifer Urban, an Associate at K&L Gates LLP. In her article, Ms. Urban examines the cybersecurity and privacy issues that arise from drone activities. She makes the interesting and important argument that regulations on Unmanned Aerial Vehicles should address cybersecurity and privacy issues, in order for these regulations to keep abreast of new technology developments within the aviation industry.

The second article is penned by Philip M. Napoli, a professor at Duke University. In his article, Professor Napoli argues that the technological changes undermine the extent to which counterspeech, a concept of which means more speech is an effective remedy against the dissemination and consumption of false speech, can effectively operate as a fundamental assumption of the First Amendment.

Furthermore, the *Journal* is proud to publish three thought-provoking student Notes in this issue. In the first Note, Rosie Brinckerhoff addresses the phenomenon of Facebook's facial recognition technology outpacing state and federal laws and regulations. Ms. Brinckerhoff proposes that California courts are in the best position to defend consumer privacy rights, as they can enforce legal principles under state contract law, constitutional law, and tort law to strike down Facebook's privacy-invasive terms. In the second Note, Katherine Grabar examines the need for an amended Stored Communications Act to address cloud computing technology. Ms. Grabar proposes that Congress needs to enact more jurisdictional provisions to enhance law enforcement's ability to search for electronically stored data with a warrant based on probable cause. Last but not least, Michael Wallace explores the question of whether Internet streaming service providers are required to pay taxes imposed by the state and local governments. Mr. Wallace suggests that the Internet Tax Freedom Act, as well as the Commerce and the Due Process clauses of the Constitution, can prohibit the collection of such taxes.

We hope you enjoy this issue as much as we have enjoyed putting it together. We welcome your feedback or questions to fclj@law.gwu.edu. Please direct article submissions to fcljarticles@law.gwu.edu. This issue and our archive will be available at www.fclj.org.

Jane Lee
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

GW | LAW

FCBA
FEDERAL COMMUNICATIONS BAR ASSOCIATION

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

Federal Communications Law Journal

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

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,500 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at http://www.fclj.org.

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

Federal Communications Bar Association

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

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

The George Washington University Law School

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

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

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

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

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

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

Production: The citations in the *Journal* conform to the *Bluebook: A Uniform System of Citation* (20th ed., 2015), copyright by the *Columbia*, *Harvard*, and *University of Pennsylvania Law Reviews* and the *Yale Law Journal*. Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Joe Christensen, Inc.

Citation: Please cite this issue as 70 FED. COMM. L.J. ___ (2018).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW | LAW

VOLUME 70 ISSUE 1

APRIL 2018

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLES

Drones are increasingly being used in various sectors of the U.S. economy. Although current drone-specific regulations exist, there is a gap at the federal level for drone-specific regulations that address cybersecurity and privacy issues. Through international collaboration of actors from both the public and private sectors, effective cybersecurity and privacy regulations and Best Practices will hopefully emerge.

This paper begins with background information on drone technology and current drone regulations. Next, there is a discussion on cybersecurity and privacy issues arising from drone operations, along with the current laws that touch on these two areas. Third, an analysis of other countries solutions to cybersecurity and privacy issues portrays new answers that could potentially be implemented in the U.S. regulatory scheme. Finally, the paper concludes with suggestions on the best ways to address drone-specific cybersecurity and privacy issues.

Although the country is deeply divided ideologically, and this divide nominally may seem to halt opportunity for policy advances, this need not necessarily be the case. Notwithstanding our *ideological* differences, a number of *practical* opportunities for policymakers to improve economic welfare have emerged and for which there is considerable agreement, if not complete political consensus, that allow policy progress. These opportunities create the potential for practicality to forge agreement even in the face of more widespread ideological discord across our society.

This basic thesis is no more evident than in the set of infrastructure industries that policymakers across the political spectrum have identified as crucial for

U.S. competitiveness in the 21st century. As a case in point, I focus on broadband technologies (both wired and wireless), which policymakers of all political stripes have identified as crucial for economic growth. In this *Economic Policy Vignette*, I first identify the practical, as opposed to ideological, case for regulatory reform in the broadband sector. I then identify a number of specific measures that present themselves at this moment which create opportunities for meaningful and beneficial regulatory reform.

NOTES

Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray Into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever

Facebook undeniably has extraordinary facial recognition capabilities, so much so that its technology outranks the federal government's facial recognition database in both size and accuracy. Facebook maintains its enormous and eerily precise database by routinely updating and cultivating photos posted nearly every ten seconds by the company's 1.86 billion users. In other words, this feat is accomplished with the help of users like you.

With no comprehensive federal data privacy protection law in place to regulate private industry's use and collection of facial recognition data, Facebook's 1.86 billion users do not suspect the significant privacy implications threatened by the company's vague yet deceptively overbearing Terms of Service and Data Policy. Taken together, these policies bestow upon the social media giant free rein over its users' biometric data and information collected through its use of facial recognition technology.

Facebook simply cannot be trusted to self-regulate, especially when its commercial gain comes at the expense of the privacy of incognizant consumers. "If you don't like it, don't use it" is no longer a sustainable argument. Facebook's brazen and unregulated ability to exploit the biometric identifiers of its billions of users is strictly dependent on both users and courts allowing the company to do so. Yet with only three states espousing applicable biometric collection laws, and a host of other states having nothing to show but failed attempts at regulating facial recognition, legislative efforts simply are not keeping pace with this rapidly evolving technology.

This note seeks to draw attention to the very real problem of Facebook's facial recognition technology capabilities and its subsequent biometric data collection practices outpacing state and federal laws and regulations. This note will assess Facebook's capabilities and practices with respect to facial recognition technology and analyze the related privacy implications for consumers. Through an examination of the company's Terms of Service and Data Policy, this note will demonstrate why California courts should deem Facebook's user agreements unconscionable in order to safeguard consumer privacy rights. In doing so, this note will conclude by offering three plausible legal avenues for the California judiciary to consider to strike down the imperious and heavily invasive terms that Facebook imposes on its users.

What Is the Eye in the Sky Actually Looking at and Who is Controlling It? An International Comparative Analysis on How to Fill the Cybersecurity and Privacy Gaps to Strengthen Existing U.S. Drone Laws

Jennifer Urban *

TABLE OF CONTENTS

* Jennifer Urban is an Associate in the Charleston, South Carolina office of K&L Gates. Ms. Urban would like to thank Jacqueline Serrao for her helpful insights and Ann Urban for her endless support.

> Recent years have proved such a splendid success for aeronautics that it really seems justifiable for law to begin to take its share in the aerial labour.
>
> - Johanna Francina Lycklama À Nijeholt.[1]

I. INTRODUCTION

Drones are no longer seen as toys only techies get as Christmas gifts;[2] nor are they seen as only being used in new military operations; drones are becoming an integral part of today's global society. UAVs are being used for many different purposes ranging from the National Aeronautics and Space Administration's ("NASA's") use of a drone to collect data and monitor Hurricane Matthew,[3] to construction companies use of drones to map out and supervise large construction projects in order to cut their labor time from months down to minutes.[4]

While UAVs are making many things easier, the benefits come with unique challenges. For example, over the last two years, Dubai International Airport ("DXB") had to shut down three times due to unauthorized drone activity.[5] Each time DXB shut down, it caused a loss of approximately $1,007,310 USD per minute,[6] meaning the shut down on September 28, 2016, for twenty-seven minutes cost Dubai's economy $27,197,370 USD.[7] These shut downs prompted the United Arab Emirates General Civil Aviation Authority ("GCAA") to make DXB a no-fly zone, illustrating the immediate need for drone regulations globally. After these shut downs occurred, Emirates airline asked the GCAA and Dubai Civil Aviation Authority ("Dubai CAA") to enact stricter regulations regarding drone operations around DXB in order to improve the safety of manned aircraft flights

---

1. *See* DONNA A. DUOLO, UNMANED AIRCRAFT IN THE NATIONAL AIRSPACE 3 (Donna A. Dulo, ed., 2015) (citing JOHANNA FRANCINA LYCKLAMA À NIJEHOLT, AIR SOVEREIGNTY 4 (1910)).

2. Many different terms are used to described drones, such as "unmanned aerial vehicles" (UAV), "unmanned aircraft systems" (UAS), and "remotely piloted aircraft" (RPA). These terms will be used interchangeably throughout this paper and each will be discussed in more depth.

3. *See* Alyssa Newcomb, *NASA Deployed This Whale-Shaped Drone to Monitor the Hurricane*, NBC NEWS (Oct. 7, 2016, 1:50 PM), http://www.nbcnews.com/tech/tech-news/nasa-deployed-whale-shaped-drone-monitor-hurricane-n661931 [https://perma.cc/QS3B-XR88].

4. *See* Julian Mitchell, *This Startup Uses Self-Flying Drones to Map and Manage Construction Sites*, FORBES (Sept. 27, 2016, 6:33 PM), https://perma.cc/BB59-F5SRhttp://www.forbes.com/sites/julianmitchell/2016/09/27/this-startup-uses-drones-to-map-and-manage-massive-construction-projects/#7480a81f4334.

5. *See* Sarah Townsend, *Drone Prompts Shutdown at Dubai International Airport*, ARABIAN BUS. PUB. LIMITED (Sept. 28, 2016, 10:17 AM), http://www.arabianbusiness.com/drone-prompts-shutdown-at-dubai-international-airport-647000.html#.V_lrd9x1ZR0 [https://perma.cc/JHD6-8ETG].

6. Approximately AED 3.7 million.

7. *See* Townsend, *supra* note 5.

departing from and arriving at DXB.[8] Due to the difficult nature of identifying the drone operator, it has proven to be challenging to enforce UAS no-fly zones.[9] In order to better enforce the UAS no-fly zone around DXB, the Dubai CAA has begun experimenting with a "drone-hunting" drone that can identify unlawful drone operations within the zone.[10] According to UAS attorneys Jennifer E. Trock and Chris Leuchten, "[t]he drone-hunter aerially patrols the airport perimeter, using a thermal and infrared imaging to detect unauthorized drones, tracks their frequencies, follows the UAS back to its owner, and sends a signal to the Dubai police."[11] The "drone-hunting" drone is one solution posed thus far to help solve unauthorized drone operations and could be helpful in protecting the privacy of ordinary citizens.[12]

Drones violating air space is not the only problem this new technology creates. Both cybersecurity and privacy issues arise as a result of drone activities. A research team at the University of Texas at Austin employed "spoofing"[13] to hack a drone belonging to the university.[14] The spoofing was done through a mechanism where the hackers were able to get the drone to mistake their signals for the ones sent by the owner's GPS satellites.[15] This hack was done for research on drone vulnerability, which confirmed the fear that it is not very difficult for a drone to be hacked and the realization that many cybersecurity implications that could come from this.

The privacy issue related to drones arose in a 2015 lawsuit where David Boggs, a resident of Kentucky, had his drone shot down by his neighbor William Merideth.[16] Merideth argued that the drone operations caused a trespass on his right to privacy.[17] On the opposing side, Boggs argued that, according to title 49, section 40103 of the U.S. Code, "the United States Government has exclusive sovereignty of airspace of the United States," and therefore, Merideth did not own the airspace, so no trespass could have

8. *See* Jennifer E. Trock & Chris Leuchten, *Dubai Airport's New Guardian: a Drone-Hunting Drone*, PILLSBURY: UAS L. BLOG (Dec. 22, 2016), http://www.uaslawblog.com/2016/12/22/dubai-airports-new-guardian-drone-hunting-drone/ [https://perma.cc/SP9T-Z46H].

9. *Id*.

10. *Id*.

11. *Id*.

12. *Id*.

13. Spoofing is defined as "sending a network packet that appears to come from a source other than its actual source. [It] involves – 1) the ability to receive a message by masquerading as the legitimate receiving destination, or 2) masquerading as the sending machine and sending a message to a destination." RICHARD KISSEL, NAT'L INST. OF STANDARDS & TECH., GLOSSARY OF KEY INFORMATION SECURITY TERMS 188 (2013), http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [https://perma.cc/9WK2-JTU6].

14. See *Researchers Use Spoofing to 'Hack' Into a Flying Drone*, BBC NEWS (June 29, 2012), http://www.bbc.com/news/technology-18643134 [https://perma.cc/P368-T4PJ].

15. *Id*.

16. *See* Cyrus Farivar, *After Neighbor Shot Down His Drone, Kentucky Man Files Federal Lawsuit*, ARS TECHNICA (Jan. 6, 2016, 4:00 AM), http://arstechnica.com/tech-policy/2016/01/man-whose-drone-was-shot-down-sues-shotgun-wielding-neighbor-for-1500/ [https://perma.cc/JB7E-F6YS].

17. *Id*.

occurred.[18] There is a lack of precedent on this issue. The most recent case on point is *United States v. Causby* in 1946, where the United States Supreme Court held that a landowner's property rights extended up to 83 feet above his land into the air space.[19] Although this case is relatively on point, it is outdated. It is unlikely the justices in 1946 could have imagined the holding's implications on drones decades later.

Another theory that has been argued is the common law rule of *Cujus Est Solum, Ejus Est Usque Ad Ccelum Et Ad Inferos*, which is defined as "[t]o whomever the soil belongs, he owns also to the sky and to the depths. The owner of a piece of land owns everything above and below it to an indefinite extent."[20] Therefore, if a drone trespasses in air space, it will depend on how high the drone is flying as to whose air space it is violating. Also, this raises the following question: if drones are always violating either a third party's or the government's air space, then where can drones legally fly, besides right above the drone operator's own property? Boggs' lawyer, James Mackler, noted that an important precedent could be set by this case when he stated, "[p]roperty owners deserve to be free from harassment and invasion of their privacy . . . Likewise, aircraft operators need to know the boundaries in which they can legally operate without risk of being shot down. This lawsuit will give clarity to everyone."[21] In a press release, the Federal Aviation Administration ("FAA") clarified that the assumption that airspace below 400 feet is not controlled by the FAA, was false.[22] The FAA further stated that, "[t]he FAA is responsible for the safety of U.S. airspace from the ground up. This misperception [about the FAA's jurisdiction over airspace below 400 feet] may originate with the idea that manned aircraft generally must stay at least 500 feet above the ground."[23] Both cybersecurity issues and privacy issues relating to drones exemplify the lack of laws and solutions on how to handle UAS flights.

This paper will argue that it is imperative for regulations on UAVs to address cybersecurity and privacy issues in order to remain on the forefront of technology within the aviation industry. Although it may seem like it is more important to establish basic laws on UAS usage, legislators need to work proactively, rather than retroactively, to prevent detrimental cybersecurity and invasions of privacy from occurring.

---

18. 49 U.S.C. §40103 (1994).

19. *See generally* United States v. Causby, 328 U.S. 256 (1062).

20. *Cujus Est Solum, Ejus Est Usque Ad Coelum Et Ad Inferos*, BLACK'S LAW DICTIONARY FREE (2nd. ed.), http://thelawdictionary.org/cujus-est-solum-ejus-est-usque-ad-ccelum-et-ad-inferos/ [https://perma.cc/N7H7-4EXT]; Farivar, *supra* note 16.

21. *See* Farivar, *supra* note 16.

22. *See Busting Myths About the FAA and Unmanned Aircraft*, FAA (Feb. 26, 2014), https://www.faa.gov/news/updates/?newsId=76240 [https://perma.cc/R22B-PDRY].

23. *Id*.

II. TECHNOLOGICAL EXPLANATIONS

The definition of "unmanned aircraft" is "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[24] Hot air balloons are likely the first unmanned aircraft; however, they are not always considered as such because the pilot cannot fully control the balloon's flight operations.[25] Further, the term "unmanned aircraft system" means "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system."[26] A small unmanned aircraft is "an unmanned aircraft weighing less than 55 pounds."[27] The small unmanned aircraft is what the newly enacted Part 107 regulates, which will be discussed later in this paper.[28]

The International Telecommunication Union defines cybersecurity as:

> the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise… availability, integrity, … [and] confidentiality.[29]

According to the United States National Academy of Sciences, cyber attacks are defined as the "deliberate actions to alter, disrupt, deceive,

---

24. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331, 126 Stat. 11, 72 (2012).

25. *See* THE FUTURE OF DRONE USE: OPPORTUNITIES AND THREATS FROM ETHICAL AND LEGAL PERSPECTIVES 9 (Bart Custers ed. 2016); Tom Harris, *How Hot Air Balloons Work*, HOW STUFF WORKS, http://science.howstuffworks.com/transport/flight/modern/hot-air-balloon2.htm [https://perma.cc/U65B-MXRF] (last visited Dec. 26, 2016).

26. FAA Modernization and Reform Act § [?].

27. *Id*.

28. *See* Mary Ellen Callahan & Laura Fong, *FAA final rule doesn't advance drone debate*, L.A. DAILY JOURNAL, (June 29, 2016), https://www.americanbar.org/content/dam/aba/images/air_space/course/16-annual/am16-3-faa-final-rule-drone.pdf [https://perma.cc/2382-NXR6].

29. *Definition of Cybersecurity*, INT'L TELECOMM. UNION, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [https://perma.cc/QY2H-GZTX] (last visited Dec. 27, 2016).

degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[30]

III. HISTORY OF BASIC DRONE LAW

The United States' airspace is the busiest in the entire world;[31] yet, the government has not provided adequate solutions on how to handle drones and its operations within US airspace. In February 2007, the FAA released a statement that UAS are aircrafts and, as such, the FAA banned commercial drone operations unless the drone operator was given an exemption and was a licensed pilot.[32] The exemptions for commercial operations were to be reviewed by the FAA on a case-by-case basis.[33]

In 2012, Congress enacted the FAA Modernization and Reform Act, which required that the FAA establish regulations to bring UAS into the overall national airspace system.[34] The new FAA regulations had to be established by September 30, 2015.[35] The FAA missed the deadline for enacting regulations regarding drones, claiming that their number one goal was safety and that the enactment of these regulations would take additional time.[36] Thus, litigation ensured.

The Federal Aviation Administration v. Raphael Pirker was the first case in which the FAA fined a drone operator.[37] On October 17, 2011, Pirker used a Zephyr drone to take aerial photographs of the University of Virginia.[38] Due in part to Pirker's use of the drone for commercial purposes without FAA approval, he was charged with operating a drone in a reckless manner and was fined $10,000.[39] The FAA claimed that "Pirker operated the aircraft within about 50 feet of numerous individuals, about 20 feet of a crowded street, and

30. Jennifer Ann Urban, *Not Your Granddady's Aviation Industry: The Need To Implement Cybersecurity Standards and Best Practices Within the International Aviation Industry*, __ ALB L.J. SCI. & TECH. __, (forthcoming 2017) (quoting NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

31. *See* Naveen C. Rao, *Federal Regulation of Airspace and Air Traffic*, *in* AVIATION REGULATION IN THE UNITED STATES 333 (David Heffernan & Brent Connor eds., 2014).

32. *See From A Drone's Eye*, CONCORD ACAD. (Nov. 8, 2016), https://concordacademy.org/news/drones-eye-view/ [https://perma.cc/T867-YTWP].

33. *Id*.

34. *See generally*, FAA Modernization and Reform Act § [?].

35. *Id*.

36. *See* Keith Wagstaff, *FAA Misses Deadline for Creating Drone Regulations*, NBC NEWS (Oct. 1, 2015, 3:29 PM), http://www.nbcnews.com/tech/innovation/faa-misses-deadline-creating-drone-regulations-n437016 [https://perma.cc/5NR3-ENVW].

37. *See* Stephen Pope, *FAA Settles Landmark Pirker UAV Case*, FLYING MAG. (Jan. 27, 2015), http://www.flyingmag.com/news/faa-settles-landmark-pirker-uav-case [https://perma.cc/6ZG3-2GNR].

38. *Id*.; *See also* Mike M. Ahlers, *Pilot Wins Case Against FAA Over Commercial Drone Flight*, CNN (Mar. 6, 2014, 10:07 PM), http://www.cnn.com/2014/03/06/us/drone-pilot-case-faa/ [https://perma.cc/TWV5-2F8M].

39. *Id.*

within approximately 100 feet of an active heliport at UVA."[40] When Pirker challenged the $10,000 fine, he initially won and Administrative Law Judge Patrick G. Geraghty dismissed the fine, ruling that model aircrafts were not aircrafts and therefore, not covered by the FAA's commercial aircraft operations regulations.[41] The FAA appealed to the National Transportation Safety Board ("NTSB"), which appointed a new judge who subsequently overturned the initial decision and found that the FAA did have the authority to regulate drones because drones fell within the definition of "aircraft."[42] Due to the FAA's win on appeal, the original $10,000 fine was re-imposed.[43] The FAA and Pirker finally reached a settlement in January 2015.[44] The settlement allowed Pirker to not admit guilt and dropped the fine to $1,100.[45] A key takeaway from this case is that it portrayed the need for clear regulations on drone operations.

The FAA separated its regulations of UAS based on the type of operation of the drone, as well as its specific characteristics, such as size and power.[46] On December 21, 2015, the FAA's first regulations regarding recreational use of drones went into effect.[47] One of the key regulations enacted requires owners of a drone weighing between 0.55 and 55 pounds to register the drone with the FAA before it legally can be operated.[48] After the recreational owner registers the drone, it must abide by the following FAA safety guidelines:

- "Fly at or below 400 feet;
- Be aware of airspace requirements and restrictions;
- Stay away from surrounding obstacles;
- Keep your UAS within sight;
- Never fly near other aircraft, especially near airports;
- Never fly over groups of people;
- Never fly over stadiums or sports events;

40. *Id*.
41. *Id*.
42. *See* David Esler, *FAA vs. Raphael Pirker*, AVIATION WK. NETWORK (Dec. 28, 2015), http://aviationweek.com/bca/faa-vs-raphael-pirker [https://perma.cc/4QF6-LS69].
43. *Id*.
44. *Id*.
45. *Id*.
46. *See generally* FAA Modernization and Reform Act § [?].
47. *See From A Drone's Eye*, CONCORD ACAD. (Nov. 8, 2016), https://concordacademy.org/news/drones-eye-view/ [https://perma.cc/RR8U-8K6K]; The recreational use of small unmanned aircraft systems ("UAS") is the operation of an unmanned aircraft for personal interests and enjoyment. For example, using a sUAS to take photographs for your own personal use would be considered recreational; using the same device to take photographs or videos for compensation or sale to another individual would be considered a commercial operation. *See Recreational Users*, KNOW BEFORE YOU FLY, http://knowbeforeyoufly.org/for-recreational-users/ [https://perma.cc/5PFT-MYTU] (last visited Dec. 28, 2016).
48. *See* Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. 78593 (Dec. 21, 2015).

- Never fly near emergency response efforts such as fires; [and]
- Never fly under the influence of drugs or alcohol."[49]

Before the new commercial use of small drone regulations went into effect in 2016, there were three specific ways to partake in commercial UAS operations.[50] The three options were:

> (i) apply for and obtain an exemption from the supervision and registration requirements of the Federal Aviation Act pursuant to Section 333 of the FAA Modernization and Reform Act of 2012 (Section 333 Exemption) and operate the UASs pursuant to the express terms of the Section 333 Exemption;
> (ii) obtain an airworthiness certificate for the UASs and operate the aircraft by a pilot pursuant to an operating certificate; or
> (iii) obtain a Certificate of Waiver or Authorization from the FAA and operate the UASs pursuant to the terms of such Certificate of Waiver of Authorization.[51]

An Airman Certificate was required by the drone operator under all three of these options.[52] Although most commercial drone usage at that time fell under the Section 333 Exemption, when operations were conducted by public entities it was only necessary to get a Certificate of Waiver/Authorization.[53] The section 333 exemption allowed the Secretary of Transportation to determine, on a case-by-case basis,[54] as to whether individual drone operations could be conducted safely within the United States national airspace.[55] Through the Section 333 petitions reviewed before

49. *Fly for Fun*, FAA, https://www.faa.gov/uas/getting_started/fly_for_fun/ [https://perma.cc/832E-GLZL] (last visited Dec. 28, 2016).

50. *See* Marcelle Lang & Thomas A. Zimmer, *Update: Commercial Drone Operations in the US*, VEDER PRICE PC (Dec. 2016), http://www.vedderprice.com/Update-Commercial-Drone-Operations-in-the-US-12-20-2016/.

51. *Id*.

52. *Id*.

53. *See* Lang & Zimmer, *supra* note 50. A Certificate of Waiver or a Certificate of Authorization is defined as "a Federal Aviation Administration grant of approval for a specific flight operation." FAA Modernization and Reform Act § [?].

54. FAA Modernization and Reform Act of 2012 § 333(b). According to Section 333(b): [i]n making the determination under subsection (a), the Secretary [of Transportation] shall determine, at a minimum – (1) which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, and operation within visual line of sight do not create hazard to users of the national airspace system or the public or pose a threat to national security; and (2) whether a certificate of waiver, certificate of authorization, or airworthiness certification . . . is required for the operation of unmanned aircraft systems.

55. *Id*.; *See also* Lang & Zimmer, *supra* note 50.

Part 107 was enacted,[56] the FAA was able to learn from and adjust its original regulations to help create the final regulations in Part 107.[57]

The highly anticipated FAA regulations on small drones were released in June 2016, with a focus on balancing safety and economic factors.[58] These rules are for commercial drone operations, as opposed to recreational flights.[59] According to the FAA, over the next ten years, these new regulations could help create at least an $82 billion increase in the U.S. economy and 100,000 new jobs.[60] Part 107, the non-recreational drone operation regulations, finally went into effect on August 29, 2016, nearly a year after they were supposed to have been enacted.[61] Part 107 rules apply to drones that weigh less than 55 pounds and regulate many different types of commercial operation.[62] One key aspect of Part 107 is that it requires the operator hold a "remote pilot airman certificate with a small UAS rating" or be directly supervised by a person that has earned this certificate.[63] Another important aspect of Part 107 is that, if a planned drone operation does not completely comply with the FAA's regulations, the operator must obtain a waiver before this drone operation can take place.[64] the other Part 107 basic rules for commercial drone operation are similar to the recreational operation rules discussed above and require that the operator:

- operate the Small UASs within visual line of sight of the Remote Pilot;
- operate the Small UASs during daylight hours;
- operate the Small UASs at a height of not more [than 400 feet];
- operate the Small UASs at or below 100 mph;
- not fly the Small UASs over people except for those participating in the operation or those under a covered structure;
- not operate the Small UASs from a moving vehicle unless the operation is over a sparsely populated area;
- yield the Small UASs to manned aircraft; and

56. *See Section 333*, FAA, https://www.faa.gov/uas/beyond_the_basics/section_333/ [https://perma.cc/M5L5-DR2R] (last visited Dec. 28, 2016). As of September 28, 2016, 5,551 petitions had been granted and 1,780 had been closed. *Id.*

57. *See* Lang & Zimmer, *supra* note 50.

58. Callahan & Font, *supra* note 28.

59. *Id*.

60. *Id*.

61. *The FAA's New Drone Rules Are Effective Today*, FAA (Aug. 29, 2016, 12:07 PM EST), https://www.faa.gov/news/updates/?newsId=86305 [https://perma.cc/PCN6-6V3X].

62. *Fact Sheet – Small Unmanned Aircraft Regulations (Part 107)*, FAA (June 21, 2016), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516 [https://perma.cc/K22C-HKR8].

63. *Id.*

64. *Id.*

- only operate the Small UASs in non-FAA controlled airspace.[65]

If the FAA finds that the operations outside Part 107 allowances can be done in a safe manner, it is likely that the FAA will issue the waiver or airspace authorization.[66] As of October 25, 2016, the FAA had denied 71 Part 107 waiver requests and 854 airspace authorization requests.[67] The FAA announced that most of these denials were due to the request having wrong or missing information.[68] Further, the FAA clarified that many of the denied requests were due to applicants trying to receive too many waivers of Part 107 regulations or gain authorization in the types of airspace that the FAA has not yet approved for drone operations.[69] Although Part 107 allows the FAA a flexible model with which to work for commercial drone operations,[70] it does not provide enough clarification on how the issues of privacy and cybersecurity with drones should be handled.

IV. DRONE CYBERSECURITY ISSUES

The potential for cyber attacks may not initially be viewed as a concrete threat to the United States as compared to other security issues, such as bombings and in-person hijackings, but cyber attacks can create just as much damage.[71] According to researchers at the National Research Foundation of Korea, drones are highly susceptible to cybersecurity issues because they have a "highly exposed technical system due to the unique configuration such as open state of the sensors at all times, wireless network, serially safety structure, etc."[72] The three main classifications under which cyber attacks on drones can be categorized are hardware attacks,[73] wireless attacks,[74] and sensor spoofing.[75] Each of these presents new obstacles that must be overcome in order to ensure secure and safe drone operation and require legislators to establish regulations that pertain to each classification. Drone

65. Lang & Zimmer, *supra* note 50.

66. *Id*.

67. *See FAA Issues Part 107 Waivers, Airspace Authorizations*, FAA (Oct. 25, 2016, 9:50 AM EST), https://www.faa.gov/news/updates/?newsId=86707 [https://perma.cc/57S6-2U2J].

68. *Id*.

69. *Id*.

70. *Id*.

71. *See* Urban, *supra* note 30, at 64.

72. Young Sil Lee et al., *An Overview of Unmanned Aerial Vehicle: Cyber Security Perspective*, 4 ASIA-PACIFIC PROCEEDINGS OF APPLIED SCI. & ENG'G FOR BETTER HUMAN LIFE 128, 129 (2016).

73. Hardware attacks occur when the "attacker has access to the UAV autopilot components directly." *Id*. at 130.

74. Wireless attacks occur when the "attacker carries out the attacks through one of the wireless communication channels." *Id*.

75. Sensor spoofing is occurs when the "attacker passes false data throughout the on-board sensors (e.g., GPS receivers, vision, radar, sonar, LIDAR, and the IR sensors) of the UAV autopilot." *Id*.

cybersecurity issues are a great context within which the government can be proactive rather than reactive in developing its regulations, if substantial work begins immediately. While discussing the difficulty of keeping cybersecurity standards up-to-date with technological advances, Axel Jahn, the managing director of vice president of business development for connectivity at TriaGnoSys, stated, "[w]hat has been established is going to be outdated as soon as you publish it so we maybe need to have a new philosophy on how we are installing things in an aircraft."[76] In this regard, it is imperative that any new regulatory measures be flexible enough to advance a technology as drones advance.[77] Cybersecurity solutions are currently emphasized in aviation,[78] so it makes sense to continue on this path to include UAS in the aviation sector, which needs guidance for these types of potential risks.

In its commentary on the new FAA regulations on UAS, the Electronic Privacy Information Center ("EPIC") stated that "[t]he integration of drones into the NAS ["National Airspace System"] will mean that thousands of new, hackable devices will be hovering over our homes and streets without any clear security guidance, despite known vulnerabilities."[79] Drone operations can be hacked and its stored information could then be intercepted and compromised, creating both a security problem and a privacy issue.[80] In October 2016, the United States Federal Trade Commission ("FTC") illustrated how easily drones can suffer cybersecurity issues when it hacked into three different types of drones sold to civilians, which cost the FTC less than $200 to do so.[81] The FTC hacks also portrayed how easily an operator's and a third-party's privacy rights could be violated by a hacker.[82] According to the FTC, these are the four main points demonstrated by the hacks:

- Researchers were able to take over the video feed on all three of the drones, since the data was sent unencrypted.
- With two of the drones, they were able to take control of the flight path, as well as turn off the aircraft, causing both to fall from the sky.
- All of the smartphone apps made for the devices gave no indication or inconsistent notifications when a third party

76. Juliet Van Wagenen, *Experts Speak to Cyber Security in* Aviation, AVIONICS TODAY (June 12, 2015), http://www.aviationtoday.com/av/topstories/Experts-Speak-to-Cyber-Security-in-Aviation_85266.html [https://perma.cc/SH6Q-A9T9].

77. *Id*.

78. Urban, *supra* note 30, at 64.

79. Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016)

80. *See* Amie Stepanovich, *Legal Safeguards Are Needed to Protect Against Domestic Use of Drones*, *in* DRONES 100, 103 (Louise Gerdes ed., 2014).

81. *See* April Glaser, *The U.S. Government Showed Just How Easy It Is to Hack Drones Made by Parrot, DBPower and Cheerson*, RECODE (Jan. 4, 2017, 5:07 PM), http://www.recode.net/2017/1/4/14062654/drones-hacking-security-ftc-parrot-dbpower-cheerson [https://perma.cc/YWW6-V45D].

82. *Id*.

was connecting to the drone, so the operator wouldn't know if someone was watching the video feed.

- Each of the drones acted as a Wi-Fi access point, allowing devices to connect to the drone like a home router, but, according to the FTC, they required no password to actually connect.[83]

The FTC stated that UAS manufacturers can tighten drone security and prevent successful cyber attacks on drones by encrypting the UAS with a wi-fi signal that is password protected.[84] This hacking lesson is a perfect demonstration of drone cybersecurity issues and provides ways UAS operators can prevent or limit these types of issues from occurring. The United States Government should keep taking actions similar to those of the FTC in order to continue the development of drone cybersecurity solutions in areas where these issues can be regulated.

On December 27, 2016, then President-elect Donald Trump announced that Thomas P. Bossert would serve as assistant to the president for homeland security and counterterrorism.[85] In this position, Bossert would be responsible for addressing cybersecurity issues.[86] When discussing his appointment of Bossert, President-elect Trump stated, "[h]e has a handle on the complexity of homeland security, counterterrorism and cybersecurity challenges."[87] In response to his appointment, Bossert said that the country:

> [M]ust work toward [a] cyber doctrine that reflects the wisdom of free markets, private competition and the important but limited role of government in establishing and enforcing the rule of law, honoring the rights of personal property, the benefits of free and fair trade and the fundamental principles of liberty.[88]

The statements released around this appointment by both President-elect Trump and Bossert do not give the impression that there will be substantial cybersecurity policy changes by the new administration, but only time will tell how cybersecurity issues are addressed.[89] Bossert has the ability to address and help solve a vast array of cybersecurity issues' hopefully, one of which will be cybersecurity surrounding drones. In turn with his free market stance, Bossert could possibly use his position to bring together different industry members to help solve drone cybersecurity threats without

83. *Id*.
84. *Id*.
85. *See* Michael D. Shear, *Trump Picks Thomas Bossert as Top Counterterrorism Adviser*, N.Y. TIMES (Dec. 27, 2016), http://www.nytimes.com/2016/12/27/us/politics/thomas-bossert-national-security-trump.html?_r=0 [https://perma.cc/B8T5-3YFW].
86. *Id*.
87. *Id*.
88. *See* Jimmy H. Koo, *Trump Names Cybersecurity Adviser with Free Markets View*, BLOOMBERG (Dec. 29, 2016), https://www.bna.com/trump-names-cybersecurity-n73014449113/ [https://perma.cc/92ES-2ZHG].
89. *Id*.

the need for only government legislators being involved. It is imperative that all members of the international UAS community help develop, implement, and follow cybersecurity frameworks and measures in order to maintain safety throughout the entire UAS industry and all drone operations.

Another cybersecurity issue that has recently arisen is in the market for drone-countering technologies.[90] The purpose of drone-countering technology is to stop drones from operating where they should not be flying or from conducting intrusive activities.[91] Although non-governmental use of these technologies is outlawed in the United States due to drones being private property, there is still a chance they will be used illegally.[92] Recently, the FAA has been testing drone-countering technologies at Denver International Airport.[93] The technologies being tested range from services that detect UAS around airports and "geofencing software," that could potentially be required on non-government operated drones, to automatically prevent drones from flying in certain areas.[94] This testing is authorized under and funded by the Fiscal Year 2016 appropriations regulations, which require the FAA look into drone-countering technologies, and the FAA Extension, Safety and Security Act, which allowed for $6,000,000 to be spent on "airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems."[95] The FAA's goal is to have set drone-countering technologies that will be used at airports by the Fall of 2017.[96]

These new drone-countering technologies are working on "cracking the radio wireless protocols used to control a drone's direction and payload to then take it over and block its video transmission."[97] For example, DroneVision Inc. of Taiwan claims that it is the first drone-countering company that is able to "anticipate the frequency hopping that many drones use . . . " [and] "the anti-drone gun – resembling a rifle with two oversized barrels, coupled with a backpack – blocks the drone's GPS signals and video transmission, forcing it to return to where it took off via the drone's own failsafe features."[98] The argument for drone-countering technologies is that they allow people to stop drone operations from infringing on their privacy rights.[99] Non-governmental use of drone-countering technologies creates a huge cybersecurity problem and many safety issues.

One reason for the development of drone-countering technologies is the lack of regulations protecting a person's privacy from drone operations. The

90. *See* Jeremy Wagstaff & Swati Pandey, *Dog Fight: Start-ups Take Aim at Errant Drones*, REUTERS (Jan 2, 2017, 8:29 PM), http://www.reuters.com/article/us-tech-drones-idUSKBN14M180 [https://perma.cc/Q8LV-C6TX].

91. *Id*.

92. *Id*.

93. *See* Bill Carey, *FAA Will Evaluate 'Counter-UAS' Technology at Denver Airport*, AIN (Nov. 9, 2016, 10:53 PM), http://www.ainonline.com/aviation-news/aerospace/2016-11-09/faa-will-evaluate-counter-uas-technology-denver-airport [https://perma.cc/KY9B-S49N].

94. *Id*.

95. *Id*.

96. *Id*.

97. *See* Wagstaff & Pandey, *supra* note 90.

98. *Id*.

99. *Id*.

lack of drone cybersecurity regulations across the world allows the public to try and take on the issue by themselves. Cybersecurity issues pose a risk to safety, making them fall under the purview of the FAA, therefore, the FAA quickly needs to determine how best to regulate and solve the existing and future problems that come with drones. It is critical to regulate how cybersecurity technologies can and cannot be used by the public to interfere with drone operations.

V. DRONE PRIVACY ISSUES

Privacy law is defined as "[r]egulation[s] or statute[s] that protect a person's right to be left alone, and govern collection, storage, and release of his or her financial, medical, and other personal information."[100] In regards to technology as a whole, most privacy laws are outdated.[101] For example, the United States government has not updated or clarified privacy laws regarding technology devices, such as Fitbit, which as of right now are likely much more widely used than drones.[102] Although a Fitbit could allow for infringement on the user's privacy and a drone would allow for a drone user to infringe on a third-party's privacy rights, both portray the issue of privacy laws not adequately regulating technological devices. When referring to drones, former United States Defense Secretary Robert Gates claimed, "[t]he more we have used them, the more we have identified their potential in a broader and broader set of circumstances," which exemplifies the increasing uses that need to be regulated.[103] The rulemaking body has a difficult task of balancing the needs of security, such as drone surveillance in criminal matters, and not infringing on privacy rights.[104] It is critical that rulemaking bodies prioritize the crafting of new laws to handle the privacy concerns that come with drones.

A. History of Drone Privacy Laws

Many privacy advocates argue that, before more drones are allowed to enter airspace, there needs to be adequate legal safeguards established to protect citizens from drones violating their constitutionally protected privacy.[105] According to EPIC's association litigation counsel, Amie Stepanovich, "[d]rones may … carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers."[106] These

100. *Privacy Law*, BUS. DICTIONARY, http://www.businessdictionary.com/definition/privacy-law.html [https://perma.cc/42LP-T3BQ] (last visited Oct. 6, 2016).

101. *See* Jennifer Ann Urban, *Has GPS Made the Adequate Enforcement of Privacy Laws in the United States a Luxury of the Past?*, 16 J. BUS. L. & INTELL. PROP. L. 400, 414 *(2016).*

102. *Id*. at 402-03.

103. *See* John W. Whitehead, *The Domestic Use of Drones Poses Serious Threats to Civil Liberties*, *in* DRONES 63, 64 (Louise Gerdes ed., 2014).

104. *See generally* COUNTERTERRORISM TECHNOLOGY & PRIVACY 16 (2005).

105. Stepanovich, *supra* note 80, at 100.

106. *Id*. at 101.

capabilities allow for in-depth and constant surveillance, which human surveillance could not provide on the same level.[107] Although this technology continually advances, the laws surrounding it have not followed suit. Currently, there are no sufficient laws in place to protect privacy rights from drone technology and its increasing use in everyday life.[108]

B. General Privacy Laws

The First, Third, Fourth, and Fifth Amendments to the United States Constitution pertain to privacy.[109] The First Amendment gives persons the right to have their own personal, private beliefs.[110] The Third Amendment protects a person's privacy within their home by not allowing soldiers to use a private person's home.[111] The Fourth Amendment protects the privacy of a person in the United States against unlawful search and seizure.[112] The Fifth Amendment protects the privacy of personal information by not requiring a person to commit self-incrimination.[113] None of these four amendments adequately address privacy violations committed by private persons to other persons. While the Fourth Amendment helps solve the privacy issue of government officials potentially using drones to commit unlawful searches, it does not help when a non-governmental entity uses a drone to commit surveillance and violate a person's privacy rights. The public cannot rely on these amendments alone to address privacy risks posed by new technologies, such as drones.

Another place to look for guidance on privacy laws is in Section 652B of the Second Restatement of Torts.[114] This section states "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[115] The standard used by this restatement is that of the reasonable person, which can be difficult to apply to drones.[116] This is because the technology is so new that it may not be possible to determine what a reasonable person would do in a situation.

Two examples may exemplify this issue better. First, if a drone operator was purposefully using his drone to hover over the fenced in pool of his neighbor to record her sunbathing, it is likely that a court would find his actions to be highly offensive to a reasonable person. The neighbor is likely

---

107. *Id*. at 102.

108. *Id*. at 105.

109. *See* Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVE SCIENCE (June 12, 2013, 5:34 PM EST), http://www.livescience.com/37398-right-to-privacy.html [https://perma.cc/78V7-TDES], *cited in* Urban, *supra* note 101.

110. *Id*.

111. *Id*. *See also* U.S. CONST. amend III.

112. *See* Urban, *supra* note 101.

113. *Id*. *See also* U.S. CONST. amend. V.

114. *See generally* RESTATMENT (SECOND) OF TORTS § 652 (AM. LAW INST. 1979), https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

115. *Id*.

116. *Id*.

to feel as though her private backyard pool no longer remained private and that there had been an invasion of her privacy. Second, if a new drone operator was testing the drone he received for his birthday and intentionally flew it over his neighbor's backyard trying to record a bird, but also accidentally in turn recorded not only the bird, but his sunbathing neighbor, the standard would likely prove to be more difficult to decipher. A reasonable person may not find his action highly offensive since he did not intend to record his neighbor, despite violating herprivate backyard. The reasonable person standard also would require the determination of whether intent was needed for a violation of privacy through drone operations to occur. If the drone operator immediately deletes the recording of his neighbor, since he only wanted pictures of the birds, a reasonable person may be more likely to not find a violation of privacy in this context versus if he purposely wanted to keep or distribute the images of the neighbor. Due to the lack of clarification on how to apply the reasonable person standard to drone operations, tort law does not provide an adequate solution to privacy issues raised by drones.

In his concurrent opinion in *United States. v. Jones*, Justice Alito also used Justice Murphy's quote from *Goldman v. United States*, which perfectly sums up technology's impact on privacy laws, stating:

> the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.[117]

Similar to the analysis of Section 652B of the Second Restatement of Torts, the changes and advancements in technology create gaps in the legal framework because differing perceptions of privacy make it difficult to develop a privacy standard.[118]

Justice Alito further emphasized, in his concurrence in *Jones*, that while people may not like the decrease in privacy that new technologies may create, people may still accept less privacy rights because they see the technologies' diminishment of privacy as unavoidable.[119] In respect to drone operations, it is important that people do not fall into the trap of accepting diminished privacy laws and, instead, push for better privacy legislation to protect their fundamental rights.[120] Without this push, the detrimental consequences of drone operators not having to consider the privacy of others would leave a world where one would have nearly no privacy, unless they were inside a room with no windows so that drone cameras could not see them (at least until drone technologies had the capability to see through walls). Justice Alito

117. United States v. Jones, 132 S. Ct. 945, 959 (2012) (Alito, J., concurring) (quoting Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting)), *cited in* Urban, *supra* note 101.

118. *Id.*,*cited in* Urban, *supra* note 101, at 424.

119. *Id.*

120. *Id.*

suggested that the best way to handle technology changes and privacy laws is through legislative action.[121] Justice Alito explained that:

> The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.[122]

By developing and enacting new drone privacy laws, the legislature will limit the amount of interpretation that courts will need to do and will help to avoid courts' ruling on these issues with inconsistent interpretations.[123] Although *Jones* was about deciphering global positioning systems' impact on privacy laws, the technological advancement of privacy issues are similar to those created by drones and, at least, provide a bit of direction on the best path to solutions.

C. Drone Specific Privacy Laws

Thus far, the bits and pieces of privacy laws and explanations put into place in the United States cannot be compiled to make a clear or comprehensive privacy law doctrine that can be applied to new technologies within this "cyber age."[124] In 2012, the Association for Unmanned Vehicles Systems International ("AUVSI") established a Code of Conduct for the drone industry.[125] Although the idea was well intentioned, the usefulness of this action was minimal due to the lack of consequences for any violations of the Code.[126] The Code specifically states, "[w]e will respect the privacy of individuals" but it does not give an answer as to what should be done if this privacy is not respected by a drone operator.[127] This Code of Conduct calls on the industry to hold other members to "a high professional and ethical standard," yet it does not have support from the rest of the industry.[128] Even though AUVSI claims it is "serving more than 7,500 members from

121. Stepanovich, *supra* note 80, at 105.

122. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring), *cited in* Urban, *supra* note 101, at 425.

123. Urban, *supra* note 101.

124. *See* AMITAI ETZIONI, THE NEW NORMAL 105 (2015).

125. Peter W. Singer & Jeffrey Lin, *A Drone Industry Code of Conduct Is Inadequate to Protect Americans*, *in* DRONES 94, 96–97 (Louise Gerdes ed., 2014); *Unmanned Aircraft System Operations Industry "Code of Conduct"*, ASSOC. FOR UNMANED VEHICLE SYS. INT'L (2012) [hereinafter *Code of Conduct*], http://www.auvsi.org/content/conduct [https://perma.cc/V56B-ZL92].

126. Singer & Lin, *supra* note 125.

127. *Code of Conduct*, *supra* note 125; Singer & Lin, *supra* note 125, at 96–97.

128. *Code of Conduct*, *supra* note 125.

government organizations, industry and academia,"[129] the Code of Conduct only listed seventeen members that supported it.[130] The fact that the Code of Conduct itself mentions how it hopes to gain the support of the entire UAS industry and the small number of listed supporters, solidifies that support from industry members of all sectors is still significantly lacking.[131] Additionally, the Code of Conduct is extremely vague and short. It provides no real guidance or regulation on the operation of drones by any type of user. The Code of Conduct helped initiate the general discussion on privacy and security issues, but lacked actual substance in tackling these problems. Therefore, it is necessary industry members from both the public and private sectors to work together to establish a solution that can significantly handle the large issues of privacy and security in terms of drone usage before the issues get even more out of hand.

Aviation attorney, Mark Dombroff's, prediction that "it is pretty much a 'slam dunk' that Part 107 won't have any privacy rules," was found to be accurate when the new regulations were finally released.[132] The FAA consciously chose not to address critical privacy concerns within Rule 107.[133] EPIC brought suit against the FAA for not addressing privacy issues created by unmanned aircraft, however, the Court rejected EPIC's suit as premature, since the proposed rulemaking had not yet gone into effect.[134] The FAA argued that it is not tasked with addressing privacy concerns and that it is exclusively tasked with "maintaining a safe and efficient national airspace."[135] Instead of tackling these privacy concerns on its own, the FAA explained that it "intend[ed] to continue addressing privacy concerns through engagement and collaboration with the public, stakeholders and other agencies with authority and subject matter expertise in privacy law and policy. Privacy is beyond the purview of its mission of safety and efficiency."[136] Different solutions from around the world as to how these issues should be

129. *See Who is AUVSI?*, ASSOC. FOR UNMANED VEHICLE SYS. INT'L (2012), http://www.auvsi.org/home/learnmore [https://perma.cc/9AYS-KH2E].

130. *Code of Conduct*, *supra* note 125. The members that are listed on the AUVSI website as supporters of the Code of Conduct are: American Aerospace Airborne Systems Group, Arcturus UAV, Aviation Management, CAV Ice Protection, Cochise College, Domaille Engineering LLC, Dragonfly Pictures Inc., FreeWave, INSITU, ISR Group, Kawak Aviation Technologies, Mesa County Sheriff's Office – Colorado, Reactel, Incorporated, Tiffin Technologies, Toyon Research Corporation, UAV MarketSpace, and XRDi. *Id.*

131. *Id.*

132. *See* Mark Dombroff, *UAS/FAA: The FAA Has No Business In The Privacy Business!*, DENTONS: PLANE-LY SPOKEN BLOG (May 26, 2016), http://www.planelyspokenblog.com/uasfaa-the-faa-has-no-business-in-the-privacy-business [https://perma.cc/C2BA-DXQC].

133. Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016).

134. *See generally* Electronic Privacy Info. Ctr v. FAA, 821 F.3d 39 (D.C. Cir. 2016).

135. *See* Bryan Koenig, *FAA Tells D.C. Circ. Drone Privacy Challenge Doesn't Fly*, LAW360 (Nov. 5, 2015, 7:46 PM EST), http://www.law360.com/articles/723976/faa-tells-dc-circ-drone-privacy-challenge-doesn-t-fly [https://perma.cc/6R9L-GEEU].

136. *See* Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016).

regulated, and who is in charge of the regulating, are discussed *infra*. These other nations' regulators vary between courts, legislatures, and government agencies. In order to remain consistent with aviation laws, the overall regulations on drone operations should remain within the purview of the federal government. It would be helpful for Congress to enact additional legislation that addresses privacy issues regarding drones, but guidance from federal agencies could also be useful in quickly creating solutions to these issues.

Part 107's analysis provided by the FAA points interested individuals to the National Telecommunications and Information Administration's ("NTIA's") "Voluntary Best Practice for UAS Privacy, Transparency, and Accountability" ("NTIA Best Practices"), which will be discussed *infra*.[137] Although these Best Practices at least attempt to solve drone privacy issues, its self-regulating and non-binding nature make it unlikely that they will be followed.[138] While the FAA is correct in that privacy falls outside its areas of duty, the unsolved issue of who should be tasked with handling drone privacy concerns continues to hamper the discussion on solutions and delay this time-sensitive issue.[139] As mentioned previously, the best group to address privacy issues, since the FAA is unable, is the United States legislature. The legislature should not be the only entity tasked with solving these issues, though. The entire drone industry should be involved in developing solutions, but the legislature should take the lead.

D. Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

On May 19, 2016, NTIA released a "Best Practices document" encompassing the ways multistakeholder group best addressed the issues of privacy, transparency, and accountability for civilian drone operations, including commercial operations.[140] The NTIA Best Practices suggest guidelines for drone operators to follow.[141] For example, one suggestion is to attempt not to fly over private property.[142] This may sound sensible in theory, but in reality, it is very unlikely to be followed or even plausible.[143] A big problem surrounding the Best Practices is the fact that they are completely

137. Callahan & Fong, *supra* note 28.

138. *Id*.

139. *Id*.

140. The multistakeholder group consisted of "representatives from industry, news organizations, consumer and privacy advocacy groups, academics and trade associations." *NTIA Releases Drone Privacy Best Practices*, HUNTON & WILLIAMS: PRIVACY BLOG (May 20, 2016), https://www.huntonprivacyblog.com/2016/05/20/ntia-releases-drone-privacy-best-practices/ [https://perma.cc/C2J4-K3LJ].

141. Callahan & Fong, *supra* note 28.

142. *Id.*

143. *Id*.

voluntary and no one is actually required to follow them.[144] NTIA makes clear that "[i]n some cases, these Best Practices are meant to go beyond existing law and they do not – and are not meant to – create a legal standard of care by which the activities of any particular UAS operator should be judged."[145]

The five main best practices that NTIA gives are quoted as follows:

1. Inform others of your use of UAS . . .
2. Show care when operating UAS or collecting and storing covered data . . .
3. Limit the use and sharing of covered data . . .
4. Secure covered data . . .
5. Monitor and comply with evolving federal, state, and local laws.[146]

Under Best Practice one, it is recommended that drone operators notify individuals of the approximate timeframe of the operations and that the drone may be purposefully capturing covered data.[147] Under Best Practice two, the drone operator should not purposefully use a UAS to collect covered data where it is reasonable to believe a person in that area has an expectation of privacy.[148] Best Practice three recommends that a drone operator should not use covered data that they have collected from their UAS operations without permission for these purposes: "employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility."[149] Best Practice four suggests that UAS pilots take reasonable steps to handle security threats of covered data by establishing adequate safeguard measures.[150] The Best Practices suggest the following ways of minimizing drone security risks, "appropriate administrative, technical, and physical safeguards include those described in guidance from the Federal Trade Commission, the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, and the International Organization for the Standardization's 27001 standard for information security management."[151]

It is great that the Best Practices address cybersecurity. The solutions they give are on the right track to preventing cybersecurity attacks. These solutions will hopefully lead to regulation in this area and more guidance on

144. *See Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*, NAT'L TELECOMMS. & INFO. ADMIN. (May 19, 2016), https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf [https://perma.cc/2RGC-6W89].

145. *Id.*

146. *Id*. The term "covered data" is defined as "information collected by a UAS that identifies a particular person. If data collected by UAS likely will not be linked to an individual's name or other personally identifiable information, or if the data is altered so that a specific person is not recognizable, it is not covered data." *Id.*

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id*.

151. *Id.*

how to address cybersecurity threats. Finally, Best Practice five makes sure to remind drone operators to stay informed about the changing laws regarding the UAS industry.[152]

There are still many issues that remain unsolved by NTIA's Best Practices. First, it remains unclear how much privacy a person can expect to have on their own property.[153] Due to the advancements in technology, the reasonable expectation of privacy standard has been brought into question.[154] Second, data collection by drones has raised the issue of how legal it is to collect data on other people or activities without permission.[155] This involves the need to regulate the data in many contexts, such as the type of information, its purpose, and its storage.[156] The guidelines do provide some guidance on the data issue, but they are not detailed enough to completely clarify data collection, storage, and distribution with the many different ways in which they can be done. Overall, the Best Practices provide decent guidance on how to prevent some privacy and cybersecurity issues with UAS operations. The multistakeholder approach is the perfect way to get members of all areas of the drone industry involved, but the Best Practices are still a long way from providing critical, concrete, and mandatory solutions to these issues.

VI. GLOBAL DRONE LAWS AND SOLUTIONS

In a 2014 statement, the FAA challenged the notion that commercial drone operations' approval is behind that of other nations.[157] The FAA claimed that:

> The United States has the busiest, most complex airspace in the world, including many general aviation aircraft that we must consider when planning UAS integration, because those same airplanes and small UAS may occupy the same airspace. Developing all the rules and standards we need is a very complex task, and we want to make sure we get it right the first time. We want to strike the right balance of requirements for UAS to help foster growth in an emerging industry with a wide range of potential uses, but also keep all airspace users and people on the ground safe.[158]

The FAA is not solely focused on aviation regulations within the United States, but is tasked with working with other nations to solve joint aviation

152. *Id*.
153. *See* Callahan & Fong, *supra* note 28.
154. *Id*.
155. *Id*.
156. *Id*.
157. See *Busting Myths About the FAA and Unmanned Aircraft*, *supra* note 22.
158. *Id.*

issues.[159] The objectives of the Agreement on Rulemaking Cooperation Guidelines for the Federal Aviation Administration and the European Aviation Safety Agency are to:

> 1. Exchange rulemaking intentions and priorities of the Participants to align as much as possible their respective rulemaking programmes;
> 2. Identify rulemaking initiatives of common interest that through regulatory collaboration would allow the FAA and the EASA to[160]: (i) avoid unnecessary divergence and duplication of work, (ii) maximize available resources, and (iii) further harmonization.
> 3. Define the corresponding working methods … to be followed by the Participants when executing tasks which have been identified as of 'common interest.[161]

Through collaboration with other countries, such as the European Union, there can be more thorough development of drone laws and solutions to privacy and cybersecurity problems with drone activities.

It is also important to look to global differentiations in the drone laws because countries with laws that give more structure and better provide for businesses within the drone industry will likely gain economic advantages. Companies using drones are likely to move some of their operations to those countries. For example, Jeff Bezos, the founder of Amazon, announced in 2013 that he wanted to use drones to deliver Amazon packages sometime in the future.[162] At that time, the United States had not enacted any laws that prohibited drone operations, however, once Part 107 was enacted, it highly burdened the idea of drone delivery services.[163] Due to the barriers on drone delivery services in the United States, Amazon has begun testing these services in Canada and Australia instead.[164] According to Michael Drobac, senior policy advisor at Akin Gump Strauss Hauer & Feld, "the U.S. has fallen

159. *See* Jonathan B. Rupprecht, *The Federal Aviation Administration Rulemaking Process*, *in* UNMANNED AIRCRAFT IN THE NAT'L AIRSPACE 43, 67 (Donna A. Dulo, ed., 2015). According to the United States Code, "[t]he [FAA] shall promote and achieve global improvements in the safety, efficiency, and environmental effect on air travel by exercising leadership with the [FAA]'s foreign counterparts, in the International Civil Aviation Organization and its subsidiary organizations, and other international organizations and fora, and with the private sector." 49 U.S.C. §40104(b) (1994).

160. *Rulemaking Cooperation Guidelines for the Federal Aviation Administration and the European Aviation Safety Agency*, FAA (June 13, 2013), https://www.faa.gov/regulations_policies/rulemaking/media/FAAandEASA.pdf [https://perma.cc/R7VQ-SY32].

161. *Id.*; *see also* Rupprecht, *supra* note 151, at 67–68.

162. *See* Seung Lee, *Amazon's Dream of Drone Package Delivery Can Be Real In 'Less Than Five Years'*, NEWSWEEK (June 29, 2016, 9:49 AM EST), http://www.newsweek.com/amazons-dream-drone-package-delivery-can-be-real-less-five-years-475667 [https://perma.cc/XGG6-XT77].

163. *Id*.

164. *Id*.

behind other developed countries in accommodating drone technology due to FAA's reticence to take action."[165]

Although the United States has not been conducive in the past for drone delivery services, Part 107 could lead the way to better regulatory relations between the government and drone entities within the private sector.[166] One view is that the Part 107's legal framework sets a path where the FAA, with the input of drone delivery companies, can enact laws that accommodate this type of operation and keep more of the drone market within the United States.[167]

Bezos provided another view that, rather than having the FAA focus on drone delivery regulations, it would be faster and provide a more proactive approach if, instead, Congress took on this role and enacted drone delivery service legislation.[168] Finally, there is still a chance that drone delivery services will be permitted on a case-by-case basis under Part 107, but only time will tell if the FAA will allow these types of exceptions.[169] Privacy issues with drone cybersecurity , probably more so with drone delivery services, remain, such as drones getting hacked and packages or personal information being stolen. Whatever the way that drone delivery services are established, it is critical that they encompass solutions to privacy and cybersecurity issues.

Even though United States legislators have currently chosen to avoid enacting privacy and cybersecurity regulations, either because legislators are not tasked with it or it is unclear who is in the best position to handle these issues, other countries have taken measures to try and solve these issues.[170] Legislators have struggled to keep up with the continually advancing drone technologies.[171]

A. Additional Country Specific Solutions

Each country has its own way of handling the regulation of drone technologies, including not addressing it at all. It is important to look at the different solutions around the world to drone privacy and cybersecurity that other countries have implemented in order for the United States to be able to develop the best and most efficient solutions. Appendix A includes a chart of additional countries that have enacted privacy laws that drone operators must

165. *Id*.
166. *Id*.
167. *Id*.
168. *Id*.
169. *Id*.
170. *See* THE LAW LIBRARY OF CONGRESS, REGULATION OF DRONES 11 (2016), https://www.loc.gov/law/help/regulation-of-drones/regulation-of-drones.pdf.
171. *See* Kris Graham, *Kris Graham: FAA Requiring Drone Registration*, CLARION LEDGER (Dec. 16, 2015, 4:07 PM), http://www.clarionledger.com/story/business/businessledger/2015/12/16/kris-graham-faa-requiring-drone-registration/77386932/ [https://perma.cc/4HAV-38RF].

follow, but that are not discussed in depth below.[172] A common theme portrayed in Appendix A is that most of the countries listed have generic laws that require the operator to respect the privacy of persons not involved in the drone operations, but do not specify the requirements the operator must follow regarding another's privacy.[173] The lack of clarity provided by nearly all of these laws perfectly portrays the great size of the issue: how should a drone operator not infringe on other's privacy rights and abide by privacy laws?[174]

1. Australia

The Civil Aviation Safety Authority ("CASA") of Australia claims that "Australia was the first country in the world to regulate remotely piloted aircraft[s], with the first operational regulation for unmanned aircraft in 2002."[175] CASA enacted regulations regarding commercial drone operations on September 29, 2016.[176] Not more than two weeks after these new laws were implemented, the Australian government began a large-scale review of safety under these regulations.[177] The new regulations followed a risk-based model, where drone operations that were seen as less risky fell under more lenient regulations.[178] This type of law has struck a debate between traditional aircraft pilots and the drone industry.[179] Manned aircraft pilots and others involved in air traffic management argue that the regulations are too flexible and allow for unsafe operations.[180] Others in the drone industry disagree and claim that CASA's new regulations allow drone industry competition to increase and be less burdensome on regulatory authorities.[181]

There have been few, if any, cases in Australia where a person succeeded in bringing a violation of privacy claim against a drone pilot for his UAS operations.[182] According to Australian attorney, Matthew Craven, "[u]nless the drone pilot is working for an organization with at least $3 million in annual revenue, 'it is not possible for a private individual to take action against an individual drone pilot under the Privacy Act as it currently

172. *See Drone Laws By Country*, UAV SYS. INT'L, https://uavsystemsinternational.com/drone-laws-by-country/ [https://perma.cc/7NC9-S7UF] (last visited Jan. 2, 2017).

173. *Id*.

174. *Id*.

175. *See* Meenal Dhande, *The Current Scenario of Global Drone Regulations and Laws*, GEOSPATIAL MEDIA & COMMN'S. (Nov. 19, 2016) [hereinafter *Regulation of Drones*], https://www.geospatialworld.net/article/present-global-drone-regulations-laws/ [https://perma.cc/T2B3-FCTA].

176. *Id.*

177. *Id*.

178. *Id*.

179. *Id*.

180. *Id*.

181. *Id*.

182. *See generally* Andy Kollmorgen, *Drones and Australian Law*, CHOICE (Oct. 10, 2016), https://www.choice.com.au/electronics-and-technology/gadgets/tech-gadgets/articles/drones-and-privacy-rights [https://perma.cc/9SSF-UE5V].

stands.'"[183] There are other ways that private individuals can seek a remedy to privacy violations, such as trespass tort law, but the strength of this type of a case remains uncertain.[184]

CASA is similar to the FAA in that it is not tasked with providing solutions to privacy issues brought about by drone activities.[185] CASA acknowledges that drone operations can create privacy concerns, but states, "CASA's role is restricted to aviation safety – privacy is not in our remit."[186] The Office of the Australian Information Commissioner is tasked with handling privacy issues, however, it has not yet issued solutions to privacy questions regarding UAS operations.[187] Further, in 2014, an Australian parliamentary committee advised that current laws should be reviewed to consider if new legislation was needed to solve drone operations impact on privacy rights, however, no changes to the existing laws were ever made.[188] The current laws also do not provide any solutions to cybersecurity threats on drone activities.

2. Canada

In December 2016, Canada initiated a new drone reporting tool for citizens to report drone operations that it believes are unsafe or reckless.[189] This new tool provides people access via their mobile devices to alert the Canadian government of unsafe drone operations and provides specifics of the drone immediately, rather than hoping the individual can remember details later.[190] This mobile reporting tool does not replace the current reporting mechanisms, such as the Civil Aviation Daily Occurrence Reporting System ("CADORS") or reporting to local police any emergencies,[191] that may occur from drone usage.[192] Besides the basic time, date, and location of the reckless drone operation, the incident-reporting mechanism also asks:

- Was the drone flying near an aircraft?

183. *Id*.

184. *Id*.

185. *See Flying Drones/Remotely Piloted Aircraft in Australia*, AUSTL. GOV'T CIV. AVIATION SAFETY AUTH., https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia [https://perma.cc/Y9Z9-7XDZ] (last visited Jan. 3, 2017).

186. *Id*.

187. *See Id*.

188. *See* Regulation of Drones, *supra* note 170.

189. *See* Kirsten Thompson, *Transport Canada Launches Online "Drone Incident" Reporting Tool*, MCCARTHY TÉTRAULT LLP (Dec. 23, 2016), http://www.canadiancybersecuritylaw.com/2016/12/transport-canada-launches-online-drone-incident-reporting-tool/ [https://perma.cc/3TG3-R4FC].

190. *Id*.

191. Transport Canada tells citizens that if they see someone operating a drone "in a way that poses a threat to safety, security, or privacy" that they should contact their local police right away. *See Report a Drone Incident*, TRANSPORT CAN., https://www.tc.gc.ca/eng/civilaviation/opssvs/report-drone-incident.html [https://perma.cc/UWR5-DMHE] (last visited Dec. 29, 2016).

192. *See* Thompson, *supra* note 189; *Report a Drone Incident*, *supra* note 191.

- Was the drone flying at a high altitude?
- Was the drone flying close to an airport/aerodome . . . ? and
- Did the drone fly close to or over . . . a populated area[;] home/private property[;]crowd (sporting event, concert, festival)[;] firework show[;] forest fire[;] national park[;] wildlift[;] moving vehicles, highways, busy streets, bridges
- Give a brief description of the incident[;]
- Description of drone
- Colour, Category,[193] Make/Model
- Description of the operator
- Name of operator and/or company . . .; Operator's vehicle/License plate number . . .[;] physical description . . .
- Have you gathered evidence such as photos or videos of this incident?
- Can a Transport Canada official contact you for more information regarding this evidence?[194]

Further, the form allows the reporter to remain anonymous if he or she chooses.[195] Through this simpler method of incident reporting, it is likely that Canada will have much more information to identify and prosecute illegal drone operations. This reporting method is a wonderful solution to help the government learn about and solve privacy violations by drone operators. For example, if someone is sunbathing in their fenced-in backyard and they notice a drone taking pictures of them, they can immediately report it.

In addition to the new incident reporting tool, the Canadian government has focused on three other key areas.[196] First, Canada announced in the Fall of 2017 the proposed laws for "small drones (25 kilograms or less) that are operated within visual line-of-sight".[197] Previously, this type of drone usage was not covered by legislation, but the government believes these new proposed regulations are necessary in order to clarify how persons can legally conduct this type of drone operations.[198]

Second, the Canadian government has established partnerships with numerous drone manufacturers to better promote safe drone operation.[199] These partnerships require that the participating UAS manufacturers include government safety cards with each drone purchase and participating UAS

193. The form provides pictures of common drones, but also allows for a user to mark that it is unsure of the type of drone. *See infra* App. B.

194. *See Report a Drone Incident*, *supra* note 191.

195. *Id.*

196. *See* Thompson, *supra* note 189.

197. *Id.*

198. *Id.*

199. *Id.*

retailers to include a link to Transport Canada's drone safety website on the retailer's own website.[200]

Third, the Canadian government implemented a "No Drone Zone" campaign to inform the public about drone safety regulations.[201] This campaign focused especially on working with airports to ensure that "No Drone Zone" signs were placed throughout various airport properties, with the hope of minimizing the chance a UAS would interfere with airport or manned aircraft operations.[202]

3. China

In December 2015, the Civil Aviation Authority of China ("CAAC") issued new drone-specific regulations that were to be used on a trial basis before CAAC would decide whether or not to permanently implement them.[203] Soon after these regulations were announced, a drone crashed into power lines in Sichuan, which caused a major blackout and initiated a heated debate regarding drone regulations.[204]

The drone industry is quickly growing.[205] It is especially important that CAAC keep China's laws up-to-date with the industry because . . . .[206] China's regulations cover what lawful drone operations entail, but still focus on the allowance of approved UAS operations to be seen as normal everyday practices. Under the regulations, drones are classified into seven different categories depending on how much they weigh or its specific activities.[207] The strictness of the laws for operation depends on the location of the drone activities, for example, rural locations have more lenient laws while highly populated areas have extremely strict laws.[208] Drones that fall into the first classification are the smallest and have very few regulations to follow, besides not injuring others and conducting safe flights.[209]

Two of the unique and most important regulations established by CAAC are the "UAS Cloud" and the "electronic fence."[210] The "UAS Cloud" is defined as "a dynamic database management system that monitors flight data, including operation information, location, altitude, and speed, in real

200. *Id*.
201. *Id*.
202. *Id*.
203. *See* Dhande, *supra* note 175.
204. *See China: New Drone Regulatory System to Limit Accidents*, https://www.suasnews.com/2016/01/new-drone-regulatory-system-to-limit-accidents/ [https://perma.cc/L88D-Z6JW].
205. *See* Dhande, *supra* note 175.
206. *Id*.
207. *See* App. C; E. Tazewell Ellet et al., *China Launches First Operational Rules for Unmanned Aircraft*, HOGAN LOVELLS (Jan. 20, 2016), http://ehoganlovells.com/rv/ff0024ec11e538d3067f1ce89a4d910aeea3f45d [https://perma.cc/WZ9S-VGLC]; *see also* Dhande, *supra* note 175.
208. *See* Ellet et al., *supra* note 207; *see also* Dhande, *supra* note 175.
209. *See* Ellet et al., *supra* note 207.
210. *See Regulation of Drones*, *supra* note 170, at 39.

time… [and includes] an alarm function for UAS connected to it that is activated when these UAS fly into the electronic fence."[211] The "electronic fence" is defined as "a system consisting of hardware and software that stops aircraft from entering certain areas."[212] Drones that fall into classifications III, IV, VI, and VII are required to use both of these technologies, while also reporting every single second they are operating in highly populated locations and every thirty seconds in less populated areas.[213] UAS that fall into classifications II and V are only required to use the electronic fence and the UAS Cloud, while reporting once a minute if they are flying in specific locations,[214] and airport clear zones.[215]

If the drone operations do not fall under these classifications, they are not required to use the electronic fence or the UAS cloud, but still must include the operators contact information on the drone to allow for easy identification.[216] One way that CAAC could solve privacy issues is to use the electronic fence to block drone operations from going outside specific non-public areas, however, this use is likely to be found to be way too narrow and would not allow for beneficial advancements in the drone industry. CAAC should consider better solutions while still using these technologies to address privacy and cybersecurity concerns. Both the UAS cloud and the electronic fence portray China's ability and desire to use technology to enforce and combat issues arising from new technologies, such as UAS.[217]

Chinese experts have called on CAAC to implement laws that protect a person's privacy from drone operations.[218] These experts have also suggested that more security precautions, such as criminal background checks before one is allowed to operate a UAS, be taken to help address threats to privacy and cybersecurity[219] This is a great model for every country to follow and would help prevent bad actors from joining the UAS community, thereby preventing the occurrence of some malicious and unlawful drone activities.

211. *Id*. at 36.
212. *Id*.
213. *Id*. at 39.
214. Specific locations are defined by CAAC as "key areas" that include "military sites, nuclear plants, administrative centers and their neighboring areas, and areas temporarily designated as key areas by local governments." *Id*.
215. *See* Ellet et al., *supra* note 207.
216. *Id*.
217. *See* Dhande, *supra* note 175.
218. *See Absence of Regulations Leaves China's Drone Sector Vulnerable to Security Threats*, BEIJING INT'L, http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1404043.htm [https://perma.cc/4Q8J-D5XY] (last visited Jan. 3, 2017).
219. *Id*.

4. European Union

The European Union's ("EU's") parliament defines a drone as "an aircraft that operates without a crew aboard."[220] Currently, the EU allows for drone operations that are remotely controlled, but not for drone operations that are fully automatic.[221] Most EU countries that have regulated drone operations require that drones weighing more than the 44 – 55 pound threshold (depending on the country) have special authorization before they are flown.[222] Thus far, drones weighing less than 55 pounds have been the most popular in the European region.[223]

The EU is also concerned with increasing the public's knowledge about drone regulations and has created an interactive website as a part of its public awareness campaign.[224] The website informs visitors of both privacy and safety rules by which drone operators must abide.[225] Drone intrusions on privacy and personal data are considered violations of fundamental human rights within the EU.[226] The legislation on this point is general in nature and not drone specific, however, drone operations fall under it.[227] Drone operators should remember that drone operations can easily violate these fundamental rights and that drones that include any type of recording devices must conduct lawful activities under data protection regulations.[228]

One example given by the public awareness campaign is that "you should not take photographs, videos or sound records of people in their home, their garden, their car, etc. without their permission; and remember that data protection and privacy apply even in public spaces."[229] Drones without recording devices can still violate privacy laws.[230] In certain circumstances, privacy laws can also be found to protect personal property.[231] A person who believes their privacy rights have been violated by drone operations may bring a claim against the drone operator either in court or to the national data protection authority.[232]

---

220. *See Civilian Drones: Different countries, different rules*, EUROPEAN PARLIAMENT, http://www.europarl.europa.eu/resources/library/images/20161111PHT50912/20161111PHT50912_original.jpg [https://perma.cc/X7TZ-YRZP] (last visited Jan. 2, 2017).

221. *Id*.

222. *Id*.

223. *Id*.

224. *See Drone Rules*, EUROPEAN UNION, http://dronerules.eu/en/ [https://perma.cc/HR7V-2TJS] (last visited Jan. 2, 2017).

225. *Id*.

226. *See Summary of Privacy Rules in EU*, EUROPEAN UNION, http://dronerules.eu/en/recreational/obligations/summary-of-privacy-rules-in-eu-1 [https://perma.cc/4CRA-PBS9] (last visited Oct. 5, 2017).

227. *See Drone Rules*, *supra* note 224.

228. *Id*.

229. *See Summary of Privacy Rules in EU*, *supra* note 226.

230. *Id*.

231. *Id*.

232. *Id*.

In July 2016, the European Commission began a partnership between both the public and private sectors to focus on solving cybersecurity threats.[233] By 2020, it is expected that, through the donations from both sectors, 1.8 billion euros will be invested in European cybersecurity initiatives.[234] According to the Commissioner for the Digital Economy and Society, Gunther H. Oettinger:

> There is a major opportunity for our cybersecurity industry to compete in a fast-growing global market. We call on Member States and all cybersecurity bodies to strengthen cooperation and pool their knowledge, information and expertise to increase Europe's cyber resilience. The milestone partnership on cybersecurity signed today with the industry is a major step."[235]

Commissioner Oettinger has exactly the right idea. Collaboration of representatives from all different sectors and entities is the best path for finding a solution that works and solves issues for the industry as a whole. Although the partnership is focused generally on cybersecurity,[236] solutions that come out of it will hopefully be applicable to the drone industry. Further, this partnership is a perfect model for the global drone industry and nation-specific drone industries to follow as to how to create the best solutions for both cybersecurity and privacy issues pertaining to UAS activities.

European organizations are also involved in helping to develop solutions in regard to drone laws. The Innovation and Digital Technologies Division of the European Commission has separated drone operations into three basic categories: open operations, specific operations, and certificated operations.[237] Appendix D displays a chart with more detail regarding the categories, however, while the basic classification of drone operations is useful at clarifying some drone operations, it does not have a good structure for providing which detailed rules operators in each category will have to follow.[238] It also does not explain whether each category will get its own rules regarding each issue or if rules will overlap between the categories.[239]

The Single European Sky Air Traffic Management ("ATM") Research initiative ("SESAR") is an EU entity that develops insights into how its

233. *See Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tack Cyber-threats*, EUROPEAN COMMISSION (July 5, 2016), http://europa.eu/rapid/press-release_IP-16-2321_en.htm [https://perma.cc/Q2KB-MUM6].

234. *Id*.

235. *Id*.

236. *Id*.

237. *See Setting Up Rules for Safe Drone Operations in the EU*, EUROPEAN COMMISSION (Nov. 2016), http://ec.europa.eu/transport/modes/air/aviation-strategy/innovation_en [https://perma.cc/2VYF-BHRJ].

238. *Id*.

239. *Id*.

members believe drones should be handled.[240] SESAR proposes that their seven pillars of research, one of which is "security and cyber resilience," are key to enacting proper drone procedures for the EU.[241] SESAR claims that the EU's ability to address cybersecurity threats from drones will be the determining factor in how quickly the entire European UAS industry will grow.[242] Further, SESAR argues that the EU community will become more accepting of drones the longer the period in which no cybersecurity drone incidents occur.[243] Although this is true, drone technologies have already quickly started to play a large role in EU's society.[244]

According to SESAR, one of the best ways for the EU to regulate the UAS industry is to ensure that "the capabilities of drone flights must be preserved for beneficial purposes, meaning risks associated to privacy violations, flights in protected environments, and cybersecurity aspects must be properly managed to avoid negative impacts to society."[245] It is wonderful that SESAR mentions the importance of privacy and cybersecurity regulations and, if followed by the European Commission, it will be a good example for other nations. They will see that it is critical to prioritize these issues. SESAR does address the fact that they have not yet developed clear guidelines on how to solve the cybersecurity issues, but, with proper legislation, it will motivate private entities to help create concrete solutions.[246]

Another argument SESAR makes is that "[p]rivate initiatives are exploring potential solutions such as digital identification but clear concepts of operations, requirements and standards are needed to drive research into a more advanced and coordinated phase."[247] SESAR may not have developed the best solutions to privacy and cybersecurity issues, but simply by working to solve these issues proactively, the EU is likely to be on track to having some of most encompassing regulations.

5. France

France has a very advanced drone industry and was one of the first nations to enact legislation on commercial drone operations.[248] The regulation

240. *See* SESAR JOINT UNDERTAKING, EUROPEAN DRONES OUTLOOK STUDY 2 (Nov. 2016), http://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf [https://perma.cc/7YHS-ZWJK].

241. *Id.* at 6.

242. *Id.* at 10.

243. *Id.* at 16.

244. *See Drones: New EU Rules to Ensure Safety and Privacy*, EUROPEAN PARLIAMENT NEWS (November 11, 2016), http://www.europarl.europa.eu/news/en/news-room/20161107STO50307/drones-new-eu-rules-to-ensure-safety-and-privacy [https://perma.cc/X5BF-4E3J].

245. *See European Drones Outlook Study*, *supra* note 240, at 35.

246. *Id.*at 39.

247. *Id.*

248. *See* Rude Ruitenberg, *What the French Know About Drones That Americans Don't*, BLOOMBERG (Mar. 16, 2015, 6:00 AM), https://www.bloomberg.com/news/articles/2015-03-16/what-the-french-know-about-drones-that-americans-don-t [https://perma.cc/5Q8X-622Z].

of commercial drone operations in 2012 has allowed for the commercial drone industry to grow significantly.[249] According to Redbird's CEO, Emmanuel de Maistre,[250] "France has about a year of advance on the U.S. . . . [t]he regulation created the market."[251] On January 1, 2016, France enacted two regulations regarding civilian drone operations, one of which categorizes drones based on the type of operation.[252] The three categories are "(1) hobby and competition flying, (2) flying for experimental and testing purposes, and (3) 'particular activities', which are defined as any use that does not fall into categories (1) or (2)."[253] While not completely clear, it seems as though commercial operations falls into category 3.[254]

France heavily regulates the areas where drones may fly and these laws are likely to get stricter soon.[255] French legislators are developing a law that would penalize drone operations in prohibited locations.[256] These penalties could include a six month jail sentence and a fine up to approximately $17,500.[257] Another law currently being drafted would require drones weighing over 28 ounces to have extra security devices installed on them.[258] The security devices would prevent drones from entering prohibited areas and alarms would be triggered if the drones lose control.[259] These penalties and additional security devices help to prevent drones from operating outside of the permitted zones,[260] but, in order for the law to be adequate, it should include a clause about how these regulations help protect privacy. The drone regulations in France fail to adequately address privacy and cybersecurity issues, therefore, in these terms, France is not as advanced in the drone sphere as one may think.

6. Germany

One way Germany has addressed privacy and cybersecurity concerns is by enacting laws specifically created to address privacy and protection measures for data obtained through drone operations.[261] Drones that weigh between approximately 11 and 55 pounds must obtain a specific authorization

249. *Id*.

250. Redbird is a French company that uses drones to map construction and mining sites. *See Better Data, Better Decisions*, REDBIRD, http://www.getredbird.com/en/ [https://perma.cc/HC9X-Z6SE] (last visited Jan. 5, 2017).

251. *See Ruitenberg*, *supra* note 248.

252. *See Regulation of Drones*, *supra* note 170, at 43.

253. *Id*.

254. *Id*.

255. *See France Gives Lift Off to Tough New Drone Laws*, LOCAL (Sept. 28, 2016), http://www.thelocal.fr/20160928/france-draws-up-new-tougher-drone-laws [https://perma.cc/S7A5-9FSQ].

256. *Id*.

257. *Id*.

258. *Id*.

259. *Id*.

260. *Id*.

261. *See Regulation of Drones*, *supra* note 170, at 11.

from the aviation authority before they are allowed to fly.[262] In order to get a specific authorization, one requirement is that the operator submit a data privacy statement.[263] Germany requires these types of specifications be followed; noncomplying drone activity will not be permitted.[264]

The data privacy statement clarifies that data protection and privacy laws are not violated by drone operations. If the drone operations include processing personal data for any other use than "personal or family activities,"[265] the Federal Data Protection Act applies.[266] Drones equipped with a video camera for non-recreational operations also fall under the Federal Data Protection Act.[267] According to the Federal Data Protection Act, "video surveillance of public places may only be conducted to fulfill public tasks, to exercise the right to determine who shall be allowed or denied access to a property, or to pursue rightful interests for precisely defined purposes – for example, protection against theft or vandalism."[268] Drone operations of this nature, even in private areas, still must lawfully process data and have the permission of any persons whose data is taken.[269]

Drones that are not equipped with a camera, but that have one installed and use it to take videos and pictures must abide by the Copyright Arts Domain Act.[270] According to section 22 of this Act, "images can only be disseminated with the express consent of the person concerned."[271] There are exceptions to this regulation. For instance, a picture of society in a contemporary sense that does not conflict with legitimate privacy concerns may be lawful.[272]

People in Germany also have a "General Right of Personality."[273] Both data protection rights and the "Right to Control the Use of One's Image" are included in the General Right of Personality.[274] Not only are people protected from drone operation violations, but also the privacy of their property may be found to be protected.[275] Under Section 2 of Germany's Copyright Act, it can be found that "utilizing a drone to take pictures of public buildings, bridges, sights, or statutes is therefore only permissible if the image is made for private use," however, the outside of buildings in public areas is usually lawful.[276]

---

262. *Id.* at 54.
263. *Id.* at 55.
264. *Id.* at 52.
265. The Federal Data Protection Act defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual." *Id* at 56.
266. *Id.*at 56–57.
267. *Id.* at 57.
268. *Id.*
269. *Id.*
270. *Id.*
271. *Id.* Disseminated means both public and private circulation, even if only to a small amount of people. *Id.*
272. *Id.*
273. *Id.*
274. *Id.* at 57–58.
275. *Id.* at 58.
276. *Id.*

German privacy laws for drone operations are thus far some of the most clear and efficient in the world. Other countries should look to Germany as a model for privacy laws regarding drones.

Germany has not implemented laws to help protect drones from cybersecurity issues, but this is an area where the United States and Germany may be able to work together to develop regulations. On March 22-23, 2016, the fourth round of the U.S. – Germany Cyber Bilateral Meeting occurred and both countries agreed to work together to protect critical infrastructure from cyber attacks.[277] They also agreed to "continue to work closely to enhance cybersecurity of critical infrastructure, improve incident management and coordination, and build cyber capacity of other countries."[278] It is imperative that leaders within this partnership make drone operations one of the focal points of where cybersecurity issues arise. They must also be proactive in implementing regulations that will continue to adequately regulate as drone technologies advance.

7. Israel

The drone market in Israel is known to be very large, but the market consists mostly of the use of drones for military purposes, not civilian uses.[279] Due to the limited civilian drone operations, partially because of the difficult nature of getting such operations approved, there are not many regulations in Israel for non-military drone flights.[280] It is imperative for Israel to put strong drone regulations in place because the Comorant, the first passenger carrying drone, recently completed its first solo flight.[281] The Comorant is being labeled as a flying car and the Israeli technology firm that created it hopes to have it on the market as soon as 2020.[282]

In Israel, privacy issues related to drone operations are especially a problem with the use of drones by police, yet a privacy violation public uproar has not occurred. Companies are marketing what would normally be seen as privacy-violating services to the Israeli government. For example, when a riot erupted in Jerusalem, "Bladeworx fitted drones with thermal cameras and flew them just ahead of the light-rail trains as they passed near trouble spots.

---

277. *See* Aisha Chowdhry, *U.S. and Germany Expand Cyber Cooperation*, FCW (Mar. 28, 2016), https://perma.cc/manage/create?url=https://fcw.com/articles/2016/03/28/us-germany-cyber.aspx [https://perma.cc/5LQV-4VHD].

278. *Id*.

279. *See* Christa Case Bryant, *What Privacy Debate? Police Drone Use in Israel Flies Under the Radar*, CHRISTIAN SCI. MONITOR (Sept. 19, 2014), http://www.csmonitor.com/World/Middle-East/2014/0919/What-privacy-debate-Police-drone-use-in-Israel-flies-under-the-radar.

280. *See* Aurore Geraud, *Drones in Israel: From Military to Civil Use*, L'ATELIER (Sept. 9, 2016), http://www.atelier.net/en/trends/articles/drones-israel-military-civil-use_443364.

281. *See* Stuart Winer, *Flying Ambulance Heading for Take Off: Israeli-made Cormorant Could be Used to Rescue People in Dangerous Situations, or Ferry Troops in Combat*, TIMES ISRAEL (Jan. 4, 2017), http://www.timesofisrael.com/flying-ambulance-drone-heading-for-take-off/ [https://perma.cc/5LQV-4VHD].

282. *Id*.

. .The drones relay[ed] real-time video to the train operators, police, and even City Hall, enable[ed] officials to spot potential attackers and track those who tried to escape."[283] When the police used drones in this incident, no one mentioned the privacy issues that could occur with government use of thermal camera drone flights.[284] Israel is an example of a country that may have different views on privacy than those in the United States and where it may not be necessary, under those views, to regulate privacy issues.

Israel has also failed to regulate cybersecurity issues related to drone flights, but this is likely to change in the near future. In February of 2016, the Israeli Security Agency and Israeli National Police arrested Majed Awida, who had been asked by the Palestinian Islamic Jihad to hack into the drones belonging to Israel's Defense Forces as well as other areas of the Israeli government.[285] This was not the first time one of Israel's Defense Forces' drones was hacked and, if no measures are quickly put in place, it is unlikely to be the last hack.[286] On December 16, 2016, President Obama signed the U.S. – Israel Advanced Research Partnership Act of 2016.[287] This partnership is a way for the U.S. and Israel to work together to solve cybersecurity issues and provides an opportunity to address these concerns as they relate to drone operations.[288] Israel could likely learn about beneficial regulatory models for drones and the United States. could likely learn a great deal about drone technology advancements.[289] According to United States House Representative John Ratcliff, one of the congressmen that introduced the partnership measure:

> Our discussions with Israeli national security and cybersecurity leaders revealed the immense wealth of untapped potential we can leverage together to collectively vamp up our efforts to combat growing cyber threats . . . We are extremely grateful for the opportunity to work more closely with a country that's a proven pioneer in cyber science and a top leader in cyber expertise.[290]

283. *See* Bryant, *supra* note 279. Bladeworx is a company based in Israel. *See* BLADEWORX, http://www.bladeworx.co.il/, (last visited Jan. 5, 2017).

284. *Id*.

285. *See* Elad Popovich, *The 'Palestinian Idol' that Hacked Into Israel's Drones*, SMALL WARS J. (Apr. 1, 2016, 2:00 AM), http://smallwarsjournal.com/blog/the-%E2%80%98palestinian-idol%E2%80%99-that-hacked-into-israel%E2%80%99s-drones [https://perma.cc/32BK-4MWP].

286. *Id*.

287. *See US-Israel Cybersecurity Collaboration Legislation Signed Into Law*, JEWISH TELEGRAPHIC AGENCY (Dec. 20, 2016, 12:06 PM), http://www.jta.org/2016/12/20/news-opinion/politics/us-israel-cybersecurity-collaboration-legislation-signed-into-law [https://perma.cc/5EH8-9P7P].

288. *Id*.

289. *Id*.

290. *Id*.

This partnership will hopefully get Israeli officials to focus on establishing cybersecurity drone laws.

8. New Zealand

New Zealand has drone laws that directly address privacy issues.[291] Regulations on drone operations, including provisions on privacy, came into force in New Zealand on August 1, 2015.[292] One of the regulations requires that drone operators gain consent both from private property owners of land over which they are flying and from any person over which they are flying.[293] New Zealand is similar to Germany in that its Privacy Act applies to drone operations that record people.[294] The Privacy Act 1933 regulates how information about individuals is collected, stored, and disbursed.[295] Although the Privacy Act 1933 is applicable to drones, the Office of the Privacy Commission made sure to note that "the Privacy Act is a technology neutral piece of legislation which gives the basic principles by which we can make an assessment on the privacy implications of an emerging technology."[296]

The New Zealand Privacy Commission states that privacy issues surrounding drones are consistent with the privacy issues surrounding cameras, therefore, New Zealand's CCTV[297] guidelines apply to drones and their operations that involve cameras.[298] In order to abide by the Privacy Act, the CCTV guidelines state that the key issues for any camera operator, such as the operator of a drone with a camera, to observe are:

- Being clear about why you are collecting the information;
- Making sure people know you are collecting the information;
- How you intend to use the information;
- Keeping the information safe and making sure only authorized people can see it;

---

291. *See Regulation of Drones*, *supra* note 170, at 71.

292. *See id.* at 71; *New Zealand: - New Drone Rules Protect Home Privacy*, SUAS NEWS (July 14, 2015), https://www.suasnews.com/2015/07/new-zealand-new-drone-rules-protect-home-privacy/.

293. *Id*.

294. *See Regulation of Drones*, *supra* note 170, at 11.

295. *See* Charles Mabbett, *Game of Drones*, PRIVACY COMMISSIONER (Jan. 21, 2015), https://www.privacy.org.nz/blog/drones/.

296. *Id*.

297. "'CCTV' stands for 'closed circuit television.'" "This term is relatively out of date," but when used by New Zealand's Privacy Commissioner it means "camera surveillance systems that capture images of individuals or information relating to individuals." *See* PRIVACY COMMISSIONER, PRIVACY AND CCTV: A GUIDE TO THE PRIVACY ACT FOR BUSINESSES (2009), https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf.

298. *See* Mabbett, *supra* note 295.

- Disposing of the information after it has served its purpose; and
- Right of access to the information by the individual or individuals concerned.[299]

At a minimum, these guidelines provide a framework of issues drone operators should keep in mind to lessen the chance of violating any privacy rights.

In addition to the Privacy Act and the CCTV guidelines, other New Zealand regulations may apply to drones that have the capability to film or take photographs.[300] One of these regulations makes it illegal to take "intimate recordings" of people and publish them when permission to do neither action was given.[301] The example given by the Privacy Commissioner for this regulation states, "if you are sunbathing semi-naked in your own back yard surrounded on all sides by a three metre high fence, you would have an expectation that you won't be spied on."[302] Under this example, if a drone operator was to take pictures of a person sunbathing semi-naked, the person could potentially file an invasion of privacy claim against the operator with the New Zealand courts.[303] Another regulation that applies to drone operations with cameras is Summary Offences Act 1981, Section 30, which makes it illegal to look into and record any activity happening inside a person's home.[304] Although New Zealand has only enacted a couple of regulations specifically related to drone privacy issues, the Privacy Commissioner's blog post provides wonderful guidance that solves many of these issues.[305] Other nations should consider publishing clarifying statements if they do not want to enact permanent legislation that advises drone operators as to how they can avoid any privacy issues from their operations.

Currently, New Zealand does not have any regulations that provide UAS cybersecurity solutions. Officials in other areas of New Zealand's government should consider following the Privacy Commissioner's model of providing clarification through blog posts to address the issues of cybersecurity and drones.

9. Sweden

Sweden recently made important advancements in its privacy laws regarding drones. On October 21, 2016, the Swedish Administrative Supreme Court decided the issue of whether drone operations that involve camera use fell under the definition of "camera surveillance" according to Swedish

299. *Id*.
300. *Id*.
301. *Id*.
302. *Id*. *See also* Crimes Act 1961, ss 216G–216J (N.Z.).
303. *See* Mabbett, *supra* note 295.
304. *Id.*
305. *Id.*

law.[306] The court held that this type of drone operation does constitute camera surveillance, thus, an operator must obtain a license before using drone cameras.[307] These licenses are not easily obtained because the drone operator must show that the benefit of the camera drone operations outweighs the public concern of privacy violations.[308] The cost of a license for camera drone operations ranges from $1,270 per year to $38,095 per hour, with the most expensive licenses being for more professional operations.[309] Critics of this court decision argue that it is too restrictive and overbroad as a way to protect privacy rights, which will have a detrimental effect on the Swedish drone industry.[310] UAS Sweden claims that this court decision could cause a potential loss of 5,000 jobs.[311] Sweden perfectly exemplifies the importance of weighing privacy concerns against economic harm, which is something all countries must consider when implementing new drone regulations. It is too soon to know if the Swedish court decision was a poor way to regulate privacy issues due to a harmful economic effect or if it provides a positive solution to preventing drone operations from violating fundamental privacy rights.

Sweden does not yet specifically regulate cybersecurity drone issues. Due to the privacy law determination in Sweden coming from a court opinion, it may take an actual cybersecurity case to get the Swedish government to provide solutions to drone cybersecurity issues. It is important for Sweden to regulate cybersecurity in drone operations as one way of allowing the UAS industry continue to advance.

10. United Kingdom

According to a drone survey conducted by the United Kingdom Civil Aviation Authority, 48 percent of individuals viewed drone operations as being unregulated throughout the country.[312] The government admitted that it does not have very much evidence that drone operators are purposefully violating privacy laws, however, it still believes that privacy is a concern that must be addressed.[313] Currently, there are privacy focused regulations in place

306. *See Regulation of Drones*, *supra* note 170, at 104; Tonya Riley, *Sweden's Ban on Drone Photography Raises Questions of Privacy*, INVERSE (Oct. 23, 2016), https://www.inverse.com/article/26005-honda-creriding-assist-motorcycle.

307. *See Sweden Bans Cameras on Drones*, BBC (Oct. 25, 2016), http://www.bbc.com/news/technology-37761872.

308. *See* Lisa Vaas, *Sweden Bans Cameras on Drones, Deeming It Illegal Surveillance*, SOPHOS LTD. (Oct. 27, 2016), https://nakedsecurity.sophos.com/2016/10/27/sweden-bans-cameras-on-drones-deeming-it-illegal-surveillance/.

309. *See* JP Buntinx, *Sweden Bans Unlicensed Usage of Camera Drones*, MERKLE (Oct. 28, 2016), http://themerkle.com/sweden-bans-unlicensed-usage-of-camera-drones/.

310. *Id*.

311. *See Sweden Bans Cameras on Drones*, *supra* note 307.

312. *See* CIV. AVIATION AUTH., CONSUMER DRONE USERS 7 (2016), http://dronesafe.uk/wp-content/uploads/2016/11/CAA_Consumer_Drone_Users_report.pdf.

313. *See* DEP'T FOR TRANSP., UNLOCKING THE UK'S HIGH TECH ECONOMY: CONSULTATION ON THE SAFE USE OF DRONES IN THE UK 56–58 (Dec. 21, 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579562/consultation-on-the-safe-use-of-drones.pdf.

for the operation of drones that weigh less than 150kg.[314] Under these regulations, drone operations that collect personal data have to abide by the Data Protection Act 1988 ("DPA"), unless the operator has gotten an exception or the use falls under a general exemption.[315] If an operator violates the DPA, the Information Commissioner's Office can penalize the operator by requiring the person to stop that type of operation and/or fining the person.[316] It is also important to note that a person harmed because of a drone operator violating the DPA can bring a case against the operator for monetary compensation.[317]

Another privacy regulation for UAS 150kg or under is that "[d]rones should be flown at a height over the property of another person which is 'reasonable' in all circumstances. Failure to do so could amount to trespass if the flight interferes with another person's ordinary use and enjoyment of land and the structures upon it."[318] The repercussion for trespass is that the victim can bring a civil case against the pilot for monetary compensation and can request that an injunction be put in place to make sure a trespass by this operator's drone does not occur in the future.[319] This law does not provide much guidance. Its subjectivity of the meaning of "reasonable" makes it less effective at properly regulating trespass by drone. While the idea behind it is well intentioned, other countries should consider including a more definite height-based description of when trespass could occur if they implement a similar regulation.

In addition to the regulations already in place, the United Kingdom has begun to lay the groundwork for clearer and more drone-specific laws by establishing a consultation that was announced on December 21, 2016 by the Minister for Aviation in the United Kingdom's Department for Transportation, Lord (Tariq) Ahmad of Wimbledon and will last until March 15, 2017.[320] The consultation allows for people and entities to submit ideas and weigh in on proposed legislation on how to regulate drones and how to solve legal issues regarding operations.[321] Both security and privacy are two of the main focuses of the consultation.[322] One privacy issue for which the United Kingdom is using the consultation for help is the use of cameras and recording devices on drones.[323] The United Kingdom Department for Transport is working with two other main offices, the United Kingdom

314. *Id*. at 18.
315. *Id*.
316. *Id*.
317. *Id*. at 57.
318. *Id*. at 58.
319. *Id*.
320. *Id*. at 8.
321. *Id*. at 7–8.
322. *Id*.
323. *See* Victoria Hordern & Paul Maynard, *UK Department for Transport Launches Consultation on Regulations for Civil Drone Usage*, HOGAN LOVELLS: CHRONICLE DATA PROTECTION (Dec. 23, 2017), http://www.hldataprotection.com/2016/12/articles/international-eu-privacy/uk-department-for-transport-launches-consultation-on-regulations-for-civil-drone-usage/ [https://perma.cc/WEB3-SKLY].

Information Commissioner's Office and the Surveillance Camera Commissioner, to develop drone privacy regulations and ways to make the public aware of how their UAS operations can hamper another person's privacy.[324] The consultation notes that it is the belief of the government that most privacy issues happen because the operator is unaware of the regulations they are violating, however, the government does admit that there are still some violations that are done maliciously.[325] This observation portrays the United Kingdom's motive for not only enacting laws, but also undertaking a public awareness campaign, which will hopefully decrease the amount of privacy and security issues from drone use.[326]

One solution the consultation proposes is the collection of drone operators and owners personal information in order to better enforce the laws and identify persons who are conducting illegal drone activities.[327] Also, the Department of Transport is considering if it should be mandatory for all drones to have a tag that could be scanned to help with identification.[328] According to British privacy law attorney, Victoria Hordern, the tag "would allow an individual drone to be pinpointed to a specific location at a particular time. Not only might this assist with enforcement in . . . possible privacy breaches, but data on the use of drones in particular areas could be utilized to improve coverage of drone-based services."[329] The consultation, especially its inclusion of privacy and security issues, is a great model for the United States and other countries to consider adopting. It allows key members from all sectors of the UAS industry to play a role in regulating drone operations for the greater good and, in the process, it allows people to become more informed about critical legislation that must be followed.

In addition to the consultation, the United Kingdom is solving many of the issues surrounding drones through a public awareness model.[330] The "Drone Code," published by the United Kingdom Civil Aviation Authority, uses unique graphics and a mnemonic device to help those involved in drone operations remember key regulations for safe operations.[331] For example, it is easy to remember the helpful mnemonic device, DRONE, which stands for:

- **D**on't fly near airports or airfields;
- **R**emember to stay below 400ft (120m);
- **O**bserve your drone at all times – stay 150ft (50m) away from people and property;

---

324. *Id*.

325. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313, at 19.

326. *Id*.

327. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313, at 19.

328. *Id*.

329. *Id*.

330. *See* CIV. AVIATION AUTH., THE DRONE CODE, http://dronesafe.uk/wp-content/uploads/2016/11/Dronecode.pdf (last visited Dec. 30, 2016).

331. *Id*.

- **N**ever fly near aircraft;
- **E**njoy responsibly.[332]

An improvement for this mnemonic device would be to add reminders about not interfering with others privacy and taking the proper measures to ensure an operator's UAS is as secure as possible from cyber attacks. The United Kingdom has failed to adequately address cybersecurity issues. The consultation does not specifically mention any ideas on how these issues might be resolved,[333] the United Kingdom has failed to adequately address cybersecurity issues.

VII. SOLUTIONS

The increase in drone activity calls for an increase in both cybersecurity regulations and privacy laws surrounding it.[334] The easiest, but probably the least popular, solution is to completely ban drone usage. The countries that have currently taken the complete ban approach include Bhutan, Brunei, Cuba, Nicaragua, Uzbekistan, Saudi Arabia, Oman, and Bahrain.[335] It is important to note that remote sensing operations, while sometimes heavily regulated and only used for specific purposes, are still allowed in these countries, even though drone operations are not.[336] While it may be easy to

---

332. *Id*.

333. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313.

334. *See* Stepanovich, *supra* note 80, at 109.

335. *See, e.g.*, Courtney Trenwith, *UAE Enters the Drone Age of Technology*, ARABIAN BUS. PUB. LTD. (Sept. 30, 2016, 12:26 AM), http://www.arabianbusiness.com/uae-enters-drone-age-of-technology-647344.html#.V_miitx1ZR1; *Bhutan Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bhutan-drone-laws/; *Brunei Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/brunei-drone-laws/; *Cuba Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/cuba-drone-laws/; *Nicaragua Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/nicaragua-drone-laws/; *Uzbekistan Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/uzbekistan-drone-laws/.

336. *See generally, e.g.*, *Bhutan Customs*, VisaHQ, https://bhutan.visahq.com/customs/, (last visited Jan. 2, 2016); THE LEGAL ASPECTS OF REMOTE SENSING 24 (Geospatial Insight Ltd., 2014); P.J. Blount, *Taiwan, Nicaragua Ink Satellite Imaging Pact*, RES. COMMUNIS BLOG (Oct. 6, 2010, 2:15 PM), http://rescommunis.olemiss.edu/2010/10/06/taiwan-nicaragua-ink-satellite-imaging-pact/; ASIAN DISASTER REDUCTION CTR., MINISTRY OF EMERGENCY SITUATION OF REPUBLIC OF UZBEKISTAN, http://www.adrc.asia/acdr/2010kobe/documents/S2-1_04_Uzbekistan.pdf (last visited Jan 2, 2016); Mohammad Rasooldeen, *Kingdom to use 'LIDAR' for Satellite Imagery*, ARAB NEWS (Jan. 18, 2016), http://www.arabnews.com/saudi-arabia/news/866791; *Oman – Sultanate Looks Towards Space Satellite Technology Forum Begins*, MIDDLE EAST NORTH AFRICA FIN. NETWORK (Oct. 10, 2016), http://menafn.com/1095036157/Oman--Sultanate-looks-towards-space-satellite-technology-forum-begins; *Investigating Land Use and Land Cover Change in Bahrain: 1987-2013*, AM. ASSOC. ADVANCEMENT SCI., http://www.aaas.org/page/investigating-land-use-and-land-cover-change-bahrain-1987-2013 (last visited Jan. 2, 2016).

ban UAS operations, it would hamper both technology and business, which would have further negative implications, such as economic loss. Also, if some countries ban drones and others do not, the gap widens between technologically advanced countries and those that are already being left behind.

Another solution is for Congress to make passing adequate drone privacy safeguards a priority.[337] Electronic Privacy Information Center ("EPIC") suggests a three-pronged regulation encompassing:

> - Use Limitations – Prohibitions on general surveillance that limit drone surveillance to specific, enumerated circumstances, such as in the case of criminal surveillance subject to a warrant, a geographically-confined emergency, or for reasonable non-law enforcement use where privacy will not be substantially affected;
> - Data Retention Limitations – Prohibitions on retaining or sharing surveillance data collected by drones, with emphasis on identifiable images of individuals;
> - Transparency – Requiring notice of drone surveillance operations to the extent possible while allowing law enforcement to conduct effect investigations. In addition, requiring notice of all surveillance policies through the Administrative Procedures Act.[338]

These three aspects would be a good start to having sufficient privacy protections from drone usage. The new legislation would also need to allow for private legal action against other private actors that violate privacy rights.[339] Effective privacy laws dealing with drone activities by the government must have a structure for supervising and auditing to ensure that drone usage remains for proper purposes and does not infringe on civil liberties.[340]

In addition to large scale drone regulations, simple changes or advice can also make a big difference in solving both privacy and cybersecurity concerns that drone operations raise. For example, Hong Kong does have drone-specific laws that it has enacted, but it also includes "recommended areas" for drone operations.[341] Even though Hong Kong's government does not require drone operations to be conducted only in the recommended areas, by providing this advice, it helps clarify areas where drone operators are less likely to run into legal issues. A few other countries, such as New Zealand,

337. Stepanovich, *supra* note 80, at 105.
338. *Id*. at 108.
339. *Id*.
340. *See* ETZIONI, *supra* note 124, at 120.
341. *See Hong Kong Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/hong-kong-drone-laws/.

have also provided guidance statements, or even used social media as a way to clarify rules, or answer questions from the public.[342]

It would be wise for other countries to establish many recommended areas to allow for an increase in drone activities. For example, the United States could recommend areas for drone usage in each county, or if a county is highly populated, then the closest other areas that drone operators are advised to fly. These areas should include places where privacy concerns of others would not arise, such as unpopulated areas. The Best Practices provide small scale and short time solutions, but without federal regulations, safety and privacy concerns will continue to exist.[343]

VIII. CONCLUSION

If commercial drone registrations and operations in the U.S. continue to rise, it is imperative that the industry work quickly and collaboratively to develop privacy and cybersecurity standards to keep up with this expanding rate of drone operations. According to AUVSI, within the next ten years, the United States drone industry will likely help develop around 100,000 jobs and put approximately $82 billion into the economy.[344]

Mississippi UAS attorney, Kris Graham, described the likely future of the drone industry best when he said, "[d]rones are on pace to change society as pervasively as mobile phones and the Internet.[345] Inevitably, there will be bumps in the road as this new technology matures. Both existing businesses and new start-ups can avoid disruption (or worse) by starting out on a proper, legal footing."[346] Drone operations are soon to become integral within our society. Without the proper measures in place, the legal issues that come with increased UAS operations will burden the industry and lessen the benefits. Representatives from around the global UAS community need to work together to develop the best ways to handle privacy and cybersecurity issues. This global approach will allow countries to learn from each other and will provide varying ideas on what regulations work (or do not work) at keeping laws up to date with the continually advancing UAS technology. Without adequate drone laws that address both cybersecurity and privacy, drone operations will get more out of hand. The longer there are no regulations of this type, the tougher it will be to enact clear and acceptable laws in the future.

342. *See* Mabbett, *supra* note 295.

343. *See The Disrupter Series: The Fast-Evolving Uses and Economic Impacts of Drones Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 40–47 (2015) (statement of Margot E. Kaminski, Assistant Professor of Law, Moritz College of Law).

344. *Id*.

345. *See* Kris Graham, *Regulations Surround Drone Use*, CLARION LEDGER (Sept. 9, 2015, 2:00 PM CT), http://www.clarionledger.com/story/money/business/2015/09/09/regulations-surround-drone-use/71918534/.

346. *Id*.

APPENDIX A: ADDITIONAL COUNTRIES THAT HAVE ENACTED PRIVACY LAWS REGARDING DRONE OPERATIONS

COUNTRY	LAW
Afghanistan	• Drone operations must respect the privacy of others.[347] • Media may not use drone cameras that can cause security issues.
Bahamas	• Drone operators may not fly their drones over property belonging to others, unless they have the property owner's consent.[348]
Bangladesh	• Drone operations must respect the privacy of others.[349]
Bermuda	• Drone operators must obtain permission from all property owners of land the operators plan to conduct drone activities over.[350]
Brazil	• Drone operators may not invade others' privacy.[351]
Dominican Republic	• Drone operators must respect other's privacy.[352]
Ecuador	• Drone operators are responsible for knowing privacy laws and must respect the privacy of others when conducting any drone operations.[353]

347. *Afghanistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/afghanistan-drone-laws/.

348. *Bahamas Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bahamas-drone-laws/.

349. *Bangladesh Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bangladesh-drone-laws/.

350. *Bermuda Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bermuda-drone-laws/.

351. *Brazil Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/brazil-drone-laws/.

352. *Dominican Republic Drone Laws*, UAV SYS. INT'L. (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/dominican-republic-drone-laws/.

353. *Ecuador Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/ecuador-drone-laws/.

Fiji	• Drone operators must respect the privacy of others when flying a UAS.[354]
French Guiana	• Drone operators must respect others' privacy while conducting any drone operations.[355]
Guatemala	• Drone operators must respect the privacy of others during UAS operations.[356]
Guyana	• UAS operators must respect others' privacy while conducting drone activities.[357]
Haiti	• Drone operators have to respect others' privacy during any drone flights.[358]
Hong Kong	• Prior to any drone operations, the UAS pilot must get permission from any landowner whose property the UAS operations will take place on.[359]
India	• Drone operations may be conducted over private property as long as permission of the landowner has been obtained. Drone operations over public property requires the permission of local authorities before any operations may be conducted.[360]

354. *Fiji Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/fiji-drone-laws/.

355. *French Guiana Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/french-guiana-drone-laws/.

356. *Guatemala Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/guatemala-drone-laws/.

357. *Guyana Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/guyana-drone-laws/.

358. *Haiti Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/haiti-drone-laws/.

359. *Hong Kong Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/hong-kong-drone-laws/.

360. *India Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/india-drone-laws/.

Jamaica	• Drone operators may not fly their drones over either public property or private property, unless they have received consent from the landowner.[361]
Japan	• Drone operators cannot fly over property, unless they have the property owner's permission.[362]
Kazakhstan	• Drone operators must respect the privacy of others when conducting any drone flights.[363]
Kyrgyzstan	• The privacy of others must be respected by any drone operators.[364]
Laos	• When conducting drone flights, the operator must respect others' privacy.[365]
Malaysia	• Drones may not be flown near persons who are not involved with the drone operations.[366]
Mongolia	• Drone operators must respect the privacy of others when operating a UAS.[367]
Myanmar	• UAS operators must respect others' privacy during drone operations.[368]

361. *Jamaica Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/jamaica-drone-laws/.

362. *Japan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/japan-drone-laws/.

363. *Kazakhstan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/kazakhstan-drone-laws/.

364. *Kyrgyzstan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/kyrgyzstan-drone-laws/.

365. *Laos Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/laos-drone-laws/.

366. *Malaysia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/malaysia-drone-laws/.

367. *Mongolia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/mongolia-drone-laws/.

368. *Myanmar Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/myanmar-drone-laws/.

Nepal	• Drone operators must respect others' privacy when conducting drone flights. It is also important to note that many Nepal locals have reported drone operations near them that they are unhappy about.[369] • Surveillance of persons by drone operations is strictly prohibited, as it is a violation of privacy.[370]
Pakistan	• Drone operators must respect others' privacy during drone flights.[371]
Panama	• When flying drones, operators must respect the privacy of others.[372]
Philippines	• Drone pilots must respect others' privacy during UAS flights.[373] • The Data Privacy Act does not currently address whether or not drones violate it when using recording devices.[374]
Poland	• A drone operation that entails filming, over private property, may be considered a violation of personal rights and the property owner may file a claim against the operator. (Poland law does not have regulations specific to drones, but the general laws of privacy rights may apply to drone operations.)[375]

369. *Nepal Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/nepal-drone-laws/.

370. Purushottam Khatri, *Security Agencies, CAAN Concerned Over Rising Drone-Flying Practices*, RISING NEPAL (Sept. 3, 2016), http://therisingnepal.org.np/news/14165.

371. *Pakistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/pakistan-drone-laws/.

372. *Panama Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/panama-drone-laws/.

373. *Philippines Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/philippines-drone-laws/.

374. *CAP Regulations On Drones*, DISINI L. OFFICE (Mar. 16, 2016), http://www.elegal.ph/cap-regulations-on-drones/.

375. *Drones – Will the Law Allow Them to Crowd the Sky?*, CMS LAW-NOW (Sept. 22, 2015), http://www.cms-lawnow.com/ealerts/2015/09/drones--will-the-law-allow-them-to-crowd-the-sky?cc_lang=en.

Russia	• Persons not involved with drone operations must have their privacy respected by drone operators.[376]
South Korea	• Drones may not fly over people and drone operations must operate as to respect the privacy of others.[377]
Suriname	• Operators must respect others' privacy when flying their drones.[378]
Tajikistan	• Drone pilots must respect others' privacy when conducting UAS operations.[379]
Thailand	• Drones may not fly over people and operators must respect the privacy of others.[380]
Turks and Caicos	• Drones shall not be flown over persons not involved with their operation and the privacy of others not involved in the flight must be respected.[381]
Vietnam	• Drones cannot fly over people not involved with the drone flight and the privacy of others must be respected by drone operators.[382]

376. *Russia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/russia-drone-laws/.

377. *South Korea Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/south-korea-drone-laws/.

378. *Suriname Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/suriname-drone-laws/.

379. *Tajikistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/tajikistan-drone-laws/.

380. *Thailand Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/thailand-drone-laws/.

381. *Turks and Caicos Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/turks-caicos-drone-laws/.

382. *Vietnam Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/vietnam-drone-laws/.

APPENDIX B: CANADIAN DRONE INCIDENT REPORT FORM DEPICTIONS

The pictures below are those that are included on the Drone Incident Report Form,[383] which citizens can fill out to report unsafe drone operations.[384] These illustrations are a great way of helping people who are not familiar with different kinds of drones better identify the model of the drone they are reporting. The form also allows the reporter to check a "Not Sure" category or fill out an "Other" box if they cannot precisely identify the drone using the below illustrations.[385] If a person has seen a drone violating their privacy, but is unfamiliar with the types of drones, the depictions aid their identification and better ensure accuracy of the reported descriptive information. It is highly probable that this simple mechanism will greatly increase the ability of the government to then identify and prosecute the drone operator, which exemplifies why this model should be used in other countries' reporting methods.

(Labeled "fixed wing drone")[386]

(Labeled "Fixed Wing Drone")[387]

383. *Drone Incident Report Form*, TRANSPORT CAN., https://www.tc.gc.ca/eng/civilaviation/opssvs/drone-incident-report-form.html (last visited Dec. 29, 2016).
384. *Id*.
385. *Id*.
386. *Id*.
387. *Id*.

(Labeled “Quadcopter”)[388]

(Labeled “Quadcopter”)[389]

388. *Id.*
389. *Id.*

APPENDIX C: CLASSIFICATION OF DRONE OPERATIONS IN CHINA

CATEGORY	**DRONE'S EMPTY WEIGHT (kg)**	**DRONE'S WEIGHT ON TAKE-OFF (kg)**
I	Weight must be between 0kg and 1.5kg	Weight must be between 0kg and 1.5kg
II	Weight must be between 1.5kg and 4kg	Weight must be between 1.5kg and 7kg
III	Weight must be between 4kg and 15kg	Weight must be between 7kg and 25kg
IV	Weight must be between 15kg and 116kg	Weight must be between 25kg and 150kg
V	UAS operations specifically for agricultural use in protecting plants	UAS operations specifically for agricultural use in protecting plants
VI	Operation of "unmanned airships"[390]	Operation of "unmanned airships"[391]
VII	Operations of drones in categories I and II, but are conducted beyond the visual line of sight further than 100 meters	Operations of drones in categories I and II, but are conducted beyond the visual line of sight further than 100 meters.

Note: According to attorneys at Hogan Lovells, "if the empty weight and take-off weight of a UAS are respectively within the parameters of different classifications among Type I to Type IV, it shall be classified as the type with the higher requirements."[392]

390. Ellet et al., *supra* note 207.
391. *Id.*
392. *Id.*

APPENDIX D: CLASSIFICATION OF DRONE OPERATIONS IN THE EU

OPERATION CLASSIFICATIONS	Open	Specific	Certificated
RISK ALLOCATION	Low	The risk level varies and is dependent on the type of operation being conducted.	Traditional amount of risk in aviation related activities.
OPERATIONS	These operations include, but are not limited to: • "Flying own drone • Photography and filming • Industrial operations"[393]	These operations include, but are not limited to: • "Mailing • Infrastructure Inspections • Commercial or Industrial Operations"[394]	These operations will likely be similar to those of traditional aviation and will include the transportation of cargo.
EXAMPLE	A farmer flying a drone over his private property and no one else's property.	A drone operator photographing a sporting match.	A store operating a drone to deliver a package that a customer bought online.
SPECIAL REGULATIONS	None listed	Specific regulations will need to be adjusted to fit the particular operation's risk level.	These operations will at least require: • "[a] Remote pilot license • Certification of drones • Operation Manual"[395]
RULE CLASSIFICATION	The rules that apply to this category are considered rules that pertain to product safety.	Traditional aviation rules will be applied to these types of operations.	Traditional aviation rules will be applied to these types of operations.

393. *Setting Up Rules for Safe Drone Operations in the EU*, *supra* note 237.
394. *Id.*
395. *Id.*

ENFORCEMENT AGENCY	Local police will enforce open drone operations.	Aviation Authorities will enforce specific drone operations.	Aviation Authorities will enforce certificated drone operations.

What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble

Philip M. Napoli *

TABLE OF CONTENTS

* James R. Shepley Professor of Public Policy, Sanford School of Public Policy, Duke University; Andrew Carnegie Fellow. An earlier version of this paper was presented at the 45th Research Conference on Communications, Information, and Internet Policy. The author gratefully acknowledges the research assistance of Petra Ronald and Anne Napoli. This publication was made possible by a grant from the Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the author.

I. INTRODUCTION

The results and aftermath of the 2016 U.S. presidential election have brought increased attention to the dynamics of the contemporary news and information ecosystem and how these dynamics affect citizen knowledge and political decision-making. Specific points of focus have included the extent to which algorithmically-driven search and social media platforms are facilitating the construction of "filter bubbles" or "echo chambers",[1] the presence of political bias in content curation platforms,[2] the extent to which such platforms facilitate the widespread dissemination of false news stories,[3] and inflammatory political advertisements placed by foreign governments.[4] These phenomena interact in ways that have raised significant concerns about the nature of the relationship between contemporary news and information channels, as well as the effective functioning of the democratic process.[5]

---

1. *See generally*, Mostafa M. El-Bermawy, *Your Filter Bubble Is Destroying Democracy*, WIRED (Nov. 18, 2016, 5:45 AM), [https://perma.cc/K87X-NJ59]; s*ee also* Matthew Ingram, *Facebook and the News: Trends, Filter Bubbles and Algorithmic Bias*, FORTUNE (May 12, 2016), http://fortune.com/2016/05/12/facebook-and-the-news/ [https://perma.cc/2KLF-EP6P].

2. *See, e.g.*, Olivia Solon & Sam Levin, *How Google's search algorithm spreads false information with a rightwing bias*, THE GUARDIAN (Dec. 16, 2016, 06:00 EST), https://www.theguardian.com/technology/2016/dec/16/google-autocomplete-rightwing-bias-algorithm-political-propaganda [https://perma.cc/C9BT-2WP8]; s*ee also* Daniel Trielli et al., *Googling Politics: How the Google Issue Guide on Candidates is Biased*, SLATE (June 7, 2016), http://www.slate.com/articles/technology/future_tense/2016/06/how_the_google_issue_guide_on_candidates_is_biased.html [https://perma.cc/N8DU-Y4HR]; Nelson Granados, *How Facebook Biases Your News Feed*, FORBES (June 30, 2016, 7:26 PM), https://www.forbes.com/sites/nelsongranados/2016/06/30/how-facebook-biases-your-news-feed/#799f10621d51 [https://perma.cc/73LB-CYT4]; Issie Lapowsky, *Of Course Facebook Is Biased. That's How Tech Works Today*, WIRED (May 11, 2016, 7:00 AM) https://www.wired.com/2016/05/course-facebook-biased-thats-tech-works-today/ [https://perma.cc/5AKR-63KV].

3. *See generally*, Jen Weedon et. al, FACEBOOK, INFORMATION OPERATIONS AND FACEBOOK 8 (Version 1.0, Apr. 27, 2017), https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf [https://perma.cc/63QM-SH65]; ALICE MARWICK & REBECCA LEWIS, DATA & SOC'Y, MEDIA MANIPULATION AND DISINFORMATION ONLINE 44, https://datasociety.net/pubs/oh/DataAndSocietyMediaManipulationAndDisinformationOnline.pdf [https://perma.cc/6M9Y-FLCN].

4. *See, e.g.*, Mark Isaac & Scott Shane, *Facebook's Russia-Linked Ads Came in Many Disguises*, N.Y. TIMES (Oct. 2, 2017), https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html [https://perma.cc/ZH2B-BY6E].

5. *See, e.g.*, Clive Thompson, *Social Networks Must Face Up to Their Political Impact*, WIRED (Jan, 5, 2017, 6:01 PM), https://www.wired.com/2017/01/social-networks-must-face-political-impact/ [https://perma.cc/2WZ7-4GEJ]; Alex Kantrowitz, *How The 2016 Election Blew Up in Facebook's Face*, BUZZFEED (Nov. 21, 2016, 11:15 AM), https://www.buzzfeed.com/alexkantrowitz/2016-election-blew-up-in-facebooks-face [https://perma.cc/9JKJ-5DCA]; El-Bermawy, *supra* note 1; Nathaniel Persily, *Can Democracy Survive the Internet*, 28 J. DEMOCRACY 63.

In 2013, the World Economic Forum presciently highlighted "massive digital misinformation" as a leading global risk in its annual global risk assessment.[6] In 2016, renowned fact-checking organization PolitiFact declared "fake news" its Lie of the Year.[7] Nonetheless, at least in the U.S., issues of misinformation in the digital sphere have only very recently found their way onto the communications policy agenda.[8]

This somewhat sluggish response can be explained, at least in part, by a First Amendment tradition that has valorized the notion of "counterspeech." A central tenet of the First Amendment is that more speech is an effective remedy against the dissemination and consumption of false speech.[9] The counterspeech doctrine is a perspective that was first explicitly articulated by Justice Louis Brandeis in *Whitney v. California*.[10] Since then, the effectiveness of counterspeech has become an integral component of most conceptualizations of an effectively functioning "marketplace of ideas," in which direct government regulation of speech is minimized in favor of an open and competitive speech environment.[11]

This Article seeks to unpack the set of assumptions about the dynamics of the production, dissemination, and consumption of news that are embedded in the counterspeech doctrine. This Article then questions whether these

---

6. *See* WORLD ECONOMIC FORUM, GLOBAL RISKS 2013: EIGHTH EDITION 23 (2013), http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf [https://perma.cc/9GKG-UCW3].

7. *See generally* Angie Drobnic Holan, *2016 Lie of the Year: Fake News*, POLITIFACT (Dec. 13, 2016), http://www.politifact.com/truth-o-meter/article/2016/dec/13/2016-lie-year-fake-news/ [https://perma.cc/8X2N-SHJ9].

8. *See, e.g.*, *Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions, Hearing Before the S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism*, 115th Cong. (Oct. 31, 2017), https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions [https://perma.cc/42VE-5HSD]; *Social Media Influence in the 2016 United States Elections, Hearing Before the S. Select Comm. on Intelligence* (Nov. 1, 2017), https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections [https://perma.cc/K65Y-XAQ4]; *Russia Investigative Task Force Open Hearing with Social Media Companies, Hearing before the H. Permanent Select Comm. on Intelligence* (Nov. 1, 2017), https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=814 [https://perma.cc/8DYT-QRJU].

9. S*ee* Robert D. Richards & Clay Calvert, *Counterspeech 2000: A New Look at the Old Remedy for "Bad" Speech*, 2000 B.Y.U. L. REV. 553, 553-554 (2000) ("Rather than censor allegedly harmful speech and thereby risk violating the First Amendment's protection of expression, or file a lawsuit that threatens to punish speech perceived as harmful, the preferred remedy is to add more speech to the metaphorical marketplace of ideas").

10. Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

11. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). ("[T]he ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That, at any rate, is the theory of our Constitution."); s*ee also* Alvin I. Goldman & James C. Cox, *Speech, Truth, and the Free Market for Ideas*, 2 LEGAL THEORY 1, 3 (1996); Ronald Coase, *The Market for Goods and the Market for Ideas*, 63 AM. ECON. REV. 384, 384 (1974) ("[I]n the market for goods, government regulation is desirable whereas, in the market for ideas, government regulation is undesirable and should be strictly limited.").

assumptions remain viable in the face of the evolving structure and operation of the contemporary media ecosystem: and if not, what this means for contemporary media law and policy. Specifically, this Article argues that conditions, such as the structural and economic changes that have affected the news media, increased fragmentation and personalization, and increasingly algorithmically-dictated content dissemination and consumption, affect the production and flow of news in ways that may make it more difficult than it has been in the past to assume that legitimate news will systematically win out over false news. Thus, just as it has been asked whether the assumptions underlying the Second Amendment right to bear arms (written in the era of muskets and flintlocks) are transferrable to today's technological environment of high-powered, automatic assault weapons,[12] it may be time to ask whether this fundamental aspect of First Amendment theory, crafted in an era when news circulated primarily via interpersonal contact and print media, and in which electronic media were just beginning to develop, is effectively transferrable to today's radically different media environment.

In addressing this issue, Part I will review the counterspeech doctrine, its underlying assumptions, the ways that it has been put into practice in legal and policy decision-making, and the critiques that have been leveled against it. As Part 1 will illustrate, the focal points of these critiques have been the psychological and behavioral barriers to counterspeech, as well as the resistance of certain types of speech to the effectiveness of counterspeech. Missing from the counterspeech dialogue, however, has been a substantive consideration of whether the evolution of the media ecosystem has progressed in ways that might affect the validity of the doctrine.

Part II then will provide an overview of the profound technological changes that have affected the media ecosystem and media users over the past two decades. While most of these changes are widely recognized, this section will argue that each of these developments bears directly on the integrity of the counterspeech doctrine. Specifically, this part will illustrate that technological changes have: 1) affected the relative prominence of the production of true versus false news; 2) diminished the gatekeeping barriers that have traditionally curtailed the production and dissemination of false news; 3) increased the ability of those producing false news to target those most likely to be receptive to/affected by the false news; 4) diminished news consumers' likelihood of being exposed to accurate news that counteracts false news; 5) diminished news consumers' ability to distinguish between true and false news; and 6) enhanced the speed at which false news can travel.

---

12. *See, e.g.*, Christopher Ingraham, *What 'Arms' Looked Like When the 2nd Amendment Was Written*, WASH. POST (June 13, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/06/13/the-men-who-wrote-the-2nd-amendment-would-never-recognize-an-ar-15/?utm_term=.86da76908f41 [https://perma.cc/KA8E-WV53] ("Of course, semiautomatic firearms technology didn't exist in any meaningful sense in the era of the founding fathers. They had something much different in mind when they drafted the Second Amendment. The typical firearms of the day were muskets and flintlock pistols. They could hold a single round at a time, and a skilled shooter could hope to get off three or possibly four rounds in a minute of firing. By all accounts they were not particularly accurate either.").

Each of these six conditions contributes to undermining the extent to which counterspeech can effectively operate as a fundamental assumption of First Amendment theory.

Finally, Part III will consider the broader political, legal, and policy implications of this argument. In particular, this part will consider what the diminished efficacy of counterspeech might mean for the understanding of the marketplace of ideas metaphor and the potential for failure in the marketplace of ideas. The results of the 2016 presidential election will be used to examine possible causes and indicators of such market failure. This part will conclude with a consideration of the legal and policy implications of a media ecosystem in which the counterspeech doctrine has been undermined due to technological change.

II. COUNTERSPEECH AND THE FIRST AMENDMENT: ASSUMPTIONS, APPLICATIONS, AND CRITIQUES

The counterspeech doctrine was first formally articulated by Justice Louis Brandeis in *Whitney v. California*.[13] According to Brandeis, "[i]f there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence."[14] This perspective is in many ways a natural outgrowth of the well-known "marketplace of ideas metaphor",[15] which has served as a fundamental principle in communications law and policy,[16] but has been subject to substantial critique in its own right.[17] As Justice Holmes' famous articulation of the marketplace of ideas metaphor asserts, "the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market."[18] Under this formulation, the ideas marketplace is inherently capable of distinguishing between truth and falsity and can be counted on to accept and act upon true information and reject false information. This process is, in turn, fundamental to the well-functioning democracy that, according to many interpretations, the First Amendment is intended to protect.[19] Today, Holmes'

13. *See* 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

14. *Id.*

15. *See* Daniel E. Ho & Frederick Schauer, *Testing the Marketplace of Ideas*, 90 N.Y.U. L. REV. 1160, 1167 (2015) (observing that Brandeis' opinion in *Whitney v. California* represents a "'canonical formulation' of the marketplace of ideas metaphor").

16. *See generally* PHILIP M. NAPOLI, FOUNDATIONS OF COMMUNICATIONS POLICY (2001).

17. *See, e.g.*, Darren Bush, *"The Marketplace of Ideas:" Is Judge Posner Chasing Don Quixote's Windmills?*, 32 ARIZ. ST. L.J. 1107, 1146 (2000) (arguing that, in realms such as speech, "the market metaphor becomes increasingly less applicable or useful"); Ho & Schauer, *supra* note 15; Stanley Ingber, *The Marketplace of Ideas: A Legitimizing Myth*, 1984 DUKE L.J. 1 (1984).

18. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

19. *See generally* ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE (1960); *See also* CASS SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH (1995).

statement is echoed within more contemporary notions of the "wisdom of crowds"[20] or "the wealth of networks."[21]

Counterspeech is an outgrowth of this marketplace of ideas framework. Given the metaphor's assumption that the marketplace is capable of effectively distinguishing between truth and falsity, [22] then a speech environment that facilitates as much speech as possible is a potentially effective way of assuring that truth prevails over falsity, and that the good ideas prevail over the bad ones. "More speech" (i.e., counterspeech) thus becomes an effective and First Amendment-compliant approach to assuring that individuals have the information they need to be informed and effective participants in the democratic process.

There are a number of fundamental assumptions that underlie this perspective. First, there is the assumption that individuals are capable of discerning between true and false information.[23] The logic here is that, just as participants in the traditional product market are capable of distinguishing between high and low value products, participants in the idea market are similarly capable of distinguishing between true and false news and information. A second, related, assumption is that participants in the idea marketplace place greater value on true news and information than they do on false information.[24] This assumption strikes at the core of what it is the marketplace actually values. A third assumption is that, as late U.S. Supreme Court Justice Antonin Scalia has stated, "[g]iven the premises of democracy, there is no such thing as too much speech."[25] A fourth assumption that underlies the counterspeech doctrine is that a sufficient number of those exposed to false information also will be exposed to the countervailing true information.[26] Of course, if the previous assumptions hold true, then this exposure to true and accurate information will have its desired effect in terms

---

20. *See generally* JAMES SUROWIECKI, THE WISDOM OF CROWDS XII (2004) (arguing that "under the right circumstances, groups are remarkably intelligent, and are often smarter than the smartest people in them").

21. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 4 (2006) (illustrating "the rise of effective, large-scale cooperative efforts – peer production of information, knowledge, and culture").

22. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market").

23. *See, e.g.*, Lyrissa Barnett Lidsky, *Nobody's Fools: The Rational Audience as First Amendment Ideal*, 2010 U. ILL. L. REV. 799, 801 (discussing the "rational audience" assumption in First Amendment jurisprudence: "The first of these assumptions is that audiences are capable of rationally assessing the truth, quality, and credibility of core speech").

24. *See* Goldman & Cox, *supra* note 11, at 18 ("Thus, if consumers have no very strong preference for truth as compared with other goods or dimensions of goods, then there is no reason to expect that the bundle of intellectual goods provided and "traded" in a competitive market will have maximum truth content. If people valued falsehood, then perfect competition would provide falsehood in a Pareto-optimal way.").

25. *See* McConnell v. FEC, 540 U.S. 93, 258-59 (2003) (Scalia, J., concurring in part and dissenting in part).

26. *See, e.g.*, Vincent Blasi, *Reading Holmes through the Lens of Schauer: The* Abrams *Dissent*, 72 NOTRE DAME L. REV. 1343, 1357 (1997); *see also* Richards and Calvert, *supra* note 9, at 554-55.

of contributing to an informed citizenry. Each of these are contentious assumptions in their own right.[27] However, as will be discussed below, economic and technological changes in the media ecosystem have led to conditions that further challenge many of these assumptions.

A. The Counterspeech Doctrine in Practice

Applications of the counterspeech doctrine have been wide ranging in media law and policy, as well as in industry practice.[28] Below, are a few applications that have particular relevance to the focus on the structure and operation of the contemporary media ecosystem and its relationship to a well-functioning democracy.

The well-known (some might say notorious) Fairness Doctrine is a useful case study of a rare instance in which the counterspeech doctrine has been utilized to justify government regulation.[29] The Fairness Doctrine required broadcast licensees to devote news coverage to controversial issues of public importance.[30] In providing such coverage, broadcasters were further required to devote time to competing perspectives on an issue.[31] So, for instance, if a news broadcast ran a story on new research asserting a link between cigarette smoking and cancer, the tobacco industry was entitled to demand that time be devoted to the perspective that the causal link between cigarette smoking and cancer had yet to be determined. And, importantly, this competing perspective needed to be broadcast during a day/time when a comparable number of viewers who viewed the initial broadcast could be reached.

To the extent that the Fairness Doctrine essentially compelled additional, most likely contradictory, speech, it embodies the counterspeech doctrine and its commitment to "more speech." The irony is that the Fairness Doctrine was eliminated in the late 1980s under the logic that the requirement to provide counterspeech "chilled" broadcaster coverage of controversial issues overall,[32] essentially resulting in less speech rather than more speech.

---

27. *See generally* DARREN BUSH, *supra* note 17; HO & SCHAUER, *supra* note 15; STANLEY INGBER, *supra* note 17.

28. *See* RICHARDS AND CALVERT, *supra* note 9, at 553-585.

29. For a more detailed discussion of the Fairness Doctrine and its relationship to counterspeech, *see* Adam Welle , *Campaign Counterspeech: A New Strategy to Control Sham Issue Advocacy in the Wake of FEC v. Wisconsin Right to Life*, 2008 WIS. L. REV. 795, 823-825. (2008).

30. KATHLEEN ANNE RUANE, FAIRNESS DOCTRINE: HISTORY AND CONSTITUTIONAL ISSUES 2 (2011) (noting that the Fairness Doctrine "affirmatively established the duty of broadcast licensees to cover controversial issues of public importance in a fair and balanced manner"); *See generally* Report on Editorializing by Broadcast Licensees, 13 F.C.C. 1246 (1949).

31. RUANE, *supra* note 30, at 2 ("Broadcasters . . . had the affirmative duty to determine what the appropriate opposing viewpoints were on these controversial issues, and who was best suited to present them.").

32. *See* RUANE, *supra* note 31 at 6 ("The Commission examined the effect of its enforcement of the Fairness Doctrine upon broadcasters and came to the conclusion that the doctrine chilled speech substantially").

In the case of the Fairness Doctrine, counterspeech was used to justify speech regulation. More often, it has been used to reject speech regulation. For instance, in the realm of political campaign advertising there has been a history of efforts to impose restrictions on the dissemination of false information.[33] A useful example involves efforts in the state of Washington to impose a regulation that allowed a state agency to determine the veracity of campaign statements, and to fine campaigns found to disseminate false statements.[34] These regulations were overturned by the Washington State Supreme Court for a host of reasons,[35] including a rejection of the State's contention that protecting the integrity of elections represented a sufficiently compelling government interest.[36] According to the court, prohibiting "arguably false, but nondefamatory, statements about political candidates to save our elections conflicts with fundamental principles of the First Amendment."[37] Moreover, the court explicitly argued that counterspeech represented the more appropriate mechanism for coping with falsity in political campaign communications.[38] According to the court, "[o]ur constitutional election system already contains the solution to the problem that RCW 42.17.530(1)(a) is meant to address."[39] Quoting *Brown v. Hartlage*, the court noted that "'[i]n a political campaign, a candidate's factual blunder is unlikely to escape the notice of, and correction by, the erring candidate's political opponent.[40] The preferred First Amendment remedy of 'more speech, not enforced silence,' thus has special force.'"[41] Thus, the court concluded, "[i]n other words, the best remedy for false or unpleasant speech is more speech, not less speech."[42]

What is particularly important about both of these examples is the extent to which they reflect how the First Amendment will facilitate the dissemination of false news and information. However, the importance of the circulation of diverse ideas and viewpoints is so important that such falsity must be tolerated. This tolerance is accompanied by the confidence that a robust speech environment will allow truthful and accurate news and information to triumph over falsity. This position is well-reflected in the Supreme Court's statement in *Gertz v. Robert Welch, Inc.*, that the First

33. *See* Rickert v. State Pub. Disclosure Comm'n, 168 P.3d 826, 827 n. 2-3 (Wash. 2007).

34. *Id.*

35. Reasons included the court's rejection of the notion that "the State possesses an independent right to determine truth and falsity in political debate," *id.* at 827, as well as the fact that the statute did not require proof of the defamatory nature of the speech, *id.* at 828-829.

36. *Id.* at 830-831.

37. *Id.* at 831.

38. *Id*. at 832.

39. *Id.*

40. Brown v. Hartlage, 456 U.S. 45, 61 (1982) (quoting Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

41. *See Rickert* 168 P.3d at 855.

42. *Id.* at 855-56.

Amendment requires protecting "some falsehood in order to protect speech that matters."[43]

Compared to less-protected categories of speech, such as commercial speech, the First Amendment protections for political false speech – and thus the reliance upon counterspeech – are at their most pronounced.[44] News organizations represent the most explicitly protected category of speakers (as reflected in the "of the press" clause).[45] For news organizations, since *New York Times Co. v. Sullivan*,[46] legal liability for falsity has been largely limited to intentional and malicious falsities directed at individuals or organizations that are damaging to the individual's or organization's reputation.[47] This focus is a reflection of the Supreme Court's position that "false statements of fact [can] cause damage to an individual's reputation that cannot easily be repaired by counterspeech, however persuasive or effective."[48] No such liabilities exist for the production and dissemination of journalistic falsities for the remaining political issues and concerns around which falsities could be generated, whether it be older examples, such as AIDS conspiracy theories or Holocaust denial,[49] or more recent examples, such as the nature of the scientific evidence surrounding climate change, given the broad protections given to the press and its role in maintaining "uninhibited, robust, and wide open"[50] political discussion.

Similarly, the journalistic presentation of falsities about individuals or organizations that are beneficial rather than harmful are fully protected. So while a news outlet accusing a political figure of running a child sex ring out of a Washington, DC, pizza parlor could be vulnerable to a libel lawsuit, a news outlet that knowingly reports inflated figures for a candidate's net worth or charitable donations (thereby enhancing the candidate's status with voters) is in the clear, even if it is subsequently proven that this information was published with knowledge of its falsity, since in no way was the candidate's stature or reputation damaged by the false information.

The bottom line is that "any test of truth" when applying the First Amendment to the work of journalists has been rejected.[51] According to the Supreme Court in *New York Times Co. v. Sullivan*, "[i]njury to official reputation error affords no more warrant for repressing speech that would

43. *See* 418 U.S. 323, 340-41 (1973).

44. *See* Frederick Schauer, *Facts and the First Amendment*, 57 UCLA L. REV. 897, 912-914 (2009-2010).

45. *See* Potter Stewart, *"Or of the Press"*, 26 HASTINGS L.J. 631 (1974-1975).

46. *See* 376 U.S. 254 (1964).

47. *See* generally ANTHONY LEWIS, MAKE NO LAW: THE SULLIVAN CASE AND THE FIRST AMENDMENT (1991).

48. *See* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 52 (1988).

49. *See* Schauer, *supra* note 46 at 897. For a discussion of the First Amendment protections for Holocaust deniers, *see generally* Jonathan D. Varatt, *Deception and the First Amendment: A Central, Complex, and Somewhat Curious Relationship*, 53 UCLA L. REV. 1107, n. 27-29 and accompanying text.

50. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

51. *Id.* at 271.

otherwise be free than does factual error.."[52] From this standpoint, we can assume that the prevailing First Amendment position on fake news is the production, dissemination, and consumption of more news.

Finally, it is important to note that counterspeech has become tightly integrated into the operation of the social media platforms and content aggregators that have become the eye of the storm for escalating concerns about the impact of false news on democratic decision-making. Facebook, for example, has commissioned a series of studies that highlights the prominence of counterspeech within the context of a variety of controversial issues across different countries.[53] In addition, in 2016, the company launched the Online Civil Courage Initiative, which states its mission as to "[t]o promote the civil courage displayed by organizations and grassroots activists carrying out valuable counterspeech work online." [54] Facebook's commitment to counterspeech is reflected in its description of the Online Civil Courage Initiative: "We believe that engagement is more powerful than censorship in reforming prejudiced and bigoted opinions and voices, and are committed to amplifying campaigns which encourage positive dialogue and debate."[55] In this statement, Facebook seems to suggest that the platform will work to enhance (i.e. "amplifying") counterspeech to address prejudiced and bigoted opinions and voices.

Along similar lines, Twitter has organized online convenings to facilitate discussions about strategies for producing and disseminating counterspeech through social media.[56] Google, in its 2017 testimony before the Senate Subcommittee on Crime and Terrorism about its initiatives to combat extremist content and disinformation on its platforms, highlighted that

52. *Id.* at 272.

53. *See* JAMIE BARTLETT & ALEX KRASODOMSKI-JONES, DEMOS, COUNTER-SPEECH ON FACEBOOK (2016), https://www.demos.co.uk/wp-content/uploads/2016/09/Counter-speech-on-facebook-report.pdf [https://perma.cc/YPW5-WPHN]; JAMIE BARTLETT & ALEX KRASODOMSKI-JONES, DEMOS, COUNTER-SPEECH EXAMINING CONTENT THAT CHALLENGES EXTREMISM ONLINE (2015), https://www.demos.co.uk/wp-content/uploads/2015/10/Counter-speech.pdf [https://perma.cc/BYM6-MVW7]. It is worth noting that while these studies seek to document the prevalence of counterspeech on Facebook, they do not seek to determine its effectiveness.

54. *See* ONLINE CIVIL COURAGE INITIATIVE, FACEBOOK, https://www.facebook.com/pg/OnlineCivilCourage/about/ [https://perma.cc/SW32-SF6X] (last visited June 9, 2017).

55. *Id.*

56. *See, e.g.*, @TweeSurfing, *Counter Speech On Social Media: The New Age Activism*, TWITTER, (Dec. 2, 2016), https://perma.cc/JYE7-XK9L. *See also* Colin Crowell, *Our Approach to Bots and Misinformation*, TWITTER BLOG (June 14, 2017), https://perma.cc/68UA-DSES ("Twitter's open and real-time nature is a *powerful antidote to the spreading of all types of false information.* This is important because we cannot distinguish whether every single Tweet from every person is truthful or not. We, as a company, should not be the arbiter of truth. Journalists, experts and engaged citizens Tweet side-by-side correcting and challenging public discourse in seconds. *These vital interactions happen on Twitter every day. . . .*" [emphasis in original]).

it is "creating new programs to promote counterspeech on [its] platforms."[57] These programs include efforts to redirect consumers of extremist propaganda toward content that counters those narratives, as well as efforts to encourage YouTube content creators to speak out against hate speech, xenophobia, and extremism.[58]

B. Critiques of Counterspeech

To some extent, critiques that have been directed at counterspeech overlap with those directed at the overarching marketplace of ideas metaphor within which the counterspeech doctrine is embedded. This is particularly the case for those critiques that emphasize fundamental human characteristics and tendencies that could lead to the embracing of false news and information over true news and information. In light of the concerns that have arisen in the wake of the 2016 U.S. presidential election about the potential influence of fake news,[59] there appears to be a renewed interest in the vast literatures across fields, such as communication, cognitive psychology, and behavioral economics, that highlight fundamental human tendencies that can lead to the acceptance of false information over accurate information.[60] This literature illustrates how established behavioral patterns, such as selective exposure, confirmation bias, heuristics for coping with information overload, and directionally motivated reasoning explain how false news can be favored over legitimate news.[61]

---

57. *See Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. the Judiciary*, 115th Cong. (2017) (Statement of Richard Salgado, Director, Law Enforcement and Information Security, Google).

58. *Id.*

59. *See* Weedon et al., *supra* note 3.

60. *See, e.g.*, CASS SUNSTEIN, #REPUBLIC 71-97 (2017); Elizabeth Kolbert, *Why Facts Don't Change Our Minds*, THE NEW YORKER (FEB. 27, 2017), https://perma.cc/M354-3UYN; Parmy Olson, *Why Your Brain May Be Wired to Believe Fake News*, FORBES (FEB. 1, 2017, 5:35PM), https://perma.cc/UN3J-DFAC. It is beyond the scope of this paper to review these bodies of literature. For helpful reviews, *see* Derek E. Bambauer, *Shopping Badly: Cognitive Biases, Communications, and the Fallacy of the Marketplace of Ideas*, 77 U. COL. L. REV. 649 (2006); Goldman & Cox, *supra* note 11; Ho & Schauer, *supra* note 15.

61. *See, e.g.*, R. Kelly Garrett & Natalie Jomini Stroud, *Partisan Paths to Exposure Diversity: Differences in Pro- and Counterattitudinal News Consumption*, 64 J. COMM. 680, 693-94 (2014); Michael A. Beam, *Automating the News: How Personalized News Recommender System Design Choices Impact News Reception*, 41 COMM. RES. 1019, 1020-36 (2014); D.J. Flynn, Brendan Nyhan & Jason Reifler, *The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics*, 38 ADVANCES POL. PSYCHOL. 127,128-32 (2017). For a more detailed discussion of the range of cognitive biases that can come into play *see* Bambauer, *supra* note 60 at 673-96. *See also* Alessandro Bessi et. al., *Homophily and Polarization in the Age of Misinformation*, 225 EUR. PHYS. J. SPECIAL TOPICS 2047 (2016) (discussing research showing a correlation between polarized social networks and participation in the consumption and spread of false news and information).

These are long-standing behavioral and psychological patterns.[62] As Frederick Schauer has noted, "[t]hat people believe things that are false comes as no surprise. That a large number of people believe things that are false despite being told the truth is also hardly a revelation."[63] The bottom line is that the notion of the "rational audience," capable of processing speech from diverse sources, and capable of effectively and rationally assessing the truth, quality, and credibility, is much more an ideal-type in First Amendment theory than an empirical reality.[64] What may be different today, however is the extent to which the U.S. media system is capable of counteracting these fundamental human tendencies. Instead, it may be exacerbating them.[65]

Other critiques have explored specific speech contexts, where it has been argued that the counterspeech doctrine is particularly ineffective. It has frequently been noted that the efficacy of counterspeech can depend upon a wide range of circumstances related to the character of the speech at issue.[66] Hate speech, for instance, has been singled out as being particularly resistant to the effects of counterspeech.[67] Hate speech may have a silencing effect on would-be speakers, inhibiting their ability to engage in counterspeech or it may impose unfair or dangerous burdens on those who engage in counterspeech.[68] Further, marginalized groups that often are the targets of hate speech may lack the access and resources to effectively reach all of those exposed to the initial speech.[69]

The counterspeech doctrine is a pillar of First Amendment theory that rests on an intellectual foundation that is somewhat shaky, at best. The critiques of counterspeech have focused on either the aspects of human psychology that work against counterspeech being consumed and/or having its intended effects, or on those types of speech that the mechanisms of counterspeech are less likely to affect.[70]

Largely absent from these critiques of the counterspeech doctrine are detailed considerations of how technological and structural changes in the media and information environment may impact the extent to which we can

62. *See, e.g.*, Schauer, *supra* note 44, at 899.

63. *See* Schauer, *supra* note 44, at 898.

64. *See generally* Lidsky, *supra* note 23.

65. *See infra* notes 76-180 and accompanying text.

66. *See, e.g.*, Blasi, *supra* note 26, at 1357; *see also* Richards and Calvert, *supra* note 9, at 554-55.

67. *See* Richard Delgado & David Yun, *"The Speech We Hate": First Amendment Totalism, the ACLU, and the Principle of Dialogic Politics*, 27 ARIZ. ST. L.J. 1281, 1292 (1995).

68. *See, e.g.*, OWEN M. FISS, THE IRONY OF FREE SPEECH 25-6 (1996).

69. *See* Mari J. Matsuda, *Public Response to Racist Speech: Considering the Victim's Story*, *in* MARI J. MATSUDA ET AL , WORDS THAT WOUND: CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT 17, 48 (1993) (arguing that minority groups have "diminished access to private remedies such as effective counterspeech").

70. *See* Schauer, *supra* note 46, at 912-914; *see generally* Mari J. Matsuda, *Public Response to Racist Speech: Considering the Victim's Story*, *in* WORDS THAT WOUND: CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT 17, 48 (1993).

expect factual speech to overcome false speech.[71] How might these technological changes affect the integrity of the counterspeech doctrine? This question is the focus of the next section, which argues that the media ecosystem has evolved in ways that undermine the likelihood (however slim it already may have been)[72] that true and high-quality news and information will overcome false and low-quality news information. In this regard, the arguments presented here can be layered upon the established critiques discussed above, thereby further calling into question the validity of the notion of more speech serving as an effective antidote to false speech.

III. HOW TECHNOLOGICAL CHANGES UNDERMINE THE COUNTERSPEECH DOCTRINE

The goal of this section is to consider the range of changes affecting the contemporary media ecosystem through the lens of counterspeech, with a particular focus on contemporary concerns about the prominence of fake news and the operation of filter bubbles. That is, how do these changes potentially affect the production, distribution, and consumption of legitimate versus false news and information?

A. The Relative Prominence of True Versus False News[73]

In considering the changes that have affected the media ecosystem over the past two decades, it makes sense to begin with the changing dynamics of news production. The technological and economic changes that have transformed the media ecosystems have had a number of intersecting effects that have, on the one hand, undermined the production of legitimate news, while at the same time enhanced the production of false news.

---

71. For instance, *see* Schauer 's *supra* note 46 at 899, wherein Schauer recognizes t the apparent "increasing and unfortunate acceptance of factual falsity in public communication", but doesn't explore how the evolution of the media sector might be contributing to this increase.

72. *See supra*, notes 62-72 and accompanying text.

73. It should be noted that this analysis starts from the premise that it is possible to make valid distinctions between "legitimate" and "fake" news. Certainly, as with all dimensions of speech classification (*e.g.*, commercial vs. non-commercial speech, libelous vs. non-libelous speech), there will be areas of ambiguity and disagreement, but such ambiguity and disagreement does not invalidate the viability, legitimacy or importance of maintaining the distinction. *See* James Weinstein, *Speech Characterization and the Limits of First Amendment Formalism: Lessons from Nike v. Kasky*, 54 CASE WESTERN RESERVE L. REV. 1091, 1093 (2004) ("In a typical free speech case, . . . use of verbal formulae or case matching to determine the category in which to place the speech in question works well enough. There is often precedent so factually similar that it really is controlling; or even in the absence of such truly controlling precedent, categorizing the speech in question one way rather than the other so clearly promotes the values underlying free speech doctrine that a judge can intuitively make the right choice"). Not surprisingly, efforts to clarify the concept of fake news or to develop more precise terminology, are ongoing; *see, e.g.*, Claire Wardle & Hossein Derakhshan, INFORMATION DISORDER 4 (2017) (developing the concept of "information pollution" as an alternative to "fake news").

In terms of the production of legitimate news, the ongoing economic crisis in journalism has been well documented.[74] Key consequences of this crisis include: declines in the number of newspapers across the country, in the size of television newsrooms, and in the number of professional journalism positions.[75] The rise of various online news outlets, and the new opportunities technological change fostered for "citizen journalism," have been interpreted by some as adequate countervailing forces in the wake of declines in traditional journalism; however, the reality is that these developments have not been able to fully replace the declines in news workers or news reporting that have resulted from the declines affecting traditional media.[76] The troubling paradox here is that increases in the number of media outlets and channels have led to decreases in the production of genuine journalism.

While it is difficult to reconcile this position with the apparent abundance of online news, it is more understandable if we consider a seldom discussed, and insufficiently researched, phenomenon in the realm of digital journalism: what is perhaps best described as parasitic journalism.[77] Parasitic journalism refers to news stories that have as their origins and foundation reporting produced by another media outlet.[78] If one examines news stories produced by digital media outlets through this analytic lens, the proportion of the online news reporting that merits classification as original journalism declines dramatically. Indeed, this kind of parasitic journalism (or "vampire web pages," as they are sometimes called) has emerged as a thriving business model, due in large part to the extent to which social media platforms facilitate

---

74. *See, e.g.*, Leonard Downie, Jr., & Michael Schudson, *The Reconstruction of American Journalism*, COLUM. J. REV. 1 (Nov./Dec. 2009), http://archives.cjr.org/reconstruction/the_reconstruction_of_american.php [https://perma.cc/8MQJ-GQB8] ("As almost everyone knows, the economic foundation of the nation's newspapers, long supported by advertising, is collapsing, and newspapers themselves, which have been the country's chief source of independent reporting, are shrinking—literally. Fewer journalists are reporting less news in fewer pages, and the hegemony that near-monopoly metropolitan newspapers enjoyed during the last third of the twentieth century, even as their primary audience eroded, is ending. Commercial television news, which was long the chief rival of printed newspapers, has also been losing its audience, its advertising revenue, and its reporting resources"),; C.W. Anderson et al., *Post-Industrial Journalism: Adapting to the Present* 2 (Colum. J. School / Tow Ctr. for Digital Journalism Rep.) http://towcenter.org/wp-content/uploads/2012/11/TOWCenter-Post_Industrial_Journalism.pdf [https://perma.cc/UV9D-HPS8]. ("The effect of the current changes in the news ecosystem has already been a reduction in the quality of news in the United States").

75. *See* BUR. LAB. STAT., NEWSPAPER PUBLISHERS LOSE OVER HALF THEIR EMPLOYMENT FROM JANUARY 2001 TO SEPTEMBER 2016 (Apr. 3, 2017), https://www.bls.gov/opub/ted/2017/mobile/newspaper-publishers-lose-over-half-their-employment-from-january-2001-to-september-2016.htm; https://perma.cc/A4VT-22NH.

76. *See* PEW RES. CTR., STATE OF THE NEWS MEDIA 2016 (June, 2016), http://www.journalism.org/2016/06/15/state-of-the-news-media-2016/., [https://perma.cc/2LAM-E72U].

77. *See generally The Future of Newspapers*, THE INDEP. (Nov. 13, 2006), http://www.independent.co.uk/news/media/the-future-of-newspapers-5331270.html [https://perma.cc/8CWU-LKWM].

78. *Id*. ("Although there's an enormous amount of online news-related material, if you analyse it, very, very little is actually new fact, new information - it's almost all parasitic journalism carried out either by broadcasters or newspapers.").

the ability to identify popular news stories, and then recycle and recirculate nearly identical versions of those stories that demonstrably drain the audience (and thus, revenue) away from the outlets that produced the original story.[79]

Ultimately, the apparent multitude of online news outlets masks a journalistic ecosystem in which original reporting is recycled and circulated by scores of under-resourced news outlets incapable in engaging in original reporting.[80] In many ways, this may be the true online echo chamber – the process by which the same reporting reverberates through outlet after outlet, often reconfigured and re-summarized in ways that sometimes seek to disguise the story's true origins and that provide opportunities for original commentary – but not original reporting. The end result is that the bulk of the news produced continues to originate from a relatively small number of media outlets, each of whose economic capacity to produce news is in a continued state of decline.[81]

The bottom line is that original reporting is costly to produce and, given the degrading economics of journalism, this production is in decline. Fake news, on the other hand, is far less costly to produce.[82] Fabricated news stories do not require the same rigorous research, verification processes, or trained professionals to produce. This is why fake news has a fairly extensive history – one that certainly predates the Internet and social media[83] – with changes in communications technologies consistently affecting the dynamics of how fake news is produced, disseminated, and consumed.[84] Today, fake news can be easily and effectively produced (and monetized) by a "Macedonian" teenager in his bedroom.[85] From this standpoint, the evolution of the media ecosystem has done nothing to make the production of false news and

---

79. *See* Steven Rosenfeld & Ivy Olesen, *Vampire Webpages Suck Content from Legitimate Progressive News Sites*, ALTERNET (Mar. 6, 2017), http://www.alternet.org/media/vampire-webpages-suck-content-legitimate-progressive-news-sites [https://perma.cc/Y6BX-WF3N].

80. Even producers of fake news engage in rampant cannibalization of other fake news producers. *See* Craig Silverman & Lawrence Alexander, *How Teens in The Balkans Are Duping Trump Supporters with Fake News*, BUZZFEED.COM (Nov. 3, 2016), https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.jgOP8e208#.mc5dvo9bv [https://perma.cc/YCH9-8NN4] ("Most of the posts on these sites are aggregated, or completely plagiarized, from fringe and right-wing sites in the US").

81. *See supra* notes 76-82 and accompanying text.

82. *See generally*, Jamie Condliffe, *Fake News is Unbelievably Cheap to Produce*, MIT TECH. R. (June 14, 2017), https://www.technologyreview.com/s/608105/fake-news-is-unbelievably-cheap/.

83. *See, e.g.*, David Uberti, *The Real History of Fake News*, COLUM. J. REV. (Dec., 15, 2016), http://www.cjr.org/special_report/fake_news_history.php [https://perma.cc/K5FH-Z9C8].

84. *See* Jacob Soll, *The Long and Brutal History of Fake News*, POLITICO (Dec. 18, 2016), http://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535 [https://perma.cc/ZRR6-ZY35] (discussing impact of the printing press on production, dissemination, and consumption of fake news).

85. *See* Samantha Subramanian, *Inside the Macedonian Fake-News Complex*, WIRED (Feb. 15, 2017), https://www.wired.com/2017/02/veles-macedonia-fake-news/ [https://perma.cc/AG3C-7D6Z]; Silverman & Alexander, *supra* note 80.

information more economically challenging in the way that it has for legitimate news. On the contrary, the economics of false news have been enhanced as a result of the changes in systems of news distribution.[86] Thus, from the standpoint of the counterspeech doctrine, the relative production of legitimate news and information compared to false news and information is in the midst of perhaps an unprecedented decline.

B. Diminished Gatekeeping and Distribution Barriers

The shift in the relative prominence of legitimate versus false news is a function of the fact that the gatekeeping barriers that have traditionally curtailed the dissemination of false news relative to legitimate news have been dramatically reduced. The notion of gatekeeping barriers refers to the decision-making mechanisms controlling the type of news to which consumers have access..[87] The mass media era was defined by gatekeeping bottlenecks, in which freedom of the press was "guaranteed only to those that own one."[88] Effective distribution was confined to outlets, such as broadcast stations, cable networks/systems, newspapers, and magazines, all of which were relatively scarce for technological and economic reasons, and thus operated as news and information bottlenecks that wielded substantial gatekeeping power.[89]

The Internet has provided the opportunity to circumvent these bottlenecks. As a consequence, the economic incentives for producing legitimate journalism have been undermined, even as, the opportunities to distribute news have increased, and the costs of distribution have decreased.[90] Conversely, given the low costs associated with producing fake news, the diminished gatekeeping barriers and minimal distribution costs have enhanced the economic incentives for producing fake news.[91] The size of the potential market is, simply, larger.[92]

Even the gatekeeping to advertising dollars has been transformed in ways that enhance the opportunities for fake news outlets. Today, the allocation of online advertising dollars is increasingly handled by algorithmically-driven ad placement networks, given the overwhelming

86. *See infra* notes 92-102 and accompanying text.

87. *See generally* Pamela Shoemaker and Timothy Vos, GATEKEEPING THEORY (2009).

88. *See* A.J. Liebling, *The Wayward Press: Do You Belong in Journalism?* NEW YORKER, (May 14, 1960), at 109.

89. *See* Jonathan Taplin, *The IP TV Revolution*, in THE NETWORK SOCIETY 241 (2005) (describing the "critical transition from a media world of analog scarcity to . . . digital abundance where any maker of content (films, music, video games) could have access to the world's audience through a server based on demand media environment").

90. *See supra* notes 78-83 and accompanying text.

91. *See* Abby Ohlheiser, *This is How Internet's Fake News Writers Make Money*, WASH. POST (Nov. 18, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/?utm_term=.7c4ee4d7e8d6 [https://perma.cc/V5S9-LBJS].

92. *Id.*

number of ad placement options.[93] Often, online advertisers do not even know exactly where their advertisements are being placed.[94] This is in stark contrast to the mass media era, when information about when and where advertisements were being placed was common knowledge.[95] The end result is that, on the basis of the criteria embedded in the ad-placement algorithms, fake news sites have been on more or less equal footing with other online content providers. Even recent, initial efforts to ban known fake news outlets from major ad networks (a response to the post-2106 fake news revelations) appear to have – at least initially – proven not entirely effective.[96]

Previously, the distribution and monetization of fake news would be prevented to some extent via the limited number of gatekeepers.[97] Given their limited number, these gatekeepers had both the incentive and the opportunity to curb the dissemination of fake news. The incentive came from the fact that, in a far less fragmented media environment, neutral and objective (and thus less likely to be false) reporting represented an effective approach to attracting and retaining the largest possible audience.[98] The opportunity came in the form of the substantial economic resources these outlets had to research and verify stories – resources that were a function of the economic health of these

93. *See* Robert Thomson, *News Corp. CEO on Fake News, 'Digital Duopoly' and What Role Advertising Plays in All of It*, MEDIASHIFT (Apr. 3, 2017), http://mediashift.org/2017/04/news-corp-ceo-fake-news-digital-duopoly-role-advertising-plays/ [https://perma.cc/P382-B8VV].

94. David Iaconangelo, *Why Didn't These Companies Know They Were Advertising on Breitbart?* CHRISTIAN SCIENCE MONITOR (2016, Nov. 30), https://www.csmonitor.com/Business/2016/1130/Why-didn-t-these-companies-know-they-were-advertising-on-Breitbart ("The fact that many of the companies apparently didn't know that their ads were appearing [on Breitbart] seems to highlight how new ad technologies have loosened companies' grip over their brand's associations").

95. *Id.* (noting that it has become "a lot easier for buyers to lose a degree of control over where their ads run").

96. *See* Craig Silverman et al., *In Spite of the Crackdown, Fake News Publishers Are Still Earning Money from Major Ad Networks*, BUZZFEED (Apr. 4, 2017), https://www.buzzfeed.com/craigsilverman/fake-news-real-ads [https://perma.cc/62GN-L72N].

97. *See* A.J. Liebling, *The Wayward Press: Do You Belong in Journalism?* NEW YORKER, May 14, 1960, at 105.

98. *See, e.g.*, JAMES T. HAMILTON, ALL THE NEWS THAT'S FIT TO SELL: HOW THE MARKET TRANSFORMS INFORMATION INTO NEWS 38 (2004) ("The evidence in this chapter demonstrates that independent news coverage grew as scale economies became more important"); *see also* GERALD J. BALDASTY, THE COMMERCIALIZATION OF NEWS IN THE NINETEENTH CENTURY 28 (1992). It should be noted that some researchers have questioned whether the development of the norm of objectivity is tied to the commercialization of the press. *See, e.g.*, Michael Schudson, *The Objectivity Norm in American Journalism*, 2 JOURNALISM 149, 160 (2001) ("The notion that the move from partisanship to objectivity was economically motivated is widely believed but nowhere justified.").

outlets prior to the damaging effects of an increasingly fragmented media environment.[99]

This scenario of diminished bottlenecks and gatekeepers represents a tremendous opportunity for the production and dissemination of fake news. As has been well-illustrated in the months since the 2016 U.S. presidential election, many of those engaged in the production and distribution of fake news did so purely because of the tremendous economic opportunity it presented, not out of any ideological motivations.[100] Economic incentives to provide false news have always existed, given the appealing economics of false news production discussed above.[101] The key point here is that the diminished barriers to entry (and thus diminished institutional gatekeeping) afforded by the Internet enhanced these incentives.

These economic incentives have been further enhanced over the past few years by social media distribution.[102] Social media provides a means to more effectively capitalize on the diminished gatekeeping barriers facilitated by the Internet by providing previously unprecedented paths to low-cost distribution and large aggregations of audiences. Research indicates that social media referrals are a more crucial component of story distribution for hyper-partisan and fake news sites than they are for legitimate news sites.[103] Another recent study found that, in the days before the 2016 election, many Twitter users received a higher volume of misinformation and conspiratorial content than professionally produced news.[104]

---

99. *See, e.g.*, Leonard Downie, Jr., & Michael Schudson, *The Reconstruction of American Journalism*, COLUM. J. REV. 1 (Nov./Dec. 2009), http://archives.cjr.org/reconstruction/the_reconstruction_of_american.php [https://perma.cc/XD6D-DBLM] ("Commercial television news, which was long the chief rival of printed newspapers, has also been losing its audience, its advertising revenue, and its reporting resources.").

100. *See, e.g.*, Subramanian, *supra* note 85 ("These Macedonians on Facebook didn't care if Trump won or lost the White House. They only wanted pocket money to pay for things—a car, watches, better cell phones, more drinks at the bar."). As Adam Mosseri, Facebook's Vice President of News, has stated, "We've found that a lot of fake news is financially motivated." Adam Mosseri, *News Feed FYI: Addressing Hoaxes and Fake News*, FACEBOOK (Dec. 15, 2016), https://newsroom.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/ [https://perma.cc/GT4S-X4QH]; Silverman & Alexander, *supra* note 82 ("Their reasons for launching these sites are purely financial, according to the Macedonians with whom BuzzFeed News spoke").

101. *See supra* notes 84-88 and accompanying text.

102. *See generally* Timothy B. Lee, *Facebook's Fake News Problem, Explained*, VOX (Nov. 16, 2016), http://www.vox.com/new-money/2016/11/16/13637310/facebook-fake-news-explained [https://perma.cc/JV55-2MZP]

103. *See* Alexios Mantzarlis, *Facebook Referrals are Crucial for Traffic to Hyperpartisan and Fake News Sites*, POYNTER (Nov. 28, 2016), https://www.poynter.org/2016/facebook-referrals-are-crucial-for-traffic-to-hyperpartisan-and-fake-news-sites/440132/ [https://perma.cc/KT3K-YBAP].

104. *See* Philip N. Howard et al., *Social Media, News and Political Information During the U.S. Election: Was Polarizing Content Concentrated in Swing States?* COMPROP DATA MEMO (Sept. 27, 2017); http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/09/Polarizing-Content-and-Swing-States.pdf [https://perma.cc/53VP-PBY2], at 1 (finding that "nationally, Twitter users got more misinformation, polarizing and conspiratorial content than professionally produced news").

It is important to emphasize that these social media platforms, like their mass media predecessors, also represent bottlenecks with substantial gatekeeping capacity.[105] The reality however, has been that, likely due to a combination of factors (scale, technological limitations, economic incentives, organizational philosophy, ignorance), this gatekeeping authority has not been rigorously deployed to combat the dissemination of fake news.

It is important to recognize that underlying this argument is the assumption that, regardless of the motivation, sources of news and information with more partisan orientations produce more false news than journalistic sources that adhere to more traditional notions of neutrality and objectivity. While perhaps controversial, this assumption is grounded in compelling empirical evidence.[106]

In sum, within the counterspeech doctrine's valorization of "more speech," the point here is that, in today's news ecosystem, more of this "more speech" is likely to be false speech.

C. Increased Ability to Target the Most Impressionable

Within the context of the distribution of news, it is also important to take into consideration the ways in which the distribution of false news can now be more effectively targeted at those individuals most likely to be affected by the misinformation.

Nicholas Negroponte's famous speculation about the inevitability (and desirability) of *The Daily Me* provides a useful starting point for the rise of personalization in digital media.[107] Personalization is a data driven phenomenon, facilitated by the information backchannels that are inherent in interactive media.[108] As Negroponte predicted, interactive media have allowed people to craft their own individual news diets. Negroponte's somewhat utopian perspective has since been tempered by concerns about the

105. *See* Emily Bell, *Facebook is Eating the World*, COL. J. REV. (Mar. 7, 2016) ("The largest of the platform and social media companies, Google, Apple, Facebook, Amazon, and even second order companies such as Twitter, Snapchat and emerging messaging app companies, have become extremely powerful in terms of controlling who publishes what to whom. . . . There is a far greater concentration of power in this respect than there ever has been in the past").

106. *See, e.g.*, Kate Starbird, Examining the Alternative Media Ecosystem Through the Production of Alternative Narratives of Mass Shooting Events on Twitter (2017) (unpublished manuscript), http://faculty.washington.edu/kstarbi/Alt_Narratives_ICWSM17-CameraReady.pdf [https://perma.cc/HS9M-8VF7]. The author notes that, "[n]ot surprisingly, we found the conversation around alternative narratives of mass shooting events to be largely fueled by content on alternative (as opposed to mainstream) media." *Id.* at 9.

107. *See* NICHOLAS NEGROPONTE, BEING DIGITAL 153 (1996).

108. *See generally*, Mary Collins, *Personalized Media: It's All About the Data*, TVNEWSCHECK (2017, Sept. 8), http://www.tvnewscheck.com/article/107097/personalized-media-its-all-about-the-data.

political and cultural detriments of residing in such filter bubbles.[109] Nonetheless, personalization continues to work its way through the news ecosystem, with even the *New York Times* recently launching an initiative to bring more data-driven personalization to the process of presenting stories to online news consumers.[110] The key point here is that interactivity provides a stream of audience data that facilitates audience targeting and personalization to an unprecedented extent.

Within the context of counterspeech, this means that those with an economic and/or political interest in the dissemination of false news are now far better equipped than in the past to deliver their content to those they most desire to reach. Targeting exclusively right- or left-leaning news consumers (or other, more specific political traits) with false news or information has never been easier, as observable social media activity provides a host of reliable indicators of an individual's political orientation.[111] In these ways, the magnitude of the "evil" (to use Brandeis' term)[112] that false speech can achieve is amplified.

In the wake of the 2016 election, it was reported that Donald Trump's campaign employed a consulting firm, Cambridge Analytica, which drew upon massive amounts of social media data to construct detailed psychological, demographic, and geographic profiles of individual voters. These data were then utilized by the Trump campaign to deliver micro-targeted political messages through social media platforms such as

---

109. *See, e.g.*, Eli Pariser, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011); SUNSTEIN, *supra* note 62 at 2 ("In the 1990s, the idea of a Daily Me seemed more than a little absurd. But it's looking astoundingly good. If anything, Negroponte understated what was coming, what has now arrived, and what is on the horizon. Is that a promise or a threat? I think it's both – and that the threatening part is what needs to be emphasized, not least because so many people see it as pure promise"); Jon Keegan, *Blue Feed, Red Feed: See Liberal Facebook and Conservative Facebook, Side by Side*, WALL ST. J. (May 18, 2016), http://graphics.wsj.com/blue-feed-red-feed/ [https://perma.cc/8SPX-SBGA]. For empirical evidence of filter bubbles, *see* Tien T. Nguyen et. al., *Exploring the Filter Bubble: The Effect of Using Recommender Systems on Content Diversity*, *in* WWW '14 *IN* PROCEEDINGS OF THE 23RD INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 677 (Apr. 2014); http://dl.acm.org/citation.cfm?doid=2566486.2568012 [https://perma.cc/TH9X-KW9F]; Alessandro Bessi et al., *Users Polarization on Facebook and YouTube*, PLOS ONE (Aug. 23, 2016), https://doi.org/10.1371/journal.pone.0159641 [https://perma.cc/NA5D-SG4P]; Walter Quattrociocchi et al., Echo Chambers on Facebook (2016, June 13) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110 [https://perma.cc/PA95-WDGD].

110. *See* Ricardo Bilton, *All the News That's Fit for You: The New York Times is Experimenting with Personalization to Find New Ways to Expose Readers to Stories*, NIEMAN LAB (Sept.28, 2017), http://www.niemanlab.org/2017/09/all-the-news-thats-fit-for-you-the-new-york-times-is-experimenting-with-personalization-to-find-new-ways-to-expose-readers-to-stories/[https://perma.cc/QJ8T-XZ8P].

111. *See* Elanor Colleoni et al., *Echo Chamber or Public Sphere? Predicting Political Orientation and Measuring Political Homophily in Twitter Using Big Data*, 64 J. OF COMMUNICATION 317, 321 (2014) ("By classifying all the content posted according to its political orientation we are able to identify the general political orientation of the users and measure levels of political homophily in their network").

112. *See* Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

Facebook.[113] Hundreds of Russian-operated Facebook accounts also have been found to have been engaging in such election-related micro-targeted advertising.[114] Congressional investigators are currently evaluating the content of these ads, so there is no clear sense yet of the extent to which false news or claims were delivered in these messages.[115] However, the point here is that the technological capacity to target citizens with tailored messages or false news stories based on their characteristics appears to have taken yet another substantial leap forward, beyond what was possible through previous communications channels.[116]

From a false news perspective, according to a U.S. Senate investigation, the Russians working to spread fake news stories specifically targeted voters in swing states such as Wisconsin, Michigan, and Pennsylvania,[117] with this geographic targeting facilitated by social media data. Further, according to the testimony of cybersecurity expert Clint Watts, some of these fake news outlets explicitly targeted Donald Trump, tweeting fake news stories directly to his Twitter account during time periods when he was known to be online, under the presumption that he has shown himself to be particularly susceptible

---

113. *See* Issie Lapowsky, *What Did Cambridge Analytica Really do for the Trump Campaign?* WIRED (Oct. 26, 2017), https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/ [https://perma.cc/72E7-8WLL]. For methodological details, *see generally* Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, with Days to Go*, BLOOMBERG BUSINESSWEEK, https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go [https://perma.cc/79L3-MVJV].

114. *See* Alex Stamos, *An Update on Information Operations on Facebook*, FACEBOOK (Sept/ 6, 2017), https://newsroom.fb.com/news/2017/09/information-operations-update/ [https://perma.cc/A5RY-Z7F5].

115. *See* Craig Timberg et al., *Facebook to Turn Over Thousands of Russian Ads to Congress, Reversing Decision*, WASH. POST (Sept. 21, 2017), https://www.washingtonpost.com/business/technology/facebook-to-turn-over-thousands-of-russian-ads-to-congress-reversing-decision/2017/09/21/9790b242-9f00-11e7-9083-fbfddf6804c2_story.html?utm_term=.0d6c72e30048 [https://perma.cc/RJ5A-TM6H].

116. *See* Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance, and Computational Politics*, 19 FIRST MONDAY, http://firstmonday.org/article/view/4901/4097 [https://perma.cc/3LWW-AWMC] ("While computational politics in its current form includes novel applications, the historical trends discussed in this paper predate the spread of the Internet. In fact, there was already a significant effort underway to use big data for purposes of marketing, and the progression of using marketing techniques for politics — and "selling of the President" — clearly reflects longer–term trends. However, computational politics introduces significant qualitative differences to that long march of historical trends. Unlike previous data collection efforts (for example, collating magazine subscriptions or car type purchases) which required complicated, roundabout inferences about their meaning (does a magazine subscription truly signal a voter preference?) and allowed only broad profiling in the aggregate, this data provides significantly more individualized profiling and modeling, much greater data depth, and can be collected in an invisible, latent manner and delivered individually[.]").

117. *See* Rachel Roberts, *Russia Hired 1,000 People to Create Anti-Clinton Fake News in Key U.S. States During Election, Trump-Russia Hearings Leader Reveals*, THE INDEP. (Mar. 30, 2017) (According to Senator Mark Warner, "[i]t's been reported to me, and we've got to find this out, whether they were able to affect specific areas in Wisconsin, Michigan, Pennsylvania [.]"). For further evidence of the targeting of fake news to swing state social media users, *see* Howard et al., *supra* note 104.

to fake news.[118] This is an extreme example of today's highly personalized media environment enhancing the opportunities for purveyors of fake news to reach those both most likely and most important to be affected by the misinformation.

One could certainly argue that these dynamics provide comparable opportunities for true and accurate news to target those news consumers most in need of being reached, or most vulnerable to fake news. The problem with this logic becomes clearer when factoring in the ways in which this process of personalization undermines the likelihood of exposure to counterspeech that directly addresses the false speech that has been consumed.[119]

D. The Diminished Likelihood of Being Exposed to Factual Counterspeech

As Vincent Blasi has emphasized, one of the key conditions impacting the effectiveness of counterspeech is the extent to which "the counter-message comes to the attention of all the persons who were swayed by the original idea."[120] The dynamics of the contemporary media environment to some extent serve to explicitly prevent this type of exposure to counterspeech from taking place. This is the essence of the filter bubble phenomenon, in which the intertwining of individual and algorithmic content personalization[121] on social media and other news aggregation platforms works to deflect news sources and content that do not correspond to the user's established content preferences and political orientation.[122] Certainly, this

---

118. *See* MEDIA MATTERS FOR AMERICA, *CNN: Fake News Trolls Pushing Conspiracy Theories "Tweet Right at President Trump" Hoping that "He Cites it Publicly* (Mar. 30, 2017) https://www.mediamatters.org/video/2017/03/30/cnn-fake-news-trolls-pushing-conspiracy-theories-tweet-right-president-trump-hoping-he-cites-it/215878 [https://perma.cc/35GH-43VN]("WOLF BLITZER (HOST): Do these fake news trolls sometimes actually target President Trump himself? BRIAN TODD: According to the cybersecurity expert Clint Watts who you had on earlier, Wolf, they do, in fact, do that. Watts testified today that some outlets pushing fake or misleading stories will tweet right at President Trump during high volume periods when they know he's online. They're pushing conspiracy theories hoping that he clicks on one and cites one publicly.").

119. *See infra* notes 122-136 and accompanying text.

120. *See* Blasi, *supra* note 26, at 1357.

121. *See* Eytan Bakshy et al., *Exposure to Ideologically Diverse News and Opinion on Facebook*, 348 SCIENCE 1130, 1130 (June 5, 2015) ("The media that individuals consume on Facebook depends not only on what their friends share but also on how the News Feed ranking algorithm sorts these articles and what individuals choose to read."); Philip M. Napoli, *Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers*, 39 TELECOM. POL'Y 751 (Oct. 2015).

122. *See* Sunstein, *supra* note 60; Seth R. Flaxman et al., Ideological Segregation and the Effects of Social Media on News Consumption, at 1 (May 2014) (unpublished manuscript), https://bfi.uchicago.edu/sites/default/files/research/flaxman_goel_rao_onlinenews.pdf (finding that "recent technological changes do increase ideological segregation"). For critiques of the filter bubble logic and some contrary empirical findings, *see* Mark S. Nadel, *Customized News Service and Extremist Enclaves in Republic.com*, 54 STANFORD L. REV. 831 (2002); Jacob L. Nelson, *Is Fake News a Fake Problem?* COLUMBIA J. REV. (January 31, 2017), https://www.cjr.org/analysis/fake-news-facebook-audience-drudge-breitbart-study.php.

process of deflection works both ways. That is, one's filter bubble might deflect fake news that contradicts previously-consumed legitimate news. Or, it might deflect legitimate news that contradicts previously-consumed false news.

But here again is where the extent to which the filter bubbles have a partisan orientation comes into play. Given the empirical connection between partisanship and falsity,[123] to the extent one's filter bubble has a partisan orientation, the likelihood of fake news making it through the filter bubble increases.[124] At the same time, the likelihood of legitimate news that counteracts that fake news decreases.[125] The current state of play is perhaps best termed the "Spiral of Partisanship."[126] In this scenario, the increased media fragmentation and personalization that began in the 1980s with the development of cable television; then accelerated through the 90s and 2000s with the rise of the Internet and social media, simultaneously facilitates the mutually dependent phenomena of the rise of more partisan news outlets and the selective exposure to more partisan news. These are mutually dependent phenomena in that partisan news outlets require an audience to justify their existence and more partisan news consumption requires the availability of more partisan news outlets.

And so, as the media environment grows more fragmented, its ability to both sow and satisfy increasing partisanship is amplified.[127] It is likely no coincidence that the upswing in self-reported partisanship begins in the 1980s, at the same time that media fragmentation begins in earnest, primarily through

123. *See* Starbird, *supra* note 106.

124. *See, e.g.*, Delia Mocanu et al., *Collective Attention in the Age of (Mis)information*, 51 COMP. IN HUM. BEHAV. 1198, 1202 (2015) (finding that "users with strong preferences for alternative information sources . . . are more susceptible to false information"); Alessandro Bessi et al., *Science vs Conspiracy: Collective Narratives in the Age of Misinformation*, PLOS ONE at 1 (finding that "polarized communities emerge around distinct types of contents and usual consumers of conspiracy news result to be more focused and self-contained on their specific contents").

125. *See* Quattrociocchi et al., *supra* note 109.

126. This term is used in reference to the well-known Spiral of Silence, which has posited that individuals who perceive their opinion to be in the minority will choose not to express that opinion, thus feeding into a downward spiral that systematically silences more and more of those holding that minority opinion, thereby creating a false impression of a widely-shared majority opinion. *See* ELIZABETH NOELLE NEUMAN, THE SPIRAL OF SILENCE: PUBLIC OPINION – OUR SOCIAL SKIN (1994).

127. *See* JONATHAN M. LADD, WHY AMERICANS HATE THE MEDIA AND HOW IT MATTERS (2011) (illustrating how increased media fragmentation has interacted with demand for more partisan news to amplify partisanship and distrust of institutional news media).

the rise of cable television.[128] And, as data tell us, consumers of partisan news are both more likely to consume false news[129] and possibly are inherently more resistant to counterspeech that corrects that false news.[130] Therefore, the net effect is one in which the dynamics of the contemporary media ecosystem tilt the balance toward the consumption/impact of fake news to an extent that was not the case in the pre-filter bubble era.

This dynamic is particularly damaging to traditional articulations and applications of the counterspeech doctrine. Traditional approaches to counterspeech have essentially operated under a broadcast-era model of media distribution. Consider the Fairness Doctrine, which operated under the assumption that counterspeech presented on the same platform and at the same time of day as the original speech would be effective.[131] Such an assumption seems at best quaint, and at worst utterly anachronistic, when applied to today's media environment of intertwined individual and algorithmic content filtering,[132] in which filter bubbles have been constructed in ways that often are fundamentally oriented toward deflecting counterspeech. From this standpoint, it seems reasonable to suggest that the ability of counterspeech to reach exactly those it needs to reach has been diminished as a result of the technological changes that have affected the media ecosystem.

E. The Diminished Ability to Distinguish Between Legitimate and False News

Technological changes are undermining news consumers' abilities to distinguish between legitimate and false news. In illustrating this point, it is important to begin with the unique challenges associated with evaluating news. To do so, it is useful to begin with how consumers evaluate the quality of the products that they consume. Economists generally recognize three

128. *See* Amanda Taub, *The Real Story About Fake News is Partisanship*, N.Y. TIMES (Jan. 11, 2017), https://www.nytimes.com/2017/01/11/upshot/the-real-story-about-fake-news-is-partisanship.html [https://perma.cc/DQ34-XERP] ("[S]tarting in the 1980s, Americans began to report increasingly negative opinions of their opposing party."). For a more detailed discussion of the relationship between fragmentation and political polarization, *see* RICARDO GANDOUR, A NEW INFORMATION ENVIRONMENT: HOW DIGITAL FRAGMENTATION IS CHANGING THE WAY WE PRODUCE AND CONSUME NEWS (2016), https://knightcenter.utexas.edu/books/NewInfoEnvironmentEnglishLink.pdf [https://perma.cc/8KZA-WG7A].

129. *See* Delia Mocanu et al., *supra* note 124.

130. *See* R. Kelly Garrett et al. *Driving a Wedge Between Evidence and Beliefs: How Online Ideological News Exposure Promotes Political Misperceptions*, 21 J. OF COMPUTER-MEDIATED COM. 331, 344 (2016) ("In the month leading up to the election, a quarter of Americans said they used biased news sites several times or more. Reliance on these websites appears to produce a distorted understanding of evidence, potentially promoting inaccurate beliefs even when evidence is understood correctly. It is sobering to recognize that online news may contribute to misperceptions even when consumers encounter a range of outlets and have been exposed to more accurate political information").

131. *See* Ruane, *supra* note 30.

132. *See* Napoli, *supra* note 121.

categories of goods: 1) search/inspection goods, for which quality can be readily determined through examination; 2) experience goods, for which quality can be determined only after usage for a period of time; and 3) credence goods, which must be consumed on faith, as quality is difficult to ascertain.[133]

News can sometimes fall into the second category (say, for example, when the local newscast reports rain for tomorrow, but it ends up snowing instead).[134] But more often, news is likely to fall into the third category, with news being consumed, and potentially being put to use in decision-making, in ways that do not always result in the kind of observable feedback that allows for a subsequent evaluation of the veracity or quality of that reporting.[135]

When it comes to the evaluation of any kind of product, the notion of "bounded rationality" comes into play.[136] And news consumers typically are extremely rational, lacking the necessary information to make fully informed determinations as to the quality of the product they are consuming. This is a reflection of the fact that "by definition, news is what the public does not know."[137] For these reasons, the consumption of false news is to some extent a function of receiving inadequate information (interacting with the various cognitive biases discussed above),[138] and the resulting inability of consumers to distinguish between true and false information, and thus consuming fake news under the misperception that it is truthful. The challenge of accurately distinguishing between true and false news is further exacerbated by the dramatic increase in available news and information sources online, which places a greater cognitive burden on news consumers in terms of distinguishing between legitimate and false news sources and stories.[139]

---

133. *See* John H. McManus, *What Kind of Commodity is News?* 19 COMMC'N RESEARCH 787, 794 (1992).

134. In this situation, news is not unlike a "lemon" purchased from an automobile seller. The poor quality of the information (or car) is not revealed until well after the purchase is finalized. *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. OF ECON. 488, 490-91 (1970) (discussing "asymmetrical information").

135. *See Id.*

136. For an overview and advocacy of the concept of bounded rationality, *see generally* John Conlisk, *Why Bounded Rationality?*, 34 J. OF ECON. LIT. 669 (1996). For a discussion of the concept's relationship to the marketplace of ideas metaphor, *see generally* Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821 (2008).

137. *See* McManus, *supra* note 133, at 793.

138. *See* Garrett & Stroud, *supra* note 61.

139. *See, e.g.*, Olivia Solon, *Only 20% of U.S. Adults Have Information Overload, but Those Who do Feel the Burden*, THE GUARDIAN (Dec. 7, 2016), https://www.theguardian.com/technology/2016/dec/07/information-overload-pew-study-digital-divide. [https://perma.cc/647C-C5QP]; Xiaoyan Qiu et al., Lack of Quality Discrimination in Online Information Markets (January 2017) (unpublished manuscript) (on file with ResearchGate), https://www.researchgate.net/publication/312194354_Lack_of_quality_discrimination_in_online_information_markets [https://perma.cc/E3R6-UFWV].

Of particular importance is the extent to which the traditional mechanisms for combating this sort of uninformed consumption have been undermined by technological change. For instance, the reputations of news outlets long have served as a way for consumers to distinguish between truth and falsity.[140] Reputations have often been identified as an important factor to facilitate efficient markets for experience and credence goods.[141] The reputation of the *New York Times* for being truthful and accurate has generally been better than that of the *National Enquirer*.

This important heuristic, however, is being undermined as news consumption migrates to news aggregators and social media platforms. This is most compellingly demonstrated by research showing how seldom news consumers know the actual source of the news they are consuming. For example, recent research by the Pew Research Center indicates that individuals who consume news via social media are capable of identifying the originating source of the story consumed only about half the time.[142]

Further, this traditional outlet reputation-based mechanism for evaluating the likely truthfulness of a news story is being replaced by a new heuristic – the trustworthiness of the individual who shared the story on social media.[143] Thus, an article shared by a trusted member of an individual's social network, but written by a source unknown to that individual, will be evaluated as more trustworthy – and thus be more likely to be consumed and shared – than an article produced by a reputable news source but shared by someone viewed as less trustworthy.[144] This halo effect extends to news brands as a whole, with individuals more likely to follow and recommend news outlets that were referred to them by trusted members of their social network.[145] Given that the filter bubble dynamic discussed above is a function of the ideological homogeneity that characterizes many individuals' social

140. *See* Miriam J. Metzger et al., *Social and Heuristic Approaches to Credibility Evaluation Online*, 60 J. COMM. 413, 426 (2010) ("One of the most prevalent heuristics used for evaluating credibility that was mentioned by focus group participants was relying on site or source reputation.").

141. *See* Steffen Huck et al., Pricing and Trust 1 (Feb. 2008) (unpublished manuscript) (on file with Paris School of Economics) (noting that "[w]henever contracts for the exchange of a good are incomplete and sellers have leeway to shade its quality about which the consumer finds out only if it is too late . . . A key role in markets for such goods is assumed by trust"), https://www.parisschoolofeconomics.eu/IMG/pdf/Huck2.pdf [https://perma.cc/RS7B-EWVX].

142. *See* Amy Mitchell et al., *How Americans Encounter, Recall and Act Upon Digital News*, PEW RES. CTR. (Feb. 9, 2017), http://www.journalism.org/2017/02/09/how-americans-encounter-recall-and-act-upon-digital-news/. [https://perma.cc/L6JG-VQQA].

143. *See generally*, THE MEDIA INSIGHT PROJECT, "WHO SHARED IT?": HOW AMERICANS DECIDE WHAT NEWS TO TRUST ON SOCIAL MEDIA (2017), http://mediainsight.org/PDFs/Trust%20Social%20Media%20Experiments%202017/MediaInsight_Social%20Media%20Final.pdf [https://perma.cc/ED2R-YHEK].

144. *Id.* at 4-9.

145. *Id.* at 10 ("Those who trusted the sharer but saw the unknown outlet were more likely than those who did not trust the sharer and saw the reputable outlet to share the article, follow the sharer, sign up for news alerts from the source, and recommend the source to friends.").

networks,[146] the situation once again presents itself in which the likelihood of exposure to counterspeech is being undermined by the social media context in which news consumption is increasingly taking place.

These dynamics help to explain recent findings indicating that trust in mainstream news outlets is much lower than the levels of trust that news consumers place in the news outlets catering to their ideological orientation.[147] The distribution of trust in news organizations is essentially being reallocated in ways that favor the consumption and acceptance of fake news over legitimate news, which works against the effectiveness of counterspeech. Ultimately, if news consumers are increasingly unable to accurately gauge whether a news source's reporting is likely to be true or false, then more speech (i.e.., counterspeech) does nothing to assure that truth prevails and that democratic decision-making is well-informed.[148]

Moreover, news consumers need to consider the issue of intentional misrepresentation of news sources. Political propaganda has always been a part of political campaigns.[149] Under the logic of counterspeech, false propaganda should be effectively counteracted by true and accurate news and information. However, a key means of enhancing the effectiveness of false propaganda involves disguising the source.[150] Propaganda disguised as

146. *See* Itai Himelboim et al., *Birds of a Feather Tweet Together: Integrating Network and Content Analyses to Examine Cross-Ideology Exposure on Twitter*, 18 J. COMPUTER-MEDIATED COMM. 40, 40 (Jan. 2013) (finding that "Twitter users are unlikely to be exposed to cross-ideological content from the cluster of users they followed as these were usually politically homogeneous"); Andrei Boutyline & Robb Willer, *The Social Structure of Political Echo Chambers: Variation in Ideological Homophily in Online Networks*, 38 POL. PSYCHOL. 551, 566-567 (2017) (finding that more ideologically extreme individuals have more homophilous social networks, which should "result in networks that embed their members in denser webs of like-minded associations, which could then insulate individuals from the demotivating effects of dissenting views, and may enable political behaviors to spread faster than they would through sparser networks").

147. *See* Amy Mitchel et. al., *Political Polarization & Media Habits*, PEW RES. CTR. (Oct. 21, 2014) (showing "little overlap in the news sources [liberals and conservatives] turn to and trust"), http://www.journalism.org/2014/10/21/political-polarization-media-habits/. [https://perma.cc/MR4D-DUHL]; "*My" Media Versus "The" Media: Trust In News Media Depends on Which News Media You Mean* 1, MEDIA INSIGHT PROJECT (May 2017), http://www.mediainsight.org/PDFs/Meaning%20of%20Media/APNORC_Trust_The_Media_Topline_final.pdf. https://perma.cc/N6FQ-5M5E. (finding that "on many fronts, Americans are skeptical of 'the news media' in the abstract but generally trust the news they themselves rely on").

148. *See* Goldman & Cox, *supra* note 11, at 23.

149. For a comprehensive overview of the history of propaganda and its use in political campaigns, *see generally* Garth S. Jowett & Victoria J. O'Donnell, Propaganda & Persuasion (6th ed.) (2014).

150. *See* Jessie Daniels, *Cloaked Websites: Propaganda, Cyber-Racism and Epistemology in the Digital Era.* 11 NEW MEDIA & SOCIETY 658, 660 (2009) ("The emergence of websites such as Weltner's Katrina Families and American Civil Rights Review illustrates a central feature of propaganda and cyber-racism in the digital era: the use of difficult-to-detect authorship and hidden agendas intended to accomplish political goals.").

legitimate news has proven to be particularly effective.[151] What is different now is the extent to which propaganda can be effectively disguised as legitimate news.[152] This is a function of the diminished barriers to entry and institutional gatekeeping, which operate in concert with the enhanced distribution capacity of social media.

The degree to which propaganda operations can masquerade as news outlets is much greater in an environment in which legitimate and illegitimate news outlets can all exist side-by-side on social media platforms.[153] This is well-illustrated by the report that as many as 1,000 Russians were actively engaged in the production and distribution of fake news through social media during the 2016 election.[154] An analysis of Russia's online propaganda efforts emphasized Russia's utilization of a multiplicity of online sources that are often disguised as news outlets.[155]

In a 2012 television interview on the influence of money on political campaigning, the late, conservative Supreme Court Justice (and established counterspeech enthusiast) Antonin Scalia was asked how Thomas Jefferson would likely have viewed the contemporary political communication environment.[156] Scalia's reply was, "I think Thomas Jefferson would have said 'the more speech the better.' That's what the First Amendment is all about."[157] He followed that statement, however, with this important caveat: "*so long as the people know where the speech is coming from.*"[158] Thus, even from a traditionalist First Amendment perspective, the counterspeech doctrine is not absolute, and is especially vulnerable when the true source of news or information is disguised.

---

151. *Id.* at 662 ("Organizations and individuals who deploy the strategies of 'black' and 'grey' propaganda online via cloaked websites can be more effective precisely because they conceal their intention and authorship.").

152. Research indicates that social media users find it particularly difficult to accurately distinguish news posts from other types of social media posts. *See* Emily K. Vraga et al., *Blurred Lines: Defining Social, News, and Political Posts on Facebook*, 13 J.INFO. & TECH.POL. 272, 272 (2016) ("[U]sers and researchers often agree on defining social and political content, but are more likely to disagree on categorizing news content.").

153. Technological changes are likely to further enhance the ability to disguise fake news as legitimate news. *See* Nick Bilton, *Fake News is About to Get Even Scarier than You Ever Dreamed*, VANITY FAIR (Jan. 26, 2017), http://www.vanityfair.com/news/2017/01/fake-news-technology. [https://perma.cc/93U3-4MY9] ("At corporations and universities across the country, incipient technologies appear likely to soon obliterate the line between real and fake. Or, in the simplest of terms, advancements in audio and video technology are becoming so sophisticated that they will be able to replicate real news—real TV broadcasts, for instance, or radio interviews—in unprecedented, and truly indecipherable, ways").

154. *See* Roberts, *supra* note 117.

155. *See* Christopher Paul & Miriam Matthews, *The Russian "Firehouse of Falsehood" Propaganda Model.* RAND CORP.: PERSP. (2016), http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf, https://perma.cc/U3N8-5LXV ("[T]here are dozens of proxy news sites presenting Russian propaganda, but with their affiliation with Russia disguised or downplayed.").

156. *See Piers Morgan Tonight* (air date: Jul. 18, 2012 at 21:00 ET), CNN, http://www.cnn.com/TRANSCRIPTS/1602/13/cnr.12.html, [https://perma.cc/5C42-7MUX].

157. *Id.*

158. *Id.* (emphasis added).

It is important to note that even mainstream news outlets have, on many occasions, shown themselves to be unable to distinguish between legitimate news and fake news, and thus have contributed to the dissemination of fake news.[159] Parasitic journalism is an increasingly prominent dimension of the news ecosystem, with news outlets facing diminished resources to produce their own reporting or to rigorously verify the reporting of other news outlets.[160] These patterns increase the likelihood that legitimate news outlets will facilitate the dissemination of fake news and thereby legitimize it for some news consumers.

Thus, it is not surprising that recent research has illustrated that the false news stories emanating from "hyper-partisan" right-wing news sites were able to influence the agenda of the mainstream news media.[161] From a counterspeech perspective, this means that even the key providers of the legitimate news that is intended (according to the counterspeech doctrine) to overcome false news are not only operating at a diminished capacity to counteract false news, but are sometimes even complicit in its perpetuation.

And then, of course, there is the question of how well new distributors of news (i.e., social media platforms) are capable of distinguishing between true and false news, and whether they take action on the basis of such distinctions. Certainly, in the wake of the election these platforms have ratcheted up their efforts to identify and curtail the spread of fake news

159. For a discussion of the challenges to the journalistic process of verifying news and information disseminated online, *see* Alfred Hermida, *Tweets and Truth: Journalism as a Discipline of Collaborative Verification*, 6 JOURNALISM PRAC. 659 (2012).

160. *See The Future of Newspapers*, *supra* note 79.

161. *See* Yochai Benkler et al., *Study: Breitbart-Led Right-Wing Media Ecosystem Altered Broader Media Agenda*, COLUM. JOURNALISM. REV. (Mar. 3, 2017), http://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php, ttps://perma.cc/B4K8-ULQA ("Our own study of over 1.25 million stories published online between April 1, 2015 and Election Day shows that a right-wing media network anchored around Breitbart developed as a distinct and insulated media system, using social media as a backbone to transmit a hyper-partisan perspective to the world. This pro-Trump media sphere appears to have not only successfully set the agenda for the conservative media sphere, but also strongly influenced the broader media agenda, in particular coverage of Hillary Clinton.").

stories.[162] Whether these efforts have thus far been successful has been called into question.[163] The bottom line, however, is that when previous iterations of content distributors (cable systems, broadcast networks, book distributors, etc.) are compared to today's social media platforms, social media platforms know far less about the sources and content they are distributing (given the massive scale at which they operate) than any previous generation of content distributor.[164] In this regard, their relatively limited ability to distinguish between fake and legitimate news stories/sources – their bounded rationality – has been transferred to the news consumer.

F. The Enhanced Speed at Which False News Can Travel

Finally, it is important to consider how changes in media technology have altered the speed at which fake news can travel. The issue of speed is particularly important given that Brandeis' original articulation of the counterspeech doctrine notes that counterspeech represents the appropriate remedy to false speech only "If there be time . . ."[165] This is a very important qualification to take into consideration within the context of today's media ecosystem, in which news can "go viral."[166]

It has been well documented how advances in media technologies have compressed the "news cycle" and facilitated ever greater immediacy in the

---

162. *See* Josh Constine, *Facebook Shows Related Articles and Fact-Checkers Before You Open Links*, TECHCRUNCH (Apr. 25, 2017), https://techcrunch.com/2017/04/25/facebook-shows-related-articles-and-fact-checkers-before-you-open-links/. https://perma.cc/P243-XPQE; Fergus Bell, *Here's a List of Initiatives that Hope to Fix Trust in Journalism and Tackle Fake News*, MEDIUM (Apr. 25, 2017), https://medium.com/@ferg/heres-a-list-of-initiatives-that-hope-to-fix-trust-in-journalism-and-tackle-fake-news-30689feb402. https://perma.cc/W72T-KQ6E; *See also* Testimony of Sean J. Edgett, Acting General Counsel, Twitter, Inc., S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism (October 31, 2017), https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Edgett%20Testimony.pdf. [https://perma.cc/YN59-VF5Z]; Testimony of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism (October 31, 2017), https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Salgado%20Testimony.pdf. [https://perma.cc/S6AS-T6FJ]; Testimony of Colin Stretch, General Counsel, Facebook, S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism (October 31, 2017), https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf. [https://perma.cc/4Z2D-H32W].

163. *See, e.g.*, Sam Levin, *Facebook Promised to Tackle Fake News. But the Evidence Shows it's not Working*, THE GUARDIAN (May 16, 2017, 5:00 EDT), https://www.theguardian.com/technology/2017/may/16/facebook-fake-news-tools-not-working [https://perma.cc/TQP6-R7KD].

164. Indeed, one could convincingly argue that the goal of these platforms is to host as many speakers, and as much speech, as possible, with relatively little consideration given to the nature of the speakers/speech – particularly in comparison to previous generations of content distributors.

165. 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

166. For a useful case study of viral news, *see* Sapna Maheshwari, *How Fake News Goes Viral: A Case Study*, N. Y. TIMES (Nov. 20, 2016), https://www.nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html?_r=1. [https://perma.cc/G53Y-DZ9X].

delivery of news.[167] The latest development in this process is the role that social media can play in accelerating the distribution of a news story.[168] An emerging literature on "digital wildfires" documents the speed at which false news can travel and seeks to explain the factors that can affect its diffusion.[169] The speed of diffusion can be enhanced by technological advances such as bots (certainly something Brandeis didn't have to consider) that can operate on a scale and pace that human false news disseminators cannot[170] distribute fake news in their efforts to influence the 2016 election.[171]

Presumably, legitimate news has the same capacity to travel at equal speeds to false news today, just as it did in Brandeis' time. However, while the underlying technological capacity is the same, the troubling reality is that the rapid dissemination capacity of social media appears more likely to be brought to bear for false news stories than for true news stories. Recent data indicate that false news stories are more likely to be shared – and are thus

167. *See generally* HOWARD ROSENBERG & CHARLES S. FELDMAN, NO TIME TO THINK: THE MENACE OF MEDIA SPEED AND THE 24-HOUR NEWS CYCLE (2008).

168. This process dates back to the development of radio, and progresses through the rise of 24-hour news networks and the dissemination of news online. *Id.*

169. For a review, *see* Helena Webb et al., *Digital Wildfires: Propagation, Verification, Regulation, and Responsible Innovation.* 34 ACM TRANSACTIONS ON INFO. SYS. 1 (Apr. 2016).

170. *See* Alessandro Bessi & Emilio Ferrara, *Social Bots Distort the 2016 U.S. Presidential Election Online Discussion*, FIRST MONDAY (Nov. 7, 2016), http://journals.uic.edu/ojs/index.php/fm/article/view/7090, [https://perma.cc/258N-D44N] ("Our findings suggest that the presence of social media bots can indeed negatively affect democratic political discussion rather than improving it, which in turn can potentially alter public opinion and endanger the integrity of the Presidential election."); Samuel C. Woolley & Douglas R. Guilbeault, Computational Propaganda in the United States of America: Manufacturing Consensus Online, Computational Propaganda Research Project Working Paper No. 2017.5, Oxford Internet Institute 3 (2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf, [https://perma.cc/K2WM-RXYC](finding that bots are used to create "the illusion of significant online popularity in order to build real political support," and "democratiz[e] propaganda through enabling nearly anyone to amplify online interactions for partisan ends").

171. *See* Gabe O'Connor & Avie Schneider, *How Russian Twitter Bots Pumped Out Fake News During The 2016 Election*, NPR (Apr. 3, 2017), http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election [https://perma.cc/BR5U-KA4G] ("When he testified before the Senate Intelligence Committee last week, former FBI agent Clint Watts described how Russians used armies of Twitter bots to spread fake news using accounts that seem to be Midwestern swing-voter Republicans").

likely to spread faster (and farther) – than legitimate news stories.[172] The explanation for this disparity once again takes us back to the role of partisanship – in this case the role that partisanship plays in increasing the likelihood of sharing a partisan news story,[173] in combination with the increased likelihood that a partisan news story is a false news story.[174] The key implication here, once again, is that social media disproportionately favor fake news over legitimate news.

In the end, given that news has never been able to travel faster and farther than it can today, it seems reasonable to conclude that the likelihood of there "be[ing] time" to rely upon counterspeech to counteract false news is less today than in Brandeis' era, and perhaps less today than has ever been the case before, particularly given the other technologically-imposed challenges that truthful counterspeech faces in counteracting false speech. The end result, then, is a compounding set of conditions that contributes to a digital media ecosystem that encourages and facilitates the production, dissemination, and consumption of false news in ways that the traditional media ecosystem did not.

IV. IMPLICATIONS

This section considers the broader legal, policy, and political implications of the arguments developed above, all of which point to a media environment in which the efficacy of counterspeech is being systematically undermined.

A. The First Amendment and Falsity

As a starting point, it is worth considering how the arguments developed here connect with other analyses of if and how First Amendment jurisprudence has addressed the issue of false news and information. As Schauer points out, the troubling irony is that First Amendment theory has

172. Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook,* BUZZFEED (Nov. 16, 2016), https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.cq7vVRj0K#.tgekXRJ0E ("During these critical months of the campaign, 20 top-performing false election stories from hoax sites and hyperpartisan blogs generated 8,711,000 shares, reactions, and comments on Facebook. Within the same time period, the 20 best-performing election stories from 19 major news websites generated a total of 7,367,000 shares, reactions, and comments on Facebook"); Craig Silverman, *Lies, Damn Lies, and Viral Content* 45 (Tow Ctr. for Digital Journalism Tow/Knight Rep.) http://towcenter.org/wp-content/uploads/2015/02/LiesDamnLies_Silverman_TowCenter.pdf (observing that "Misinformation is often more viral and spreads with greater frequency than corrective information").

173. Jisun An, Daniele Quercia, & Jon Crowcroft, *Partisan Sharing: Facebook Evidence and Societal Consequences,* PROCEEDINGS OF THE SECOND ACM CONFERENCE ON ONLINE SOCIAL NETWORKS 13, 17 (Oct. 2014) (showing that "partisan skew" in the sharing of news stories on social media "holds not only for high-activity users but also for low-activity ones").

174. *See* Starbird, *supra* note 108.

seldom grappled with the issue of truth versus falsity; or, in today's vernacular, facts versus "alternative facts."[175] Schauer proceeds to convincingly demonstrate that, "nearly all of the components that have made up our free speech tradition . . . in the cases and in the literature, and in the political events that inspired free speech controversies, have had very little to say about the relationship between freedom of speech and questions of demonstrable fact. Implicit in much of that tradition may have been the belief that the power of the marketplace of ideas to select truth was as applicable to factual as to religious, ideological, political, and social truth, but rarely is the topic mentioned."[176] Continuing in this vein, Schauer distressingly notes, "although factual truth is important, surprisingly little of the free speech tradition is addressed directly to the question of the relationship between a regime of freedom of speech and the goal of increasing public knowledge of facts or decreasing public belief in false factual propositions."[177]

As a result, the First Amendment has essentially facilitated the type of speech that, ironically, undermines the very democratic process that the First Amendment is intended to serve and strengthen. Historically, different categories of speech have received different levels of First Amendment protection based upon its relevance and value to the democratic process.[178] For instance, commercial speech receives less First Amendment protection (and more rigorous restrictions against falsity) than political speech, which represents the pinnacle of speech protection given its centrality to the democratic process.[179] The irony here is that fake news is a type of speech that is most directly and irrefutably damaging to the integrity of the democratic process, yet because it resides within the large and undifferentiated protective bubble of political speech (where journalism generally resides), it receives (as long as it is not libelous) the highest level of First Amendment protection.

B. Market Failure in the Marketplace of Ideas

It is also worth considering the troubling state of counterspeech in relation to the marketplace of ideas metaphor from which it arose, and whether the increasing inefficacy of counterspeech may cause failure in the marketplace of ideas. From a strictly economic perspective on the marketplace of ideas, false speech can be thought of as a negative externality

---

175. For a transcript of the *Meet the Press* broadcast in which the term was famously introduced, *see* Rebecca Sinderbrand, *How Kellyanne Conway Ushered in the Era of "Alternative Facts,"* WASHINGTON POST (Jan. 22, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/01/22/how-kellyanne-conway-ushered-in-the-era-of-alternative-facts/?utm_term=.b633a394a39f. [https://perma.cc/MMC2-23J6].

176. *See* Schauer, *supra* note 46 at 907.

177. *Id.* at 902.

178. *See generally* T.M. Scanlon, Jr., *Freedom of Expression and Categories of Expression*, 40 U. PITT. L. REV. 519 (1979).

179. *See, e.g.*, Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627 (May 1990).

of free speech,[180] but a negative externality of increasing magnitude, given counterspeech's increasing inadequacy as an antidote. In economics, negative externalities are accepted indicators of market failure.[181]

When considering the implications of the diminished potency of counterspeech for the effective functioning of the marketplace of ideas, the presence of such negative externalities raises the question: should the public be concerned about the possibility of market failure in the marketplace of ideas? And if so, how does market failure in the marketplace of ideas look? The prospect and nature of market failure in the marketplace of ideas has received relatively little discussion, particularly within the context of news and journalism.[182] Economist Ronald Coase, in his landmark comparative analysis of regulatory perspectives toward the market for goods and the market for ideas, noted the "results actually achieved by this particular political system suggest that there is a good deal of 'market failure'" in the marketplace of ideas, though he deemed the topic "a large subject on which I will avoid comment."[183]

In addressing these questions, an important starting point is to consider some key causes and indicators of market failure. At the general level, a market failure occurs when the allocation of goods and services are inefficient.[184] Markets for public goods, such as journalism, have proven to be uniquely prone to market failure.[185] Public goods have a tendency to be under-produced relative to their full value, given the ease with which they can be shared or consumed without payment.[186] Journalism also produces value

---

180. *See* Richard A. Tybout, *Pricing Pollution and Other Negative Externalities*, 3 BELL J. ECON. & MGMT. SCI. 252 (Spring 1972). Therefore, as Schauer notes in a statement from 2009 that sounds particularly contemporary, "[W]e are left with the conclusion that the seemingly increased pervasiveness of falsity in public discussion is a phenomenon that may possibly be a consequence of a strong free speech culture, but is certainly not a phenomenon that a free speech regime is likely to be able to remedy." Schauer, *supra* note 46 at 911-912.

181. *See, e.g.*, Francis M. Bator, *The Anatomy of Market Failure*, 72 QUARTERLY J. ECON. 351, 3633-371 (1958).

182. For exceptions, *see* Tamara Piety, *Market Failure in the Marketplace of Ideas: Commercial Speech and the Problem that Won't Go Away.* 41 LOYOLA L.A. L. REV. 181 (2007) (focusing on market failures in the marketplace of ideas within the specific context of commercial speech); Gregory Brazeal, *How Much Does a Belief Cost? Revisiting the Marketplace of Ideas.* 21 S. CAL. INTERDISC. L.J. 46 (2011). For a more general overview of forms of market failure that may affect the marketplace of ideas, *see* Bush, *supra* note 17, nn. 47-90 and accompanying text; *see also* C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964 (1978) nn 61-83 and accompanying text.

183. *See* Ronald H. Coase, *The Market for Goods and the Market for Ideas*, 64 AM. ECON. REV. 384, 385 (1974).

184. Kenneth A. Shepsle and Barry R. Weingast, *Political Solutions to Market Problems*, 78 AM. POL. SCI. REV. 417 (1984) ("According to the market failure orthodoxy, inefficiency in the marketplace provides a prima facie case for public intervention").

185. *See* Victor Pickard, *The Great Evasion: Confronting Market Failure in American Media Policy*, 31 CRITICAL STUDIES STUD. IN MEDIA COMM.153, 154 (2014) ("Because public goods are non-rivalrous (one person's consumption does not detract from another's) and non-excludable (difficult to monetize and to exclude from free riders), they differ from other commodities, like cars or clothes, within a capitalistic economy").

186. *See* Hamilton, *supra* note 100 at 8 ("A person can consume a public good without paying for it, since it may be difficult or impossible to exclude any person from consumption").

for society as a whole (positive externalities) that often is not captured in the economic transactions between news organizations and news consumers, and/or between news organizations and advertisers.[187] All of this leads to market inefficiency in the form of the underproduction of journalism,[188] a situation only exacerbated by the more challenging economic environment discussed above.[189]

From an economic theory perspective, an informed citizenry and an effectively functioning democratic process are positive externalities. From a democratic theory perspective, however, these characteristics are not peripheral; they are fundamental. Thus, an effectively functioning marketplace of ideas needs to be assessed according to different standards. According to Piety, market failures in the marketplace of ideas can be exemplified by characteristics such as: "(1) the proliferation and acceptance of false ideas, (2) the suppression of truthful information, (3) the failure to produce truthful information, and… (4) limitations on choice, and the channeling of the exercise of preferences within those limitations."[190] Each of these characteristics connects fairly clearly to the conditions described above.[191] For example, items one and two reflect the apparent increasing prominence and influence potential of fake news and the role of filter bubbles in inhibiting exposure to legitimate news.[192] Item three reflects the diminishing journalistic capacity of legitimate news organizations. Item four concerns the operation of algorithmic filter bubbles, and how they tend to constrict news and information consumption within a narrower range of options determined by demonstrated preferences.

Some might argue that the increasing production, dissemination, and consumption of fake news is a reflection of the ways in which technological changes have allowed the market to more efficiently identify and meet consumer demand for falsity (the marketplace of ideas essentially becoming more efficient in serving consumer demand for fake news), rather than a reflection of consumers' diminished ability to accurately distinguish between legitimate and false news.[193] In considering this possibility, the notion that

187. *Id.* at 13 (". . . since individuals do not calculate the full benefit to society of their learning about politics, they will express less than optimal levels of interest in public affairs coverage and generate less than desirable demands for news about government").

188. *See* Pickard, *supra* note 195 at 155 ("The inadequacy of commercial support for democracy-sustaining infrastructures suggests what should be obvious by now: the systematic underproduction of vital communications like journalistic media").

189. *See* Downie & Schudson, *supra* note 76.

190. *See* Piety, *supra* note 191 at 189-190.

191. *See supra* notes 75-180 and accompanying text.

192. *See* Piety, *supra* note 191 at 189-190.

193. *See* Goldman & Cox, *supra* note 11 at 18 ("The whole idea of economic efficiency is that the system should be responsive to consumers' tastes or preferences (subject to the limits of technology), not that it should produce certain goods in comparatively large quantities no matter what people want. Thus, if consumers have no very strong preference for truth as compared with other goods or dimensions of goods, then there is no reason to expect that the bundle of intellectual goods provided and "traded" in a competitive market will have maximum truth content. If people valued falsehood, then perfect competition would provide falsehood in a Pareto-optimal way").

consumer demand for fake news is now being better met is cynical in that it reflects a grim view of the citizenry, in terms of a conscious desire to be misinformed. Even the bulk of the literature discussed above delineating the various cognitive biases that can lead to the consumption and acceptance of false news and information does not suggest that individuals are consciously and intentionally seeking false information, but rather that their cognitive biases lead them to mistakenly embrace false news and information as true.[194]

The notion that individuals desire true and accurate information but are not always capable of making the distinction, reflects a less cynical view of the citizenry and a reasonable sense of how an idea marketplace actually functions, given the recognized prominence of "bounded rationality"[195] in limiting marketplace efficiency. Further, this perspective represents the more optimistic (and perhaps naïve) normative principle that an effectively functioning marketplace of ideas facilitates informed democratic decision-making – something that is presumably incompatible with decisions based upon false information. As Lidsky argues,

> "The ideal of democratic self-governance . . . makes no sense unless one assumes that citizens will generally make rational choices to govern the fate of the nation. If the majority of citizens make policy choices based on lies, half-truths, or propaganda, sovereignty lies not with the people but with the purveyors of disinformation. If this is the case, democracy is both impossible and undesirable.[196]

Reflecting this position, this analysis operates (perhaps naively and optimistically – but First Amendment theory is nothing if not somewhat naïve and optimistic) from the perspective that consumers generally prefer legitimate to false news.

From this perspective, the unintentional consumption of fake news is a reflection of the bounded rationality of the news consumer, which can be seen as a function of inadequate information for making determinations as to the accuracy and reliability of available news sources. Inadequate information is a recognized source of market failure.[197] According to Brazeal, "[i]mperfect information is arguably the most significant and pervasive source of market failure in the marketplace of ideas."[198] A market cannot operate efficiently if

194. *See, e.g.*, Olson, *supra* note 62. *(*"Humans have an evolutionary tendency towards gullibility and wanting to believe what people are telling them").

194. *See supra* notes 62-63 and accompanying text.

195. *See* Conlisk, *supra* note 140.

196. Lidsky, *supra* note 23 at 839.

197. For a review *see* Deborah Haas-Wilson, *Arrow and the Information Market Failure in Health Care: The Changing Content and Sources of Health Care Information*, 26 J. HEALTH POL. POL'Y & L. 1031, 1034-1037 (2001).

198. *See* Brazeal, *supra* note 191 at 32.

consumers lack the information necessary to make well-informed decisions about the relative value of the products and services available to them.[199]

Another widely acknowledged source of market failure – both in the economic marketplace and in the marketplace of ideas – is imperfect competition.[200] From an ideas marketplace standpoint, a lack of competition fails to provide the "diverse and antagonistic" sources upon which the marketplace of ideas premise is founded.[201] More relevant to this analysis, however, is the fact that any biases inherent in the monopolist producers or distributors of news and information can undermine the extent to which the news consumers that rely upon them are properly informed.[202] A suddenly more vocal concern in the wake of the 2016 election has been the extent to which platforms, such as Facebook and Google play such an increasingly powerful bottleneck role in the dissemination and consumption of news and information.[203] Such concerns have tended to focus on these platforms' dominant position in the online advertising marketplace,[204] or their increasingly dominant position in the emerging data marketplace.[205] However, these platforms' growing bottleneck position in the dissemination of news and information has begun to receive more attention – and explicitly in relationship to the fake news problem that is the focus here. As Sally Hubbard convincingly argues, "fake news is [fundamentally] an antitrust problem", given the powerful intermediary position of Facebook, and the extent to which the algorithms that underlie the platform can point news

199. *Id.* at 31-32.

200. *Id.*

201. *See* Associated Press v. United States, 326 U.S. 1, 20 (1945), (noting that the First Amendment "rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public").

202. *See* Brazeal, *supra* note 191 at 31 ("Imperfect competition in the marketplace of ideas also occurs when the promotion of ideas is subsidized unequally").

203. *See, e.g.*, Brad Auerbach, *Are Amazon, Facebook and Google Monopolies? Are They Undermining Democracy? Taplin is Persuasive*, FORBES (May 26, 2017), https://www.forbes.com/sites/bradauerbach/2017/05/26/taplin/#4f7d67d26daa, [https://perma.cc/YHW4-XVYS]; On the Media, *The Fight for Antitrust* (Sept.ember 22, 2017), https://www.wnyc.org/story/fight-antitrust/, [https://perma.cc/6THS-KR3E].

204. *See* BitClave, *The Facebook-Google Online Ads Duopoly is Bad for Business*, MEDIUM (July 8, 2017), https://medium.com/@BitClave/the-facebook-google-online-ads-duopoly-is-bad-for-business-fa2b388de8fd [https://perma.cc/E2VZ-B3VK].

205. *See* Nick Srnicek, *We Need to Nationalise Google, Facebook, and Amazon. Here's Why*, THE GUARDIAN (Aug. 30, 2017), https://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest, [https://perma.cc/HG3K-S8KN]. https://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest, [https://perma.cc/HG3K-S8KN].

consumers toward fake news and away from legitimate news organizations.[206] The extent to which so many news consumers are relying upon these same algorithms (and whatever flaws or biases are baked into them) provides the baseline from which the damage to the marketplace of ideas emerges.

C. The 2016 Presidential Election as Market Failure Case Study

In light of these market failure concerns, a looming question is whether the results of the 2016 presidential election represent a case study of market failure in the marketplace of ideas. Perhaps this is a way to make sense of an election outcome that baffled and blind-sided many journalists, political analysts, and voters[207] – and that took place within a media ecosystem that has changed significantly in the years since the 2012 presidential election. Certainly, there are other equally (and perhaps even more) plausible explanations for this outcome (discussed below). The question being posed here is whether market failure in the marketplace of ideas, as a byproduct of the increased inefficacy of counterspeech, represents another potentially plausible explanation.

In considering the increasing challenges discussed above that not only news consumers, but news producers and (perhaps most importantly) distributors face in discerning between real and fake news, there is an "information asymmetry" – a classic cause of market failure – between the creators and the distributors and consumers of news. This is a problem potentially compounded by the "imperfect competition" scenario described above. And in considering the consumption of fake news as a negative externality, then there is a potential indicator of market failure. However, to truly accept the consumption of fake news as a negative externality, one must consider its negative consequences. Given that the idea marketplace is intended to facilitate well-informed decision-making, if there is evidence of poorly-informed decision-making, then that could potentially be seen as evidence of market failure.

Well-informed voting decisions have been defined by many political analysts in terms of the extent that citizens vote in ways that reflect their best

---

206. *See* Sally Hubbard, *Why Fake News is an Antitrust Problem*, FORBES (Jan. 10, 2017), https://www.forbes.com/sites/washingtonbytes/2017/01/10/why-fake-news-is-an-antitrust-problem/#4c557dc730f1, [https://perma.cc/P8GP-TFGM] ("When viewed through an antitrust lens, news publishers are Facebook's competitors. They compete for users' time spent online, user data and advertising dollars. . . . Indeed, competitive biases baked into Facebook's design deserve a healthy portion of the responsibility for the rise of fake news. By pulling technological levers that keep users on its platform, thereby lessening clicks to news publishers' sites, Facebook has sped the decline of legitimate news and provided a breeding ground for the fake variety").

207. *See, e.g.*, Susan Davis and Scott Detrow, *A Year Later, the Shock of Trump's Win Hasn't Totally Worn Off in Either Party*, NPR (2017, Nov. 9), https://www.npr.org/2017/11/09/562307566/a-year-later-the-shock-of-trumps-win-hasn-t-totally-worn-off-in-either-party; Shane Goldmacher and Ben Schreckinger, *Trump Pulls Off Biggest Upset in U.S. History*, POLITICO (2016, Nov. 11), https://www.politico.com/story/2016/11/election-results-2016-clinton-trump-231070;

interests.[208] Economic approaches, in particular, have emphasized the role of self-interest, i.e., that voters will vote for those candidates whose policy positions are likely to benefit them the most.[209] And, it should be emphasized that this notion of self-interest has been conceptualized not purely in terms of narrow, short-term economic self-interest, but more broadly as well, to accommodate family and social network affinities.[210]

There are a variety of competing theoretical perspectives that seek to explain the dynamics of voting behavior. Other theoretical perspectives emphasize the "expressive" dimension of voting, [211] or the inherent irrationality of voting that is a function of the negligible likelihood of rational voting behavior having a meaningful impact.[212] The market failure argument being put forth here in reference to the 2016 election does not reflect these theoretical perspectives, but is rather an extension of the self-interested voter hypothesis described above, which, it should be noted, has received strong empirical support in recent research.[213]

There have similarly been a variety of competing perspectives offered to explain the results of the 2016 presidential election. Some of these explanations have emphasized the likelihood that voters were motivated

208. For an overview of this perspective, *see generally* Gordon Tullock, On Voting: A Public Choice Approach (1998).

209. *See* Bryan Caplan, The Myth of the Rational Voter 18 (2007) ("[M]ost economists . . . compare voters to consumers who shrewdly 'vote their pocketbooks'").

210. *See* Jason Weeden & Robert Kurzban, The Hidden Agenda of the Political Mind: How Self-Interest Shapes Our Opinions and Why We Won't Admit It 39-40 (2014) (Arguing that "it's probably best to jettison the term 'self-interest' altogether . . . [and] refer to 'inclusive interests.' Something is in a person's 'inclusive interests' when it advances their or their family members' everyday, typical goals," as well as those of "their friends, allies, and social networks").

211. *See* Geoffrey Brennan and Loren Lomasky, Democracy & Decision: The Pure Theory of Electoral Preference (1993) 15-16 (contending that because "electoral outcome is detached from electoral 'choice' for each voter," voting becomes a form of "expressive behavior [that reflects] various kinds of ethical and ideological principles that are suppressed in the market setting. Politics, therefore, gives much freer range to ethical considerations than do markets").

212. *See* Caplan, *supra* note 225 at 3 (arguing that "Voter irrationality is precisely what economic theory implies once we adopt introspectively plausible assumptions about human motivation").

213. *See* Weeden & Kurzban, *supra* note 226 at 203 ("The key debate in these discussions . . . is how much interests matter in driving political opinions. In chapter 2 we responded to claims that self-interest hardly matters: When we run simple tests of these simple claims, quite often the simple claims are simply untrue").

primarily by informed self-interest.[214] Others have emphasized factors, such as frustration with the entirety of the political system (i.e., a desire to "blow up the status quo" in protest),[215] or prejudices, such as racism[216] and sexism.[217]

An additional possibility is that the 2016 election represented a case of market failure in the marketplace of ideas. Under this scenario, some segment of self-interested voters was sufficiently ill-informed (i.e., "boundedly rational") due to the changing conditions in the media ecosystem described above that they failed to vote in a way that reflected their best interests, an outcome that is associated with market failure. This market failure outcome is premised upon the substantial body of analysis that has been produced in the wake of the election that has repeatedly demonstrated that many categories of voters who voted for Donald Trump are actually those most

214. *See* Robert Kurzban & Jason Weeden, *No, Trump Voters Were Not Irrational,* WASHINGTON POST (Nov. 9, 2016), https://www.washingtonpost.com/news/in-theory/wp/2016/11/09/no-trump-voters-were-not-irrational/?utm_term=.45ad6fae23c6, [https://perma.cc/QU7H-4A3U] (arguing that white, blue collar voters voted for Trump not "because they're irrational, but because they are self-interested — something generally true of voters on both sides") ; *see also* David Goodhart, *White Self-Interest is not the Same Thing as Racism*, AMERICAN RENAISSANCE (Mar. 2, 2017), https://www.amren.com/news/2017/03/white-self-interest-not-thing-racism/, [https://perma.cc/JB4A-JM33]; Ned Barnett, *Duke Professor Dispels Myth About Trump and Working Class Voters*, THE NEWS-OBSERVER (Jun. 10, 2017), http://www.newsobserver.com/opinion/opn-columns-blogs/ned-barnett/article155509549.html [https://perma.cc/U87C-AKMP].

215. *See* Daniel Henninger, *The Trump Question*, WALL STREET JOURNAL (Jan. 18, 2017), https://www.wsj.com/articles/the-trump-question-1484784436 ("It is said that the Trump electorate wanted to blow up the status quo").

216. *See generally* Sean McElwee & Jason McDaniel, *Economic Anxiety Didn't Make People Vote Trump, Racism Did,* THE NATION (May 8, 2017), https://www.thenation.com/article/economic-anxiety-didnt-make-people-vote-trump-racism-did/, [https://perma.cc/2KAH-97U4] ("Our analysis shows Trump accelerated a realignment in the electorate around racism, across several different measures of racial animus—and that it helped him win. By contrast, we found little evidence to suggest individual economic distress benefited Trump").

217. *See* Carl Bialik, *How Unconscious Sexism Could Help Explain Trump's Win,* FIVETHIRTYEIGHT (January 21, 2017), https://fivethirtyeight.com/features/how-unconscious-sexism-could-help-explain-trumps-win/, [https://perma.cc/WM6E-DCLM] ("an important obstacle to the first woman president remains: the hidden, internalized bias many people hold against career advancement by women. And perhaps surprisingly, there is evidence that women hold more of this bias, on average, than men do").

likely to be harmed by his policies.[218] These analyses have concluded, for instance, that elderly and rural voters (two demographics who were strong Trump supporters) face the greatest economic harms from Trump policy initiatives such as the repeal of the Affordable Care Act, the abandoning of the Trans-Pacific Partnership, and dramatic cuts to Medicaid and agriculture subsidies.[219] Such patterns may reflect that the role of partisan affiliation in contemporary voting decisions has become largely disconnected from the associated policy positions of the candidates,[220] which is evidence of the Spiral of Partisanship phenomenon discussed above.[221]

If we accept the conclusions of these analyses (for arguments sake) that there was an unusual degree of voter failure to engage in self-interested voting behaviors, then this could reflect the possibility that a segment of voters lacked adequate information to accurately determine the voting decision that best reflected their self-interest. From the standpoint of a politically-oriented analysis of the operation of the marketplace of ideas, such indicators of voters failing to vote in their best interests, possibly due to false or inadequate information (through the spread of fake news, which was facilitated by the

---

218. *See, e.g.*, Martha C. White, *Trump Voters Stand to Suffer Most from Obamacare Repeal and Trade War*. NBC NEWS (Feb. 6, 2017) http://www.nbcnews.com/business/business-news/trump-voters-stand-suffer-most-obamacare-repeal-trade-war-n717491 [https://perma.cc/HWU7-PP8N]; Paul Krugman, *Coal Country Is a State of Mind*, NEW YORK TIMES, (Mar. 31, 2017) https://www.nytimes.com/2017/03/31/opinion/coal-country-is-a-state-of-mind.html, [https://perma.cc/9AGM-ZLBY]; Andrew Restuccia et al., *Trump Releases Budget Hitting His Own Voters Hardest*, POLITICO (May 22, 2017), http://www.politico.com/story/2017/05/22/trump-budget-cut-social-programs-238696, [https://perma.cc/8JW9-AHRU]; Amanda Taub, *Why Americans Vote "Against Their Interest": Partisanship.* NEW YORK TIMES (Apr. 12, 2017), https://www.nytimes.com/2017/04/12/upshot/why-americans-vote-against-their-interest-partisanship.html?_r=0, [https://perma.cc/3VEG-7GRS] ; Catherine Rampell, *Why the White Working Class Votes Against Itself*, WASHINGTON POST (December 22, 2016) https://www.washingtonpost.com/opinions/why-the-white-working-class-votes-against-itself/2016/12/22/3aa65c04-c88b-11e6-8bee-54e800ef2a63_story.html?utm_term=.99d233ea82fb, [https://perma.cc/EW5N-NX22]; Neil H. Buchanan, *Why Did So Many Americans Vote to Be Poorer?* NEWSWEEK (January 15, 2017), http://www.newsweek.com/neil-buchanan-why-did-so-many-americans-vote-be-poorer-542453, [https://perma.cc/E9V7-C5LN]; Neil Macdonald, *Trump's Poor and Rural Supporters Line Up to Take their Economic Beating.* CBC NEWS (April 5, 2017), http://www.cbc.ca/news/opinion/americans-voting-for-cuts-1.4055389, [https://perma.cc/TGP8-A58M].

219. *See* White, *supra* note 234 ("Donald Trump's most ardent supporters are likely to be hit the hardest if he makes good on his promise to dismantle the Affordable Care Act and embark on trade wars with China and Mexico"); Restuccia et al., *supra* note 218 ("Donald Trump, whose populist message and promises to help American workers propelled him to the White House, issued a budget proposal on Tuesday that instead takes aim at the social safety net on which many of his supporters rely").

220. *See* Taub, *supra* note 234 ("Why do people vote against their economic interests? The answer, experts say, is partisanship. Party affiliation has become an all-encompassing identity that outweighs the details of specific policies").

221. *See supra* notes 128-131 and accompanying text.

economic and technological conditions outlined above), could be seen as evidence of market failure.[222]

Whether or not one accepts this explanation as the cause of the 2016 election results, it still seems worth considering the ramifications of the market failure in the marketplace of ideas concerns being raised here. Accepting this possibility highlights the danger inherent in the institutionalized confidence in truth to overcome falsity that is endemic of First Amendment theory. It may very well be that the media ecosystem has evolved in such a manner that the gap between normative theory and empirical reality is no longer just a gap, but something much greater and more dangerous.

D. The Future of Counterspeech and the Marketplace of Ideas

Even if this market failure argument remains unconvincing, it seems necessary that, going forward, First Amendment jurisprudence and the operational decision-making of social media platforms, recognize the more limited efficacy of counterspeech within the context of the operation social media platforms. It seems appropriate that, within the context of news on social media, the counterspeech doctrine should receive the same kind of more circumspect and limited application that has been advocated for in speech contexts, such as hate speech[223] and adopted by the courts in contexts such as libel.[224] The Supreme Court's recognition that "false statements of fact" are particularly resistant to counterspeech[225] needs to extend beyond the context of individual reputation that provided the basis for that decision. In sum, the analytical frameworks of policymakers and the courts, and the governance approaches taken by social media platforms, need to take into account that the dissemination and consumption of news in the increasingly social-mediated online environment (what we might term the *algorithmic marketplace of ideas*) merits inclusion amongst those speech contexts in which reliance on counterspeech is increasingly ineffectual and potentially damaging to democracy.

In the end, perhaps this discussion illustrates a larger problem, which is the extent to which the application of First Amendment theory has tended to conflate the marketplace of ideas with what should perhaps be termed the marketplace of facts, particularly in relation to the role and function of journalism. The "ideas" terminology contains an inherent embrace of subjectivity, analysis, and opinion that reflects some, but not all, of the functionality of journalism in a democracy. A fundamental dimension of journalism is to provide factual information to facilitate informed decision-

222. In this scenario, the decision by some voters to vote for Donald Trump is essentially the marketplace equivalent of purchasing a lemon; *see* Akerlof, *supra* note 138.

223. *See* Delgado and Yun, *supra* note 69.

224. *See, e.g.*, Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988).

225. *Id.* at 52.

making.[226] To the extent that this functionality is folded into the broader marketplace of ideas metaphor, the result is something of a mischaracterization of this aspect of journalism's function.[227] One could argue that the very notion of facts competing for acceptance in the marketplace in the same way as ideas fundamentally undermines the very meaning of the term "fact" as something "that is indisputably the case."[228] In any case, the end result is that intentional disinformation under the guise of journalism receives a degree of First Amendment protection that is not afforded to other categories of false speech; this despite the Supreme Court's explicit statement that "there is no constitutional value in false statements of fact."[229]

From this standpoint, it is encouraging that, in the wake of the 2016 election, there has been a dramatic increase in efforts by the news aggregators and social media platforms that played central roles in the dissemination of fake news to alter their policies and procedures in ways intended to combat the spread of fake news. Thus, platforms, such as Google and Facebook, have dropped fake news sites from their ad networks.[230] Facebook and Google have created initiatives to integrate fact-checking and content labeling from third parties into their presentation of news stories to users.[231] There have been more concerted efforts to shut down disguised social media accounts operating as fronts for disinformation efforts.[232]

Initiatives such as these address the growing need for "tools of truth recognition" that operate "independent of the market in order for the market to be optimal."[233] Such efforts can be seen as working to reduce the "transaction costs"[234] associated with evaluating the reliability of news sources, and thereby addressing the information asymmetry that is the fundamental cause of the postulated market failure in the marketplace of

---

226. *See* Irene Costera Meijer, *The Public Quality of Popular Journalism: Developing a Normative Framework*, 2 JOURNALISM STUD.189, 189 (2001) ("Informing citizens in a way that enables them to act as citizens has traditionally been the responsibility of the press"); Mark Cooper, *The Future of Journalism: Addressing Pervasive Market Failure with Public Policy*, WILL THE LAST REPORTER PLEASE TURN OUT THE LIGHTS, 320, 322 (2011) ("The core concept of the monitorial role involves the journalist serving as a neutral watchdog, rather than a partisan participant, holding social, economic, and political actors to account by presenting facts rather than advocating positions and offering opinions").

227. For a discussion of the Supreme Court's failure to develop adequate mechanisms for distinguishing fact from opinion as it relates to journalistic output, *see* Robert Neal Webner, *The Fact-Opinion Distinction in First Amendment Libel Law: The Need for a Bright-Line Rule.* 72 GEO. L. J. 1817 (1984).

228. *See* Google Dictionary (https://www.google.com/#q=fact&spf=1497365412638).

229. *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 339-40 (1973).

230. *See* Silverman, *supra*, note 98.

231. *See* Bell, *supra* note 167.

232. *See* Stretch, *supra* note 167 at 4 ("we incorporated what we learned from the 2016 election in our detections systems, and as a result of these improvements, we disabled more than 30,000 accounts in advance of the French election").

233. *See* Goldman and Cox, *supra* note11 at 23.

234. For a discussion of transaction costs in the marketplace of ideas, *see* Blocher, *supra* note 140 at 852-60.

ideas. Going forward, these and other initiatives need to be evaluated in terms of the extent to which they address one or more of the six changes outlined above that have affected the marketplace of ideas in ways that have increased the ability of false news to undermine legitimate news.

Of course, such efforts by news aggregators and social media platforms raise the specter of further empowering already-powerful digital media bottlenecks, such as Facebook, Twitter, Google, and YouTube. The irony in this scenario is the extent to which it reflects a transition back towards the limited number of powerful gatekeepers that characterized the pre-fragmentation mass media era, but in a technological context in which many of the barriers to entry characteristic of the mass media era are no longer present. The mass media era was accompanied by critiques about concentration of ownership and the accompanying systemic homogeneity of viewpoints.[235] These critiques gave rise to concerns about the production and influence of propaganda that are similar to the concerns that underlie the current fake news scenario.[236] Given the extent to which different technological contexts seem to be leading to surprisingly similar institutional structures, it is tempting to conclude that a media ecosystem comprised of a fairly limited number of powerful gatekeepers is an inevitability, borne of larger institutional and economic forces, as well as innate audience behavior tendencies.[237]

Fortunately, from a journalistic standpoint, it is also the case that the mass media era of few, powerful gatekeepers cultivated a stronger "public service ethos" than has been present since technological change facilitated increased fragmentation and competition, and an associated need for news organizations to prioritize audience and revenue maximization over public service.[238] Of course, within some media sectors (e.g., broadcasting), this public service ethos could be attributed, at least in part, to a government-imposed public interest regulatory framework.[239] In any case, one of the most distressing aspects of contemporary social media gatekeepers is the extent to

---

235. *See, e.g.*, Edward S. Herman & Noam Chomsky, Manufacturing Consent: The Political Economy of the Mass Media (1988).

236. *Id* at 1-36 (developing a "propaganda model" of the mass media).

237. For an historical description of evolutionary patterns in the media and telecommunications sectors that support this argument, *see* Tim Wu, The Master Switch: The Rise and Fall of Information Empires (2010) at 6 (illustrating that each communications technology became "a highly centralized and integrated new industry" and that "Without exception, the brave new technologies of the twentieth century . . . eventually evolved into privately controlled industrial behemoths, the 'old media' giants of the twenty-first, through which the flow and nature of content would be strictly controlled . . . History also shows that whatever has been closed too long is ripe for ingenuity's assault: in time a closed industry can be opened anew, giving way to all sorts of technical possibilities and expressive uses for the medium before he effort to close the system likewise begins again").

238. For an account of the increased emphasis on audience and revenue maximization that took hold in journalism in the 1980s and 1990s, *see* John H. McManus, Market-Driven Journalism: Let the Citizen Beware? (1994).

239. *See* Napoli, *supra* note 123 at 753 (". . . articulations of public interest principles inherent in the professional practice of journalism parallel, to some extent articulations of the public interest that are found in the realms of media regulation and policy.").

which they have originated and evolved from a technology sector milieu in which the journalistic norms and/or regulatory framework associated with the public interest and social responsibility have been largely foreign to them.[240]

Moving forward, then, perhaps the most essential development is that these new gatekeepers evolve in such a way as to absorb and implement a more robust public service ethos that is reflective of the institutional responsibilities associated with serving as an essential gatekeeper to the news and information necessary for an effectively functioning democracy. In the aftermath of the 2016 election, and the associated critiques of social media platforms and their role in disseminating fake news, it is certainly evident that things are moving in this direction.[241] Efforts by search engines and social media platforms, such as Facebook and Google, to work with established and reputable fact-checking organizations to identify and label fake news stories, and to figure out ways at which such fact-checking and verification can operate the scale necessary for social media seem particularly promising.[242] However, it seems important that such collaborations go beyond mere content labeling, and that the editorial discretion ascribed to these platforms under Section 230 of the Telecommunications Act of 1996[243] be put to use to filter out false news in the same way that this discretion has long been used to filter out other types of harmful speech such as hate speech and pornography. Indeed, the demonstrated commitment to counterspeech that has been

240. *See, e.g.*, Philip M. Napoli & Robyn Caplan, *Platform or Publisher?* 44 INTERMEDIA 26, 27 (2017) ("One challenge in this regard, however, is a fundamentally different set of institutional perceptions that are being cultivated around social media platforms."); Emily Bell, *We Can't Let Tech Giants, Like Facebook and Twitter, Control Our News Values*, THE GUARDIAN (Aug. 31, 2014), https://www.theguardian.com/media/media-blog/2014/aug/31/tech-giants-facebook-twitter-algorithm-editorial-values, [https://perma.cc/T8BQ-SL66] ("Platforms that want public trust should be employing many more journalists than they presently do and using their knowledge to imbue automated process with values. . . . Accountability is not part of Silicon Valley's culture. But surely as news moves beyond paper and publisher, it must become so.").

241. *See, e.g.*, Fidji Simo, *Introducing the Facebook Journalism Project* (Jan. 11, 2017), https://media.fb.com/2017/01/11/facebook-journalism-project/, [https://perma.cc/V59V-5CLA]; Mark Zuckerberg, Building Global Community (Feb. 17, 2017), https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/, [https://perma.cc/PMA9-S72D] (Among the questions Zuckerberg raises for Facebook is "How do we help people build an informed community that exposes us to new ideas and builds common understanding in a world where every person has a voice?").

242. *See* Samuel Gibbs, *Google to Display Fact-Checking Labels to Show if News is True or False*, THE GUARDIAN: TECH (Apr. 7, 2017, 11:37 AM), https://www.theguardian.com/technology/2017/apr/07/google-to-display-fact-checking-labels-to-show-if-news-is-true-or-false, [https://perma.cc/M4RV-DH25]; *Elle* Hunt, *'Disputed by multiple fact-checkers': Facebook Rolls Out New Alert to Combat Fake News*, THE GUARDIAN: TECH (Mar. 21, 2017, 8:37 PM), https://www.theguardian.com/technology/2017/mar/22/facebook-fact-checking-tool-fake-news, [https://perma.cc/34GB-5G5H]. ; Samuel Gibbs, *Google to Display Fact-Checking Labels to Show if News is True or False*, THE GUARDIAN (Apr. 7, 2017), https://www.theguardian.com/technology/2017/apr/07/google-to-display-fact-checking-labels-to-show-if-news-is-true-or-false.

243. 47 U.S.C. § 230.

articulated by social media platforms such as Facebook, YouTube, and Twitter[244] needs to be tempered and surpassed by a greater commitment and editorial responsibility toward truth and accuracy that is reflective of our most reputable journalistic institutions.[245]

It is unclear at this point, however, whether the efforts put forth by social media platforms reflect a politically savvy (and perhaps temporary) response to the current moment of increased scrutiny, or whether these efforts represent the starting point for much-needed and more substantial institutional change. If it is the former, then with the key question is if or how government intervention might be an appropriate response. Other countries have already begun heading down this path. Germany, for instance, recently adopted a law that requires social media platforms to remove stories identified as fake news (along with other content types, such as hate speech and child pornography), or face government-imposed fines of up to 50 million Euros.[246] Such approaches, of course, raise the contentious question of who should be in the position of making judgments as to what constitutes fake news.

In the U.S., given the indiscriminate and politicized ways in which the fake news label is being applied by governmental actors,[247] the prospect of establishing an objective, reliable, and widely-trusted arbiter of fake news within a government agency seems more dangerous now than perhaps at any time in recent U.S. history.

It is perhaps worth remembering that, within fairly narrow technological contexts (e.g., broadcasting), a precedent for regulatory intervention in response to false news reporting has been established.

---

244. *See, e.g.*, Bartlett & Krasodomski-Jones *supra* note 55, at 5; TweeSurfing *supra* note 58; ONLINE CIVIL COURAGE INITIATIVE, *supra* note 56.

245. *See, e.g.*, Robyn Caplan, *Like it or Not, Facebook is Now a Media Company*, NEW YORK TIMES (May 17, 2016), https://www.nytimes.com/roomfordebate/2016/05/17/is-facebook-saving-journalism-or-ruining-it/like-it-or-not-facebook-is-now-a-media-company, [https://perma.cc/ZYY9-VDLK]; Seth Fiegerman, *Dear Facebook, You're a Media Company Now. Start Acting Like One*, MASHABLE: BUSINESS (May 15, 2016), http://mashable.com/2016/05/15/facebook-media-company/#zOF0ooxw0aqo [https://perma.cc/25PB-Y366; Seth Fiegerman, *Dear Facebook, You're a Media Company Now. Start Acting Like One*, MASHABLE: BUSINESS (May 15, 2016), [https://perma.cc/25PB-Y366].

246. *See* Staff, *Germany Approves Plan to Fine Social Media Firms Up to 50 Million Euros*, THE GUARDIAN (June 30, 2017), https://www.theguardian.com/media/2017/jun/30/germany-approves-plans-to-fine-social-media-firms-up-to-50m. [https://perma.cc/L6EW-TKF9].

247. *See* Lloyd Grove, *How Will the Media Fight the Right's Weaponization of "Fake News,"* THE DAILY BEAST, (Jan. 11, 2017), http://www.thedailybeast.com/how-will-the-media-fight-the-rights-weaponization-of-fake-news/ [https://perma.cc/HBY6-QFR7] (". . . the term 'fake news'—the enduring catchphrase of the 2016 presidential campaign, initially used to describe made-up tales and internet hoaxes that tended to benefit Trump and damage Hillary Clinton—is fast becoming the nascent Trump administration's rightwing-populist bludgeon to delegitimize the purveyors of *real* news" [emphasis in original].); *see also* Wardle & Derakhshan, *supra* note 75 at 5 ("the term has also begun to be appropriated by politicians around the world to describe news organizations whose coverage they find disagreeable. In this way, it's becoming a mechanism by which the powerful can clamp down upon, restrict, undermine and circumvent the free press").

Specifically, current FCC regulations prohibit broadcast licensees from knowingly broadcasting false information concerning a crime or catastrophe, if the licensee also knows beforehand that "broadcasting the information will cause substantial 'public harm.'"[248] This public harm must begin immediately and cause direct and actual damage to the property, health, or safety of the general public, or divert law enforcement or public health and safety authorities from their duties.[249]

In addition, since the late 1960s, the Federal Communications Commission ("FCC") also has maintained a more general policy that it will "investigate a station for news distortion if it receives documented evidence of such rigging or slanting, such as testimony or other documentation, from individuals with direct personal knowledge that a licensee or its management engaged in the intentional falsification of the news."[250] According to the FCC, "of particular concern would be evidence of the direction to employees from station management to falsify the news. However, absent such a compelling showing, the Commission will not intervene." [251] News distortion investigations have been rare (especially since the deregulatory trend that began in the 1980s), and seldom have led to any significant repercussions for broadcast licensees.[252]

Of course, the nature of the regulatory rationales that have traditionally applied to broadcasting (spectrum scarcity, pervasiveness) generally do not apply to a technological context such as social media. [253] However, discussions about possible regulatory interventions into the social media

248. *See* Federal Communications Commission, *Broadcasting False Information* (November 3, 2015), http://transition.fcc.gov/cgb/consumerfacts/falsebroadcast.pdf., [https://perma.cc/4PJU-GVLS].

249. *Id.*

250. *See* Federal Communications Commission, *The Public and Broadcasting* (July, 2008), https://www.fcc.gov/media/radio/public-and-broadcasting#DISTORT, [https://perma.cc/FZX9-QFWV].

251. *Id.*

252. *See* Chad Raphael, *The FCC's Broadcast News Distortion Rules: Regulation by Drooping Eyelid*, 6 COMM. L. & POLICY 485 (2001) (Arguing that the FCC's news distortion regulations are more symbolic than genuine). *See also* William B. Ray, FCC: The Ups and Down of Radio-TV Regulation at 31 (1990) ("On the whole, the commission has done less to carry out its stated policies regarding news broadcasting than in any other field").

253. For a detailed discussion of established rationales for U.S. media regulation, the distinction between regulatory rationales and motivations, and the significance of this distinction for possible regulatory responses to issues related to social media, *see* Philip M. Napoli, *Bridging the Disconnect Between Digital Media and the Public Interest*, Paper Presented at the XVIII Nordic Political Science Congress, Odense, Denmark (August, 2017).

space have gained some momentum of late,[254] with congressional hearings on the role of social media in the 2016 elections having recently taken place.[255] Given these indicators of potential shifts in the political environment, it is important to recognize that concerns about fake news have an established, if not modest and somewhat forgotten, foothold in the U.S. media regulatory framework.

Ultimately, though, it is important to acknowledge that the current political environment lends strength to the First Amendment tradition that has placed the judgment of truth and falsity in the realm of political speech completely outside the bounds of government authority,[256] and points us back to what might – at least for the time being – be considered the lesser of two evils – the need for today's dominant digital gatekeepers to more aggressively impose editorial authority in ways that reflect well-established norms of journalistic service in the public interest.[257]

V. CONCLUSION

The goal here has been to consider how the evolution of the news ecosystem has undermined legitimate news' ability to overcome fake news. This argument builds upon a body of critique of the counterspeech doctrine that is grounded in the persistent psychological and cognitive tendencies in news consumption that also undermine the efficacy of counterspeech.[258] From this standpoint, it may be that the news ecosystem, as previously constructed, has helped to protect citizens, to some extent, from some of their innate flaws and biases as news consumers.

---

254. *See, e.g.*, Lincoln Caplan, *Should Facebook and Twitter be Regulated Under the First Amendment?* WIRED (November 11, 2017), https://www.wired.com/story/should-facebook-and-twitter-be-regulated-under-the-first-amendment/, [https://perma.cc/8HM4-P4HB]; John Herrmann, *What If Platforms Like Facebook are Too Big to Regulate?* N.Y. TIMES (October 4, 2017), https://www.nytimes.com/2017/10/04/magazine/what-if-platforms-like-facebook-are-too-big-to-regulate.html, [https://perma.cc/RD3R-NNY7]; Sally Hubbard, *Why Fake News is an Antitrust Problem*, VOX (September 23, 2017), https://www.vox.com/technology/2017/9/22/16330008/facebook-google-amazon-monopoly-antitrust-regulation, [https://perma.cc/EG5W-2K5G].

255. *See Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions, Hearing Before the S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism*, 115th Cong. (Oct. 31, 2017), https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions [https://perma.cc/42VE-5HSD]; *Social Media Influence in the 2016 United States Elections, Hearing Before the S. Select Comm. on Intelligence* (Nov. 1, 2017), https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections [https://perma.cc/K65Y-XAQ4]; *Russia Investigative Task Force Open Hearing with Social Media Companies, Hearing before the H. Permanent Select Comm. on Intelligence* (Nov. 1, 2017), https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=814 [https://perma.cc/8DYT-QRJU].

256. *See* Thomas v. Collins, 323 U.S. 516, 545 (1945) (Jackson, J., concurring) ("every person must be his own watchman for truth, because our forefathers did not trust any government to separate the true from the false for us").

257. For a discussion of journalistic norms of public service and their applicability to social media platforms, *see* Napoli, *supra* note 123.

258. *See* Bambauer, *supra* note 62.

And it may be that the contemporary news ecosystem has been doing the exact opposite. The end result may be a state of market failure in the marketplace of ideas. Consequently, this Article has suggested social media platforms, content aggregators, policymakers, and the courts temper their commitment to counterspeech. This Article has also suggested that these platforms adopt a greater institutional commitment to a public interest-grounded approach to content filtering, in keeping with the editorial responsibilities that have characterized previous generations of news organizations. In the end, counterspeech can no longer function as a viable assumption when considering the current dynamics of the social media-based flow of news and information.

Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray Into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever

Rosie Brinckerhoff *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Executive Editor & Notes Editor, *Federal Communications Law Journal*, 2017–2018. B.A., Political Science, Minor in Journalism, University of Delaware, 2014. This Note is dedicated to my father, Clarke W. Brinckerhoff, the most brilliant and humble man I know. His love for the law and penchant for fairness are what inspired me to pursue a legal career. It is only because he thought I could succeed in this field that I even dared to try. I would like to extend a special thank you to everyone who feigned interest in hearing me ramble about Facebook over the past year and a half, but especially to my patient and loving mother, Judy Brinckerhoff. Many thanks to the staff of the *Federal Communications Law Journal* for their patient and meticulous editing. I would also like to thank Kara Romagnino for asking me the tough questions throughout my writing process and for providing extensive feedback on my many drafts. Any unprincipled deviations in this Note are my own.

I. INTRODUCTION

The rapid explosion in the number of social media companies utilizing and implementing facial recognition technology has introduced many privacy risks associated with collecting and storing consumer biometric[1] data for commercial use.[2] The fundamental issue stems from the fact that "[i]n the U[.]S[.], there is no single, comprehensive federal law regulating privacy and the collection, use, . . . and security of personal information."[3] Rather, the United States has a piecemeal system with respect to consumer data privacy, consisting of industry-specific federal privacy laws,[4] state privacy laws,[5] and

1. *See* Information Security Law § 1.01(6)(d) (LEXIS 2016) ("Translated literally, 'biometrics' means 'life measurement' - *bios* is Greek for 'life'; *metricus* is Latin for 'relating to measurement.' Biometrics can relate to a variety of means for establishing an individual's identity. Popular biometric methods of authentication include fingerprints, voice prints, iris scanning, and facial recognition.").

2. For a general discussion of privacy concerns manifesting from Facebook's use of facial recognition technology, *see generally* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/58TB-RQPB].

3. Ieuan Jolly, *US Privacy and Data Security Law: Overview*, LOEB & LOEB LLP, (July 1, 2016), https://blog.richmond.edu/lawe759/files/2016/08/US-Privacy-and-Data-Security-Law-Overview.pdf [https://perma.cc/9T6T-7M8N].

4. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY REPORT 33 (2015), http://www.gao.gov/assets/680/671764.pdf [https://perma.cc/3LVE-YFLG] ("Certain federal laws do address the collection, use, and sale of personal information by private-sector companies, as discussed earlier. These laws could potentially restrict, in certain circumstances, the collection of facial images, which are used to build a database for use with facial recognition technology. For example, provisions in the Driver's Privacy Protection Act restrict state motor vehicle bureaus from selling drivers' license photographs and associated information to private parties. In addition, the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act potentially could restrict the ability of banks and health care providers to share data collected with facial recognition technology if those data were to fall within the laws' definitions of protected information. However, the reach of these laws is limited because they generally apply only for specific purposes, in certain situations, to certain sectors, or to certain types of entities.").

5. Illinois leads the way in protecting consumer privacy with respect to biometric identifiers. Before collecting or storing any biometric identifying information, Illinois statutorily requires that a company: "(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." *See generally* Illinois' Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b) (2008), http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [https://perma.cc/NH9E-J5R3]. *See infra* note 40 for more information on other state-specific privacy laws.

best practice guides[6] from various governmental agencies.[7] Fittingly, this fragmented approach to regulating consumer data privacy has best been described as a "patch-work quilt."[8] With a disjointed legislative framework and no broad federal law in place to regulate the collection and distribution of biometric data, consumer privacy is becoming increasingly vulnerable.[9]

As a result, operating with no real legal restraint and only under conditions of self-regulation,[10] social media companies are well-positioned to take advantage of unsuspecting consumers using social networking sites and applications.[11] As one legal scholar succinctly stated "we cannot justify

---

6. In 2012, the FTC released its first and only "Best Practices Guide" for companies utilizing facial recognition technology, offering merely suggestions that companies are essentially free to ignore. *See Federal Trade Commission*, Best Practices for Common Uses of Facial Recognition Technologies (Oct. 12, 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf) [https://perma.cc/KD8G-43TK]; *cf.* Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43, 52–53 (2016), http://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/7 [https://perma.cc/B6CT-BWWS] ("Even the FTC's data privacy enforcement actions have been largely ineffective. When the FTC compelled Google and Facebook to more clearly disclose to consumers the private consumer data they were capturing and selling to others, the result was not more consumer protection, but merely more dense and indecipherable privacy disclosures that most users simply click through without reading— certainly without understanding") (citing Cameron Scott, *Less than Half of Facebook, Google Users Understand Sites' Privacy Policies*, COMPUTERWORLD (May 4, 2012), http://www.computerworld.com/article/2503822/data-privacy/less-than-half-of-facebook-- google-users-understand-sites--privacy-policies.html [https://perma.cc/LGR6-WWJN])).

7. Jolly, *supra* note 3.

8. Rosemary P. Jay, Lisa J. Sotto & Aaron P. Simpson, *Data Protection & Privacy 2015*, HUNTON & WILLIAMS PG. 208 (accessed Apr. 4, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf [https://perma.cc/93JX-Q9ZE].

9. *See, e.g.*, Chris Tomlinson, *Loss of internet data privacy should concern business, consumers*, HOUSTON CHRONICLE (Apr. 3, 2017), http://www.houstonchronicle.com/business/columnists/tomlinson/article/Business-should-worry-about-lost-data-privacy-11041215.php [https://perma.cc/4QSU-SHX5] ("This isn't just about whether you watch cat videos or visit porn sites. The most frightening part is that the repeal of internet privacy protections is only the beginning of a process that will be more intrusive than any strip search or home invasion . . . In a more connected world, when every electric device is connected to the internet, the effect could be profound and disturbing.").

10. *See, e.g.*, *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 12 (2012) (testimony of Jennifer Lynch of the Electronic Frontier Foundation), https://ssrn.com/abstract=2134497 [https://perma.cc/N7R9-XPCQ], ("[I]ndustry self- regulation and consumer control are not enough to protect against critical privacy and security risks inherent in facial recognition data collection.").

11. *See, e.g.*, Maelle Gavet, *The data says Google and Facebook need regulating*, WIRED (Mar. 5, 2015), http://www.wired.co.uk/article/data-google-facebook [https://perma.cc/WJL6-69TS] ("By assuming companies can be trusted to use our data responsibly, we are complicit in the notion that self-regulation will suffice -- and that we tamper with these innovators, by binding them up in regulation, at our peril. This is dangerous. It simply isn't acceptable for the likes of Google, Facebook, Amazon and others, which amass data by the terabyte, to say,

leaving the protection of consumers in their henhouses to the foxes who are collecting and profiting from the aggregation, sale, and resale of all this formerly private consumer data."[12]

Although the problem is much more pervasive than one company alone, this note is limited to Facebook, arguably the goliath of social media due to its 1.86 billion[13] users. By maintaining vastly overreaching user agreements and privacy policies, to which consumers are required to assent on a take it or leave it basis, Facebook is essentially demanding that consumers choose between signing away any last semblance of their privacy or being ostracized from a growing community of billions of social media users worldwide.[14]

Because technological innovation and Internet reliance are unlikely to come to a halt, prospective action needs to be taken to protect consumer privacy before it is too late.[15] As Facebook continues its quest into storing, selling, and sharing arguably anything and everything it can about its users in order to turn a profit, more stringent laws and regulations governing what companies are permitted to collect, store, and use are more necessary now than ever.[16] However, because comprehensive federal consumer privacy legislation is unlikely to be enacted anytime soon,[17] this note serves to argue

---

"Don't worry, your information's safe with us as all sorts of rules protect you" -- when all evidence suggests otherwise.").

12. Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43, 49 (2016), http://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/7 [https://perma.cc/B6CT-BWWS].

13. *Company Info*, FACEBOOK, (last revised Dec. 2016), http://newsroom.fb.com/company-info [https://perma.cc/E3GK-YUTB]/ (accessed Apr. 1, 2017).

14. *See, e.g.*, Stacey Higginbotham, *Companies need to share how they use our data. Here are some ideas*, FORTUNE MAGAZINE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy/ [https://perma.cc/6YDH-Y69Y] ("Currently, the choice is often pretty black and white. You accept the onerous terms of service (which are often presented in convoluted user agreements someone clicks through on their way to download the app after purchasing a new device) or you don't get to use the service.").

15. *See, e.g.*, Mark Weinstein, *Terms and Conditions May Apply Documentary: A Must See Horror Film*, THE HUFFINGTON POST (Aug. 2, 2013), http://www.huffingtonpost.com/mark-weinstein/terms-and-conditions-may-_b_3692883.html [https://perma.cc/N86Y-ZUMN] (acknowledging that "anonymity isn't profitable . . . [which] has driven Internet monoliths such as Google and Facebook to turn the Internet into a cog that turns us into a real-time surveillance state and George Orwell into a[] historian and prognosticator instead of an acclaimed fiction writer").

16. *See, e.g.*, Gavet, *supra* note 11 ("The history of business has shown that companies usually only regulate themselves if they're forced to by legislation, or out of self-interest -- often in the shape of a marketable message that will help sell more products. Not only is self-regulation largely a fantasy, but repeated scandals across multiple industries have proved that companies are fundamentally incapable of self-regulating for the greater good.").

17. *See Federal Trade Commission*, Privacy & Security in a Connected World, Staff Report (Jan. 2015) pg. vii , https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/TX3V-EFXY] (although the FTC recommended in 2015 "for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers

that intervention by the California judiciary is the best alternative in protecting consumer privacy from Facebook's overbearing Terms of Service and Data Policy. In addition to Facebook's forum selection clause mandating that any claims be resolved under California law "in the U.S. District Court for the Northern District of California or a state court located in San Mateo County,"[18] California provides a uniquely situated forum for judicial resolution due to its proximity and history with technology litigation.[19]

Although "[t]he California legislature has introduced several bills that would directly regulate biometrics collection . . . due in part to industry pushback, none of these laws has moved out of the legislature."[20] For example, legislation proposed in 2011 in the California Senate "which would [have] require[d] a company that collects or uses 'sensitive information,' including biometric data, to allow users to opt-out of its collection, use, and storage [] faced stiff opposition from technology companies and their trade organizations."[21] In an opposition letter written in response to the proposed state legislation, the signing companies argued that "[p]rohibiting the collection and use of this data would severely harm future innovation in the state and harm consumers."[22]

Despite the fact that the industry desires to proceed unregulated in this modern-day race for data aggregation, the argument that consumer privacy comes at the expense of innovation is necessarily skewed. It is entirely possible to protect consumer privacy without stifling and impeding technological innovation; accurately stated by Federal Communications Commission (FCC) Enforcement Bureau Chief Travis LeBlanc, "[p]rivacy and innovation are not incompatible."[23] Because "[i]t is no longer enough to justify privacy invasions as technologically inevitable or as essential to the American economy,"[24] California courts have a critical opportunity to

---

when there is a security breach," Congress has not acted towards implementing broad consumer data privacy legislation).

18. FACEBOOK, *Terms of Service, Section 15*, https://www.facebook.com/terms.php (accessed Apr. 10, 2017).

19. *See, e.g.*, Campbell et al v. Facebook Inc., Case No.: 4:13-cv-5996 (N.D. Cal. 2013) (regarding Facebook's alleged interception of private user messages for purposes of data mining and sharing with third parties); Singh v. Google, No. 16-cv-03734-BLF * 2 (N.D. Cal. 2016) (regarding Google's alleged failure "to prevent invalid clicks on unspecified AdWords advertisements"). Additionally, a number of technology giants, such as Google and Apple, have forum selection clauses specifying that claims are to be litigated exclusively in California. (*See* Google, Terms of Service, https://www.google.com/policies/terms/ (accessed Feb. 15, 2018); Apple, Media Services Terms and Conditions, https://www.apple.com/legal/internet-services/itunes/us/terms.html (accessed Feb. 15, 2018).

20. Lynch, *supra* note 10, at 21.

21. *Id*.

22. Opposition Letter to Sen. Alan Lowenthal (Apr. 27, 2011), http://static.arstechnica.com/oppositionletter.pdf.

23. *See* Press Release, Federal Communications Commission, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf (LeBlanc further noted that "[c]onsumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online").

24. MacLean, *supra* note 12, at 45.

proactively remedy the growing divide between reasonably sound consumer privacy policy and rapidly emerging technology endeavors.[25] Industry pushback and failure of the California legislature to pass a proper consumer privacy bill should not bring consumer privacy efforts to a grinding halt, especially when the state constitution has sufficiently teed up California courts to address the issue.

As such, this note will demonstrate why California courts are perfectly positioned to set the standard for pro-consumer, pro-privacy user agreements by holding Facebook's Terms of Service and Data Policy unconscionable due to the company's non-consensual deployment of facial recognition technology to collect its users' biometric data. [26]

Section II of this note will provide a brief technical overview of facial recognition technology and its associated privacy implications, as well as a background discussion on Facebook's current capabilities with facial recognition technology. Section III of this note will outline the doctrine of unconscionability under California law, examining the requisite elements and interplay between procedural and substantive unconscionability. This section will also include an analysis of how Facebook fails to explicitly mention and explain its biometric data collection practices in its ambiguous and overreaching Terms of Service and Data Policy, arguing that Facebook's non-consensual collection of this sensitive data is unconscionable pursuant to California law. Finally, Section IV of this note will conclude with an explanation of why California courts are in the best position to set a standard for Terms of Service and Data Policy agreements that adequately protect consumer privacy without hindering private-sector technological innovation. Apart from discussing how and why courts should properly reach a finding of unconscionability with respect to Facebook's biometric data collection practices, this section will also propose two additional solutions, one under state constitutional law and one under state tort law, in an effort to demonstrate the many legal tools the California judiciary has at its disposal to safeguard sensitive consumer biometric data.

25. *See generally* MacLean, *supra* note 12.

26. California courts are the only hope for consumers in adequately addressing this issue, as Facebook includes a forum clause in its Terms of Service agreement requiring any and all disputes and litigation to be handled in California. Pursuant to Section 15 of Facebook's Statement of Rights and Responsibilities, "[t]he laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions." *Terms*, FACEBOOK (last revised Jan. 30, 2015), https://www.facebook.com/terms.php [https://perma.cc/U848-M6QV] (accessed Apr. 3, 2017).

II. BACKGROUND: A BRIEF GUIDE TO FACIAL RECOGNITION TECHNOLOGY

A. Facial Recognition Technology – A Brief, Technical Overview

Facial recognition technology is most simply described as a biometric technology resource "which identifies individuals by measuring and analyzing their physiological or behavioral characteristics."[27] Designed to mimic and advance the human ability to recognize and identify faces,[28] computer facial recognition technology systems are capable of holding and analyzing an enormous amount of facial data imaging.[29] To illustrate this concept, while the human brain has a limited ability in the number of faces it can precisely recall,[30] a single server computer can search over 10 million records in less than 10 seconds.[31]

The exact mechanics of a facial recognition technology system are far beyond the scope of this note.[32] However, a brief explanation of the fundamental technology is necessary in order to understand the legal argument asserted herein. Accordingly, "[t]here are generally four basic components to a facial recognition technology system: a camera to capture an image, an algorithm to create a faceprint (sometimes called a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database."[33]

After uploading a photograph, a machine learning algorithm is trained to recognize any number of "specific points (called landmarks) that exist on every face—the top of the chin, the outside edge of each eye, the inner edge of each eyebrow" and more.[34] This information is used to create a facial template, which "is a reduced set of data that represents the unique features of [a person's] face."[35] The template is then compared against other stored

27. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 2.

28. *See* Danna Voth, *Face recognition technology*, 18 IEEE INTELLIGENT SYSTEMS 3, 4–7 (May-June 2003), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1200719 [https://perma.cc/79MK-RQAZ].

29. WENYI ZHAO & RAMA CHELLAPPA, FACE PROCESSING: ADVANCED MODELING AND METHODS, 8, 9 (Academic Press 2006).

30. *Id*.

31. *See* Michael Petrov, *Law Enforcement Applications of Forensic Face Recognition*, MORPHOTRUST USA, 12 (Sept. 2012), http://www.planetbiometrics.com/creo_files/upload/article-files/whitepaper_facial_recognition_morphotrust.pdf [https://perma.cc/UJ6M-DH4B].

32. For a thorough explanation and inquiry into facial recognition technology, *see generally* STAN Z. LI & ANIL K. JAIN, HANDBOOK OF FACIAL RECOGNITION, (2d ed. Springer 2011).

33. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 3.

34. Adam Geitgey, *Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning*, MEDIUM (July 24, 2016), https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78#.gz60g6v3i [https://perma.cc/U9NQ-4TXM].

35. JOHN D. WOODWARD, JR. ET AL., BIOMETRICS: A LOOK AT FACIAL RECOGNITION, 3–4 RAND (2003).

images in the system database by way of a process that can then be used for either identification or verification purposes.[36]

Although in the past facial recognition technologies have been predominantly used by law enforcement agencies and government entities,[37] "commercial interest and [private] investment in facial recognition technology have grown as the technology has become more accurate and less costly, with new applications being developed for consumers and businesses."[38] With an ever-increasing demand, the facial recognition technology market is predicted to reach $2.67 billion in 2022.[39] However, the emerging interest and rapid growth in companies using facial recognition technology for commercial purposes creates novel consumer privacy implications and concerns that have not been addressed through federal legislation.[40]

B. Privacy Implications of Facial Recognition Technology

The greatest concern in increased use of facial recognition technology is the loss of privacy to consumers.[41] This unease stems from the fact that "if its use becomes widespread, businesses or individuals may be able to identify almost anyone in public without their knowledge or consent."[42] Because facial recognition technology essentially maps and codifies a person's facial

36. *Id*. ("In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity.").

37. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 7 (citing *The Current and Future Applications of Biometric Technologies: Hearing Before the Subcomm. on Research and Tech. of the H. Comm. on Science, Space and Tech.*, 113th Cong. 1 (2013) (statement of John Mears, Board Member, International Biometrics & Identification Association)).

38. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 7, (citing FTC, *supra* note 6.).

39. *See Facial Recognition Market Expected to Reach US$ 2.67 Bn by 2022 Globally*, TRANSPARENCY MARKET RESEARCH, (Jul. 23, 2015), http://www.transparencymarketresearch.com/pressrelease/facial-recognition-market.htm [https://perma.cc/92JU-ECGN].

40. Three states, Illinois, Texas and Washington, have enacted laws regulating the collection, use and retention of consumer biometric data, signaling a shift towards a more state-based regulatory framework. However, this piecemeal state-by-state approach raises a host of other concerns outside the scope of this note. For a discussion of the Illinois, Texas and Washington biometric laws, *see generally* Ted Claypoole &Cameron Stoll, Developing Laws Address Flourishing Commercial Use of Biometric Information, AMERICAN BAR ASSOCIATION (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html [https://perma.cc/C84P-GTGW].

41. *See, e.g.*, NANCY YUE LIU, BIO-PRIVACY; PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS, 78 (Routledge Taylor & Francis Group 2012) ("It will generally not be a difficult task to link, directly or indirectly, a biometric identifier to other personal data . . . [i]f personal information could be linked and identified using the biometric data, one's ability to remain anonymous would be severely diminished." (citation omitted)).

42. *See* Information Security Law, *supra* note 1.

geometry,[43] "[p]rivacy advocates essentially argue that conversion of facial features to machine-readable data points eliminates one's ability to voluntarily choose to disclose ones identity to the public and such features become a resource that others control."[44]

To illustrate this point, California-based facial recognition technology company FaceFirst allows retailers to upload photographs of their best customers, repeat shoplifters, or other persons of interest into a facial database. When a person in the database enters the store, the system immediately notifies the owner and sends an "alert that includes their picture and all biographical information of the known individual."[45] FaceFirst touts itself as a beneficial service for retailers, casinos, and stadiums alike that can enhance customer service while concurrently cracking down on crime and shoplifting.[46] However, FaceFirst's quest to maximize commercial profits and enhance customer service fails to take into account whether or not a consumer wants to be recognized and identified. With no consumer privacy law in place to govern, retailers are under no legal obligation to disclose its use of the facial recognition technology.

Further, the lengths to which facial recognition technology may be employed are extensive and far-reaching. For example, in Russia, a facial recognition app called FindFace enables consumers to photograph a stranger and discern his or her identity with up to 70% accuracy.[47] This application draws striking similarities to Recognizr, a Swedish mobile application that enables users to point a smartphone camera at another person, after which "[a] cloud server conducts the facial recognition [ ] and sends back the subject's name as well as links to any social networking sites the person has provided access to."[48]

---

43. *See* Woodward, *supra* note 35 ("Because a person's face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (i.e. the subject does not necessarily know he has been observed).").

44. *See* Information Security Law, *supra* note 1.

45. *See* FaceFirst, http://www.facefirst.com/services/retail (accessed Nov. 18, 2016); *accord* Natasha Singer, *When No One Is Just a Face In The Crowd*, N.Y. TIMES (Feb. 1, 2014), https://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html [https://perma.cc/92UQ-HS3F].

46. *See Face Recognition for Retail Stores*, FACEFIRST, https://www.facefirst.com/industry/retail-face-recognition/ [https://perma.cc/WW9M-EJZY] (accessed Apr. 3, 2017).

47. *See generally* Shaun Walker, *Face recognition app taking Russia by storm may bring end to public anonymity*, THE GUARDIAN (May 17, 2016), https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte [https://perma.cc/H3TG-TPQM] (touting the facial recognition technology, FindFace founder stated: "If you see someone you like, you can photograph them, find their identity, and then send them a friend request . . . It also looks for similar people. So you could just upload a photo of a movie star you like, or your ex, and then find 10 girls who look similar to her and send them messages").

48. Clay Dillow, *Augmented Identity App Helps You Identify Strangers on the Street*, POPULAR SCIENCE (Feb. 23, 2010), http://www.popsci.com/technology/article/2010-02/augmented-identity-app-helps-you-identify-friend-perfect-strangers [https://perma.cc/LL4T-7VBN].

Perhaps the biggest privacy issue with facial recognition is that "[o]nce someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the Government buildings you enter, and the photos your friends post online."[49] In fact, a series of experiments conducted at Carnegie Mellon University objectively concluded that "[i]f an individual's face on the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her."[50]

Accordingly, another significant privacy implication stems from the fact that "[o]nce data resides on the Internet, it is very difficult or impossible to erase."[51] This is because "[f]irms routinely take snapshots of the Internet that yield the cached webpages that turn up on your browser searches."[52] Even assuming that a person acted preemptively to try and protect their privacy online, the prevalence of data hacking presents a serious concern, especially in the wake of increased facial recognition technology use. For instance, in a 2013 cyber-attack, 1 billion Yahoo accounts were hacked, resulting in a data breach consisting of "sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password."[53] Although the significance of Yahoo's data breach cannot not be discounted, the consequences and repercussions could have been much more severe had facial recognition data been involved, because "[y]ou can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face."[54]

---

49. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong 1–2 (2012) [hereinafter *Facial Recognition Hearing*] (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law), https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf [https://perma.cc/DT2B-KN5N].

50. *Id.* (testimony of Professor Alessandro Acquisti from Carnegie Mellon University), https://www.judiciary.senate.gov/imo/media/doc/12-7-18AcquistiTestimony.pdf [https://perma.cc/J2FM-AXCN].

51. MacLean, *supra* note 12, at 49.

52. *Id*. (citing Bernard J. Jansen et al., *Real Life, Real Users, and Real Needs: A Study and Analysis of User Queries on the Web*, 36 INFO. PROCESSING & MGMT. 207, 207 (2000)).

53. Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/6NP7-N3RL].

54. *Facial Recognition Hearing*, *supra* note 49, at 1 (opening statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

C. Facebook's Current Capabilities with Facial Recognition Technology

Facebook currently employs facial recognition technology to help users "tag"[55] friends in photos uploaded to the platform.[56] Although Facebook originally required users to manually tag friends, the company debuted "tag suggestions" in 2010 to make the tagging process easier for users.[57] Facebook describes its tag suggestions to users as follows: "When someone uploads a photo of you, we might suggest that they tag you in it. We're able to compare your friend's photos to information we've put together from your profile pictures and the other photos you're tagged in."[58] Facebook's final step is to then "associate the tags with your account, compare what these photos have in common and store a summary of this comparison."[59]

At the heart of tag suggestions is facial recognition technology. Mentioned briefly in Facebook's Help Center, the company's "facial recognition software [ ] uses an algorithm to calculate a unique number ('template') based on someone's facial features, like the distance between the eyes, nose and ears."[60] The template is crafted through a series of each user's profile pictures and tagged photos.[61] Although users can elect to disable the tag suggestion feature, meaning that Facebook will not suggest that people "tag you in photos that look like you,"[62] the company may still create a template using the individual user's profile picture and individually uploaded photos.[63]

Facebook's facial recognition technology enables the company to identify a person's face with nearly 98% accuracy.[64] Moreover, Facebook touts the fact that it can recognize and identify an individual in a single picture out of 800 million in under five seconds.[65] Unsurprisingly, "[d]ue to the large number of Facebook users and the fact that these users actively tag each other

---

55. According to Facebook, "[w]hen you tag someone, you create a link to their profile . . . [effectively] you can tag a photo to show who's in the photo." *What is tagging and how does it work?*, FACEBOOK, https://www.facebook.com/help/124970597582337 [https://perma.cc/DP5W-M62Q] (accessed Jan. 19, 2016).

56. *See generally Tagging Photos*, FACEBOOK, https://www.facebook.com/help/463455293673370 [https://perma.cc/GAV3-CQYH] (accessed Jan. 19, 2016).

57. *See generally Making Photo Tagging Easier*, FACEBOOK, https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/ [https://perma.cc/FS3Z-VQVW] (accessed Jan. 19, 2016).

58. FACEBOOK *supra* note 56, (accessed Jan. 19, 2016).

59. *Id*.

60. *Id*.

61. *Id*.

62. *Id*.

63. *Id*.

64. *See* Stacey Higginbotham, *Inside Facebook's Biggest Artificial Intelligence Project Ever*, FORTUNE (Apr. 13, 2016), http://fortune.com/facebook-machine-learning/ [https://perma.cc/E7FW-QGHN].

65. *Id*.

and themselves in photos, Facebook's face recognition system is the most robust and well-developed of all of these private sector products."[66]

It should be noted that Facebook's Data Policy allows users to access its "Download Your Information" tool.[67] However, the tool only yields a fractional portion of a user's personal data file, offering an arguably inadequate amount of information as to the biometric data that Facebook has on file for each particular user.[68] Figure A illustrates the entirety of information provided to inquiring users curious about the facial recognition data that Facebook has on file.[69]

Biz Carson

Facial Recognition Data

Threshold 1	3.5095708370209
Threshold 2	3.2094926834106
Threshold 3	1.668349981308
Example Count	237

Figure A [70]

A user proactively trying to discern what biometric data Facebook has stored on file would be presented with the nonsensical strand of numbers above in Figure A. An exhaustive search through Facebook's Help Center provides no explanation as to what "Thresholds 1, 2, 3" or "Example Count" refers, nor does Facebook include an explanation as to what facial recognition data the company actually has.[71] As such, while a user can technically view the facial recognition data that Facebook has stored, no meaningful information is actually provided.

---

66. Lynch, *supra* note 10, at 9.

67. FACEBOOK, *Accessing Your Facebook Data*, https://www.facebook.com/help/405183566203254/ (accessed Jan. 22, 2017) [https://perma.cc/2RJN-R7FW].

68. *Id.* ("We store different categories of data for different time periods, so you may not find all of your data since you joined Facebook"); *see also* Consumer Reports, *Facebook & your privacy: Who sees the data you share on the biggest social network?*, CONSUMER REPORTS MAGAZINE (June 2012), https://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm [https://perma.cc/6VN2-47BD].

69. Facebook's Download Your Information tool says that it provides users with Facial Recognition Data, which is "[a] unique number based on a comparison of the photos you're tagged in. We use this data to help others tag you in photos." However, the company does not explain the information downloaded as exemplified in Figure B. *See Accessing Your Facebook Data*, *supra* note 67.

70. Biz Carson, *I downloaded my data from Facebook and found all of the people I unfriended in the last 10 years*, BUSINESS INSIDER (May 19, 2016), http://www.businessinsider.com/how-to-download-data-from-facebook-2016-5/#in-the-settings-menu-where-you-normally-change-your-password-click-the-download-a-copy-button-2 [https://perma.cc/48DU-DEKT].

71. *Id.* ("Facebook even has my 'Facial Recognition Data' on file. The three thresholds mean nothing to me, but apparently Facebook has 237 examples of what I look like on file.").

The problem is that with no biometric privacy law on point, Facebook is operating unrestrained in its collection of its users face prints. Acting purely in the best interest of the company, Facebook issues its extraordinarily overbroad Terms of Service and Data Policy to its users, thereby granting the company an unprecedented level of freedom with respect to its data collection. The next section will demonstrate how Facebook's Terms of Service and Data Policy are unconscionable under California law due to the company's utilization of facial recognition technology and biometric data collection practices.

III. FACEBOOK FAILS TO EXPLICITLY INFORM CONSUMERS OF ITS USE OF FACIAL RECOGNITION TECHNOLOGY: HOW THE COMPANY'S TERMS OF SERVICE AND DATA POLICY SATISFY THE CALIFORNIA STANDARD FOR UNCONSCIONABILITY

A. The Doctrine of Unconscionability Under California Law

Notwithstanding the absence of a precise definition of unconscionability, several cases adjudicated in California[72] have adhered to the guidance set forth in *Williams v. Walker-Thomas*, which states: "Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party."[73] Accordingly, it is well-established that "the doctrine of unconscionability has both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results."[74]

For a contract to be rendered unconscionable, the party opposing the contract is required to show both procedural and substantive unconscionability.[75] However, California employs a "sliding scale" test, meaning that "the more substantively oppressive the contract term, the less evidence of procedural unconscionability is required to come to the conclusion that the term is unenforceable."[76]

---

72. *See, e.g.*, A & M Produce Co. v. FMC Corp., 135 Cal. App. 3d 473, 486 (4th Cir. 1982); Stirlen v. Supercuts, Inc., 51 Cal. App. 4th 1519, 1542 (Cal. App. 4th 1997*);* Dean Witter Reynolds v. Superior Court, 211 Cal. App. 3d 758, 767 (Cal. App. 3d 1989).

73. Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965).

74. Sonic-Calabasas A, Inc. v. Moreno, 57 Cal. 4th 1109, 1133 (Cal. 2013); *see also* Baltazar v. Forever 21, Inc., 62 Cal. 4th 1237, 1233 (Cal. 2016); *A & M Produce Co.*, 135 Cal. App. 3d at 486.

75. *See* MATTHEW BENDER, CALIFORNIA CONTRACT LITIGATION, CH. 18, 18.15[3] (LEXIS 2016).

76. Armendariz v. Foundation Health Psychcare Services Inc., 24 Cal. 4th 83, 114 (Cal. 2000); *see also* Carboni v. Arropside, 2 Cal. App. 4th 76, 86 (Cal. Ct. App. 1991) (citing West v. Henderson, 227 Cal. App. 3d 1578, 1588 (Cal. App. 3d. 1991) (lending support to the fact that several California courts have acknowledged that "a compelling showing of substantive unconscionability may overcome a weaker showing of procedural unconscionability").

Pursuant to the California Civil Code, to properly assert this defense a contract or provision must "have been unconscionable at the time it was made."[77] In determining whether a contract or term is unconscionable, the "basic test is whether, in the light of the general commercial background and the commercial needs of the particular trade or case, the clauses involved are so one-sided as to be unconscionable under the circumstances existing at the time of the making of the contract."[78] Although unconscionability is more frequently litigated in situations where a contract contains an arbitration clause,[79] California courts have noted that the "unconscionability standard is, as it must be, the same for arbitration and nonarbitration agreements."[80]

In the commentary to California's unconscionability statute, the California Civil Code specifies that "[s]ection 1670.5 is intended to make it possible for the courts to police explicitly against the contracts or clauses which they find to be unconscionable."[81] Accordingly, California courts are seemingly both empowered and constrained by the lack of a precise definition of unconscionability, as they have free rein to define and apply the doctrine of unconscionability on a case-by-case context as they see fit, but are tasked with doing so without the assistance of formally defined rules and definitions.[82]

B. The Standard for Procedural Unconscionability

Procedural unconscionability is focused on "the manner in which the contract was negotiated and the circumstances of the parties at that time."[83] Specifically, this prong of the unconscionability doctrine is focused on the

77. Cal. Civ. Code § 1670.5(a) (2016).

78. *Id*. at cmt. 1.

79. *See generally*, Graham v. Scissor-Tail, Inc., 28 Cal. 3d 807 (Cal. 1981) (holding that a contract containing a mandatory arbitration clause was not unconscionable because it was within the plaintiff's reasonable expectations); Flores v. Transamerica HomeFirst, Inc., 93 Cal. App. 4th 846 (Cal. App. 4th 2001) (holding it unconscionable to include a mandatory arbitration clause in adhesion contract that is offered to consumers on a take-it-or-leave it basis).

80. Loewen v. Lyft, Inc., 129 F. Supp. 3d 945, 953 (N.D. Cal. 2015).

81. Cal. Civ. Code § 1670.5 cmt. 1 (2016) (comment 1 continues by explaining that "[i]n the past such policing has been accomplished by adverse construction of language, by manipulation of the rules of offer and acceptance or by determinations that the clause is contrary to public policy or to the dominant purpose of the contract.").

82. *See, e.g.*, Lewis A. Kornhauser, *Unconscionability in Standard Forms*, 64 CAL. L. REV. 1151, 1156 (1976), http://scholarship.law.berkeley.edu/californialawreview/vol64/iss5/2 [https://perma.cc/9C4S-THSQ] ("[t]he legal concept of unconscionability should be expanded"); *see also* Lyra Haas, *The Endless Battleground: California's Continued Opposition To The Supreme Court's Federal Arbitration Act Jurisprudence*, 94 B.U. L. REV. 1419, 1420, 1452 (2014), http://www.bu.edu/bulawreview/files/2014/08/HAAS.pdf [https://perma.cc/86K2-36AT] ("California courts have . . . *demonstrate[ed] a tendency to interpret each possible exception broadly and each power narrowly, pursuing every line of reasoning until cut off by contradictory Supreme Court jurisprudence* . . . the [California Supreme Court] still considers unconscionability a valid argument.") (emphasis added).

83. Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1179 (E.D. Mo. 2004).

elements of "oppression and surprise."[84] Additionally, several California courts have found that the "use of a contract of adhesion establishes a minimal degree of procedural unconscionability . . .".[85] In making this latter determination, courts consider whether there was an absence of real negotiation and "an absence of meaningful choice,"[86] as well as "the extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms."[87] The elements used by courts to determine the existence of procedural unconscionability in a contract are discussed respectively below.

1. First Consideration: Facebook's Terms of Service and Data Policy Constitute an Adhesion Contract

Several California courts have held that "[a] finding of a contract of adhesion is essentially a finding of procedural unconscionability."[88] Because the "[u]nconscionability analysis begins with an inquiry into whether the contract is one of adhesion,"[89] determining that Facebook's Terms of Service and Data Policy constitute an adhesion contract is fundamental to explaining why courts should find these agreements to be unconscionable under California law.

An adhesion contract is presented by way of a standardized agreement: a party with "superior bargaining strength"[90] prepares and presents the terms of the contract to the other party, who can then either accept or reject the terms.[91] Simplified, contracts offered on a take-it-or-leave-it basis are referred to as adhesion contracts, and consumers are given two choices: complete adherence or complete rejection.[92] Adhesion contacts offer advantages, such as simplifying business operations, increasing efficiency, and reducing expenses.[93] In fact, it can be said that these types of agreements "appear to be a necessary concomitant of a sophisticated, mass-consumption economy."[94] Although standardized agreements have become increasingly commonplace

84. *A & M Produce Co.*, 135 Cal. App. 3d at 486; Cal. Civ. Code § 1670.5 cmt. 1 (2016).
85. BENDER, *supra* note 75, at 18.15[4][a].
86. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (quoting Williams, 350 F.2d at 449).
87. *Id*. (citation omitted).
88. Nagrampa v. MailCoups, Inc., 469 F.3d 1257, 1281 (9th Cir. 2006) (quoting *Flores*, 93 Cal. App. 4th at 853; *see* also Circuit City Stores, Inc. v. Adams, 279 F.3d 889, 893 (9th Cir. 2002).
89. *Armendariz*, 24 Cal. 4th at 113 (citing *Graham*, 28 Cal. 3d at 817–19)).
90. Graham, 28 Cal. 3d at 817.
91. *See* E. ALLEN FARNSWORTH, CONTRACTS, ASPEN PUBLISHERS, 286 (4th ed. 2004).
92. *Id*.
93. *Id*. at 285.
94. Richard Sybert, *Adhesion Theory in California: A Suggested Redefinition and its Application to Banking*, 11 LOYOLA L.A. L. REV. 297, 298 (1978), http://digitalcommons.lmu.edu/llr/vol11/iss2/8 [https://perma.cc/2D5N-G6N3].

in society today,[95] and despite carrying with them certain benefits,[96] "[d]angers are inherent in standardization."[97]

A determination that Facebook's Terms of Service and Data Policy constitutes an adhesion contract is only the beginning of the inquiry, because "[t]o describe a contract as adhesive in character is not to indicate its legal effect."[98] Rather, an adhesion contract is presumptively deemed to be enforceable in California[99] "unless certain other factors are present which, under established legal rules – legislative or judicial -- operate to render it otherwise."[100]

As set forth in the Restatement Second of Contracts, the "more standardized the agreement and the less a party may bargain meaningfully, the more susceptible the contract or a term will be to a claim of unconscionability."[101] Significantly, although "new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract."[102] Of the many well-established principles in contract law, "[m]utual manifestation of assent, whether by written or spoken word or by conduct, is the touchstone of contract."[103]

When creating a Facebook account, prospective users are prompted to fill in their first and last name, mobile number or email, password, date of birth, and gender.[104] A small message sits above the sizable green "Create Account" button, reading: "By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any

---

95. *See, e.g.*, Neal v. State Farm Ins. Co., 188 Cal. App. 2d 690, 694 (Cal. Ct. App. 1961) ("[T]oday, the impact of these standardized contracts can hardly be exaggerated Most contracts which govern our daily lives are of a standardised character."); Sybert, *supra* note 94 ("The individual's contractual relations and the incidents of daily life are defined by standardized agreements presented to him or her as faits accomplish.").

96. *See Graham*, 28 Cal. 3d at 818, n.15 (citing Richard Sybert, *Adhesion Theory in California: A Suggested Redefinition and its Application to Banking*, 11 LOYOLA L.A.L. REV. 297, 297–98) (acknowledging the benefits to standardized contracts: "Through advance knowledge on the part of the enterprise offering the contract that its relationship with each individual consumer or offeree will be uniform, standard and fixed, the device of form contracts introduces a degree of efficiency, simplicity, and stability. When such contracts are used widely, the savings in cost and energy can be substantial. An additional benefit is that the goods and services which are covered by these contracts are put within the reach of the general public, whose sheer size might prohibit widespread distribution if the necessary contractual relationships had to be individualized. Transactional costs, and therefore the possible prices of these goods and services, are reduced. In short, form contracts appear to be a necessary concomitant of a sophisticated, mass-consumption economy. They have social and economic utility").

97. FARNSWORTH, *supra* note 91, at 286.

98. *See Graham*, 28 Cal. 3d at 819.

99. *Id*. at 819–20.

100. *Id*. at 820.

101. RESTATEMENT (SECOND) OF CONTRACTS §208 cmt. a (Am. Law. Inst. 1981).

102. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004).

103. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 29 (2d Cir. 2002).

104. *See generally Home*, FACEBOOK, https://www.facebook.com/ [https://perma.cc/RFR9-X7DR] (accessed Apr. 4, 2017).

time."[105] Users then have the opportunity to click and read Facebook's hyperlinked Terms of Service and Data Policy before consenting to the entirety of the company's legally binding terms.[106] At this point, the prospective user must choose either to wholly accept Facebook's Terms of Service and Data Policy or forego an account altogether.[107] Because the company compels users to "unambiguously manifest either assent or rejection prior to being given access to the product,"[108] Facebook's Terms of Service and Data Policy should therefore be viewed as establishing the necessary element of procedural unconscionability.

However, it is important to note that California courts have rejected arguments of procedural unconscionability in adhesion contracts where the complaining party has a reasonable market alternative.[109] Additionally, the fact that a contract is one of adhesion does not automatically render it unconscionable, especially if there is no element of surprise included in the contract and its formation.[110] Each of these additional elements is discussed respectively below.

2. Second Consideration: Facebook's Terms of Service and Data Policy Are Imposed on Consumers in an Oppressive Manner

In a procedural unconscionability analysis, "'[o]ppression' arises from an inequality of bargaining power which results in no real negotiation and 'an absence of meaningful choice.'"[111] The inequality of bargaining power to the contract is best illustrated by *Ting v. AT&T*. In the case, AT&T mass mailed a Consumer Services Agreement ("CSA") containing a binding arbitration clause to over 60 million customers.[112] Prior to this mass mailing, AT&T issued a "market study [that] concluded that most customers 'would stop reading and discard the letter' after reading [a] disclaimer [stating]: . . . '[P]lease be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to

105. *Id.*

106. Referred to as the Statement of Rights and Responsibilities, users are told: "By using or accessing the Facebook Services, you agree to this Statement, as updated from time to time in accordance with Section 13 below." *Terms of Service*, FACEBOOK, (last revised Jan. 30, 2015), https://www.facebook.com/legal/terms [https://perma.cc/5YFP-9CEW] (accessed Apr. 4, 2017).

107. *Id*.

108. *Register.com, Inc.*, 356 F.3d at 429.

109. *Dean Witter Reynolds*, 211 Cal. App. 3d at 769–72 ("Even though a contract may be adhesive, the existence of 'meaningful' alternatives available to such contracting party in the form of other sources of supply tends to defeat any claim of unconscionability as to the contract in issue."); *Cf.* Gatton v. T-Mobile USA, Inc., 152 Cal. 4th 571, 585 (Cal. 4th 2007) (noting that the existence or availability of market alternatives does not preclude a finding that an adhesion contract is sufficient to establish some level of procedural unconscionability).

110. FARNSWORTH, *supra* note 91, at 302.

111. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (quoting *Williams*, 350 F.2d at 449).

112. *See* Ting v. AT&T, 319 F.3d 1126, 1133–34 (9th Cir. 2003).

do.'"[113] The agreement stated that customers would assent to the terms "by continuing to use or to pay for AT&T's service."[114] The *Ting* Court held the CSA to be procedurally unconscionable because "AT&T imposed the CSA on its customers without opportunity for negotiation, modification, or waiver" and "offered its terms on a take-it-or-leave-it basis."[115]

a. *Consumers Have an Indisputable Inequality in Bargaining Power*

In the same vein as *Ting*, Facebook users have no meaningful opportunity to negotiate with the company. If a Facebook user has even a single concern or reservation about a term included in the Terms of Service or Data Policy, that user's only option is to forego use of the platform entirely or otherwise succumb to each and every one of Facebook's terms.[116] As in *Ting*, solely considering the lack of bargaining power and the fact that Facebook offers its terms to users strictly on a take-it-or-leave-it basis, there is at least some element of procedural unconscionability present in Facebook's Terms of Service and Data Policy.[117]

b. *Consumers Have a Lack of Meaningful Choice In Controlling Their Biometric Data, Obtained Non-Consensually by Facebook*

The lack of meaningful choice for consumers with respect to the inclusion of facial recognition data in Facebook's Terms of Service and Data Policy is highlighted by the fact Facebook provides no publicly available information regarding how long the company will retain its users biometric identifiers.[118] More troubling is that Facebook offers neither instruction nor choice for users to permanently destroy any biometric identifiers collected by the company.[119] This lack of choice and bargaining power is imperative

113. *Id*. at 1134.

114. *Id*.

115. *Id*. at 1149.

116. *See Terms of Service*, *supra* note 106 ("By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any time", offering no alternative contact information for users concerned with the company's Terms and Data Policy).

117. *Id*.

118. *See* Patel v. Facebook, Inc., No. 1:15-CV-04265, 2015 WL 2265958, ¶ 20 (N.D. Ill. May 14, 2015) (discussing "Facebook's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of its users' biometric information").

119. Although users can elect to delete their Facebook accounts, there is a 14-day window before deletion takes effect. Moreover, in its Help Center, Facebook reserves the right to keep any account data for up to 90 days after deletion (https://www.facebook.com/help/125338004213029). For a more in-depth discussion on how Facebook has been criticized for making the deletion process deceptively difficult for users, *see generally* Glenn Stok, *Facebook's Deception of Deactivated Accounts*, TURBOFUTURE (last

because "[b]iometrics [] are biologically unique to the individual; therefore, once compromised, the individual has no recourse."[120] Even after a user manually opts-out of biometric data collection, Facebook still retains the previously collected data, regardless of whether or not the user consented to collection in the first place.[121] In fact, Facebook's full Data Policy states that even after a user deletes his or her account, the company "store[s] data for as long as it is necessary to provide products and services to [] others."[122] This clause offers neither precise information for users as to a retention timetable nor guidelines for permanent destruction of data.[123] The risk of harm here is that Facebook is already in the business of profiting off consumer data,[124] and with no meaningful choice for users to completely and unquestionably opt-out of biometric data collection, and no transparency as to if and when Facebook will truly remove such data, users are left in the dark.

Although Facebook states that a user can disable the Tag Suggestions feature and manually opt-out of being included in the facial recognition database, [125] this is somewhat misleading and easily susceptible to varying interpretations. On numerous occasions, Facebook has publicly announced that if a user disables tag suggestions, then despite "if a facial recognition template was created, it will be deleted," whether from tagged photos or profile pictures.[126] However, in Facebook's Help Center it states that "[w]hen

---

updated Mar. 26, 2017), https://turbofuture.com/internet/Obsolete-Facebook-Profile-Charade [https://perma.cc/RFM9-7PVJ].

120. *See* S. 95-2400, 2nd Sess., at 1 (Ill. 2008).

121. *See Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy [https://perma.cc/MJS4-8Y2W] (accessed Jan. 22, 2017); *see also Facial Recognition Hearing*, *supra* note 49, at 2 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

122. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ [https://perma.cc/4S7T-MCEM] (last modified Sept. 16, 2016).

123. Facebook is currently being sued by Illinois users under the Illinois Biometric Privacy Information Act in the U.S. District Court for the Northern District of California. The plaintiffs are alleging, among other claims, that the company failed to "provide a publicly available retention schedule and guidelines for permanently destroying the biometric identifiers of plaintiffs and the class (who do not opt-out of 'Tag Suggestions')". *See* In Re Facebook Biometric Information Privacy Litigation, Case No. 15-cv-03747-JD (N.D. Cal. 2016).

124. *See generally* Jason Kint, *Google and Facebook devour the ad and data pie. Scraps for everyone else*, DIGITAL CONTENT NEXT (June 16, 2016), https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/ [https://perma.cc/6Q75-8VYJ].

125. *See How does Facebook suggest tags?*, FACEBOOK HELP CENTER , https://www.facebook.com/help/122175507864081?helpref=faq_content [https://perma.cc/7SCS-DVAN] (last visited Apr. 3, 2017) ("If you remove a tag from a photo, that photo is not used to create the template for person whose tag was removed.").

126. *Facial Recognition Hearing*, *supra* note 49, at 29 (statement of Richard Sherman, Manager of Privacy & Public Policy at Facebook); *see also* Alexei Oreskovic, *Facebook may add your profile photo to facial recognition database*, NBC NEWS (Aug. 29, 2013 12:23 PM), http://www.nbcnews.com/technology/facebook-may-add-your-profile-photo-facial-recognition-database-8C11030921 [https://perma.cc/FUC7-LFAP] (noting that Facebook Chief Privacy Officer Erin Egan "stressed that Facebook users uncomfortable with facial recognition technology will still be able to 'opt out' of the Tag Suggest feature altogether, in

you're tagged in a photo, or make a photo your profile picture, we associate the tags with your account, compare what these photos have in common and store a summary of this comparison," offering no indication or guarantee that any associated facial recognition data obtained from the user's profile pictures will subsequently be deleted after a user disables Tag Suggestions.[127] In fact, it seems that disabling Tag Suggestion simply removes the option for Facebook to suggest that one user tags another user in a photo. Ultimately, even if a user turns off Tag Suggestions, Facebook may still retain a summary template of that user's facial data from his or her pictures.[128] As such, users have no choice regarding if or how Facebook stores their biometric data: users simply have to sign away their right to control their biometric data or forego using the platform altogether.

Perhaps more troubling is that Facebook began collecting face prints prior to obtaining explicit consent from its users to do so, meaning that users were never initially given a choice on whether or not they wanted Facebook to start collecting their face prints. Facebook began collecting data from user-uploaded photographs in order to develop its robust facial recognition data library without knowledge or consent from its billion-plus account holders.[129] After initially announcing the creation of Tag Suggestions, Facebook hastily publicized that the feature had actually already been deployed both domestically and internationally, absent any notice or consent from its users.[130] Only after coming under fire did Facebook admit that it "should have been more clear with people during the roll-out process when this became available to them."[131] Simply put, not only were users blatantly unaware that Facebook was going to begin using facial recognition technology, but users had no meaningful choice to affirmatively opt-out of this invasive biometric data collection, because Facebook automatically opted-in all users.[132] Thus,

---

which case the person's public profile photo would not be included in the facial recognition database.").

127. *See generally* FACEBOOK HELP CENTER, https://www.facebook.com/help/218540514842030?helpref=faq_content [https://perma.cc/R6Z5-Q93K]; *See also How does Facebook suggest tags?*, FACEBOOK, https://www.facebook.com/help/122175507864081?helpref=faq_content [https://perma.cc/8P2K-H9M2] (accessed Apr. 3, 2017).

128. *Id*.; *see also* Lynch, *supra* note 10, at 10 ("even if a user deletes the summary data, it is unclear whether taking this step will prevent Facebook from continuing to collect biometric data going forward.").

129. *See* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission, 10–11 (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/6BAU-NKM7].

130. *Id*. at 10 (citation omitted).

131. *See* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission, 11 (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/6BAU-NKM7].

132. *Facial Recognition Hearing*, *supra* note 49, at 2 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

without notice, Facebook automatically enabled the facial recognition feature to its unsuspecting, non-consenting 500 million users in 2011.[133]

Facebook's lack of notice and transparency regarding its stealth and non-consensual deployment of facial recognition technology became the focal point of a 2012 Senate Subcommittee on Privacy, Technology and the Law hearing, in which Senator Al Franken asked Facebook's Privacy and Policy Manager the obvious question: "How can users make an informed decision about facial recognition in their privacy settings if you don't actually tell them that you are using facial recognition?"[134] Further, when asked whether the company would ever sell its facial recognition data and information to third parties, Facebook's Privacy and Policy Manager offered no guarantees, eerily remarking that "[i]t's difficult to know what Facebook will look like five or 10 years down the line, so it's hard to respond to that."[135] Yet six years later, in 2018, Facebook is still programmed to automatically opt-in users to its biometric data collection upon sign-up, absent any notice of this practice in the company's Terms of Service and Data Policy. Considering the above factors, courts should view the unreasonable lack of meaningful choice for consumers with respect to Facebook's biometric data collection practices as supporting evidence in finding procedural unconscionability.

c. *Practically Speaking, No Other Social Media Platforms Are Comparable as a Meaningful Alternative to Facebook*

It is true that some California courts have held that "[t]here can be no oppression establishing procedural unconscionability, even assuming unequal bargaining power and an adhesion contract, when the customer has meaningful choices."[136] But in this day and age, from a purely statistical standpoint, there really is not a meaningful alternative to Facebook. This is best evidenced by a 2016 Pew Research Center study that showed that Facebook is still the most popular and widely used social networking platform by a "substantial margin," with eight out of 10 Americans, or 79% of all Internet users, using the platform.[137] Instagram falls in second place, with a

133. *See* Charles Arthur, *Facebook in new privacy row over facial recognition feature*, THE GUARDIAN (June 8, 2011), https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition [https://perma.cc/56HN-2NPD].

134. Ricardo Bilton, *Facebook hit with tough questions on facial recognition in Senate hearing*, VENTUREBEAT (July 18, 2012), http://venturebeat.com/2012/07/18/facebook-hit-with-tough-questions-on-facial-recognition-in-senate-hearing/ [https://perma.cc/manage/create].

135. *Id*.

136. Wayne v. Staples, Inc., 135 Cal. App. 4th 466, 482 (Cal. App. 2d 2006); *see also Dean Witter Reynolds*, 211 Cal. App. 3d at 771.

137. *See* Shannon Greenwood, et al., *Social Media Update 2016*, PEW RESEARCH CENTER (Nov. 11, 2016), http://www.pewinternet.org/2016/11/11/social-media-update-2016/ [https://perma.cc/N6VM-BP6M].

mere 32% of Americans using the photo hosting platform.[138] The enormous disparity in users of each respective platform cannot be overstated, especially when comparing Facebook's 1.86 billion[139] daily active users to Instagram's 600 million[140] daily active users.

At first blush, it may seem as though Instagram provides a meaningful alternative to Facebook. However, Facebook actually owns its second-place rival Instagram. According to Instagram's Privacy Policy, the company has "collaborat[ed] with Facebook's team . . . to share insights and information with each other" since 2013.[141] In an effort to discern just how much information the two companies share, a reporter from The Wall Street Journal "created a fresh Instagram account with [her] work email and didn't sync it to Facebook . . . [finding that] 78 out of 100 [of Instagram's follower] recommendations were [her] Facebook friends."[142] This happened because "[e]ven when [users] don't upload [their] contacts directly to Instagram, the network uses information—or 'signals,' as Instagram calls them—from Facebook, which might include contacts or other tangential information."[143] Thus, even if consumers opted to use Instagram as an alternative to Facebook, Facebook would still be in total control of consumer information as the company "share[s] information about [consumers] within [its] family of companies."[144] For users seeking to distance themselves from Facebook's onerous Terms of Service and Data Policy, a Facebook-owned company simply cannot be considered a meaningful alternative to Facebook.

As such, a consumer hoping to stay socially engaged while bypassing Facebook's family of companies and their corresponding overreaching terms could turn to Twitter, the third most used social media site.[145] But with only 21% of the United States' adult population using Twitter, the application hardly stands as a meaningful alternative to Facebook.[146] In fact, it has been noted that "[p]opular digital monopolies, such as Google, Facebook, or Microsoft, *offer no free choice* compared to alternative services, which could be of inferior quality, be it because they are as yet under-developed or less

138. *Id*.

139. FACEBOOK, *supra* note 13.

140. *See generally* INSTAGRAM, http://blog.instagram.com/post/154506585127/161215-600million [https://perma.cc/B9NX-6AAS] (accessed Jan. 19, 2016).

141. *See generally* INSTAGRAM, https://help.instagram.com/155833707900388 [https://perma.cc/R6QH-XCXT] (accessed Feb. 13, 2018).

142. Katherine Bindley, *Instagram is Turning Into Facebook, And That's Bad*, WALL ST. J. (Feb. 13, 2018), https://www.wsj.com/articles/instagram-is-turning-into-facebook-and-thats-bad-1517422670.

143. *Id*.

144. *See generally The Facebook Companies*, FACEBOOK, https://www.facebook.com/help/111814505650678 [https://perma.cc/49NY-HEUK] (accessed Apr. 6, 2017).

145. Greenwood, et al., *supra* note 137.

146. *Id*.

innovative or be it that they are so because such services do not process significant data from their users."[147]

Aside from Facebook's proven and significant half-billion user advantage over its competitors, the demographics of Facebook's users bolster the argument that no other social networking platform provides a similar alternative to Facebook. To illustrate, studies have shown that 64% of all online Americans said the motivation for using social networking sites was to keep in touch with family members,[148] a sentiment that especially rings true for the baby boomer generation and beyond.[149] As such, it cannot be overlooked that while 62% of adults aged 65+ use Facebook, only a mere 8% of the 65+ population use Instagram.[150]

These numbers undoubtedly show that Facebook is the most commonly utilized social networking tool for Americans, ranging from teenagers to senior citizens. If social media is truly used to keep in touch with family members, then Facebook is the sole platform that makes this feasible. In other words, although there are a variety of other social networking platforms, none offer Facebook's cross-generational reach.

Of course, there is the argument that "if you don't like it, then don't use it."[151] However, for better or for worse, social media has engrained itself in

147. Anca D. Chirita, *The Rise of Big Data and the Loss of Privacy*, Durham Law School Research Paper, 10 (June 15, 2016), https://ssrn.com/abstract=2795992 [https://perma.cc/8QX4-N6MT] (emphasis added).

148. *See* Aaron Smith, *Why Americans use social media*, PEW RESEARCH CENTER (Nov. 15, 2011), http://www.pewinternet.org/2011/11/15/why-americans-use-social-media/ [https://perma.cc/K838-UJ84].

149. *See* Nora Krug, *Technology helping more baby-boomer grandparents stay plugged in to grandkids*, WASH. POST (Oct. 31, 2014) (accessed Jan. 19, 2016), https://www.washingtonpost.com/postlive/technology-helping-more-baby-boomer-grandparents-stay-plugged-in-to-grandkids/2014/10/31/3dda3c26-4ccb-11e4-aa5e-7153e466a02d_story.html?utm_term=.71c3d6bb6743 [https://perma.cc/JV8P-LZPN]. For example, Facebook provides a useful platform for families to stay in touch and for grandparents to be involved in the lives of their grandchildren. With the median household income in the U.S. clocking in at $56,516. *See* Bernadette D. Proctor et al., *Income and Poverty in the United States: 2015*, U.S. CENSUS BUREAU, Report Number: P60-256 (Sept. 13, 2016), http://www.census.gov/library/publications/2016/demo/p60-256.html) [https://perma.cc/4N7C-DGVZ], and average round-trip domestic airfare costs around roughly $400 per person (*see* U.S. Dep't of Transp., Bureau of Transportation Statistics (2015), https://www.rita.dot.gov/bts/airfares/programs/economics_and_finance/air_travel_price_index/html/AnnualFares.html [https://perma.cc/27PH-Y4QL]), traveling to see family and friends in other states can be costly and difficulty. In fact, a 2012 AARP study revealed that 67% of grandparents who reported infrequent visits with their grandchildren cited distance as the reason why (Cheryl L. Lampkin, PhD, *Insights and Spending Habits of Modern Grandparents*, AARP (Sept. 5, 2012), http://www.aarp.org/research/topics/life/info-2014/grandparenting-survey.html [https://perma.cc/JS6X-4G9G]).

150. Greenwood, et al., *supra* note 137.

151. *See, e.g.*, *"If you don't like it, don't use it. It's that simple." ORLY?*, SOCIAL MEDIA COLLECTIVE, (Aug. 11, 2011), https://socialmediacollective.org/2011/08/11/if-you-dont-like-it-dont-use-it-its-that-simple-orly/ [https://perma.cc/K5WV-WC8U] ("It's common, and easy, to say 'just don't use it.' There's actually a term for this– technology refusal– meaning people who strategically 'opt out' of using overwhelmingly prevalent technologies . . . [but] 'if you don't like it, don't use it' is not really simple at all.").

our society as a necessity of sorts, rapidly losing any semblance of voluntariness. [152] As indicated by the statistics above, there is arguably no meaningful alternative for consumers, as Facebook has taken a clear and decisive lead over its competitors.

This lack of meaningful choice was recognized as far back as 2010 in a New York Times article which stated: "In reality, quitting Facebook is much more problematic than the company's executives suggest, if only because users cannot extract all the intangible social capital they have generated on the site and export it elsewhere."[153] As a result, "many users find it too daunting to start afresh on a new site, so they quietly consent to Facebook's privacy bullying."[154]

The bare existence of other social media platforms does not satisfy the element of a meaningful alternative. It is well-established under California law that a "claim of procedural unconscionability cannot be defeated merely by 'any showing of competition in the marketplace as to the desired goods and services . . . ".[155] As the most utilized platform across the spectrum that is statistically and objectively proven to saturate the market, Facebook should not put its users in a position to make a value judgment between staying connected or sacrificing their privacy.

3. Third Consideration: By Explicitly Omitting Mention of Facial Recognition Technology in its Terms of Service and Data Policy, Facebook's Policies Contain a Surprise for Consumers

In a procedural unconscionability analysis, "surprise involves the extent to which the supposedly agreed-upon terms of the bargain are hidden in a

---

152. *See, e.g.*, Lynch, *supra* note 10, at 3 ("Americans cannot participate in society without exposing their faces to public view. Similarly, connecting with friends, family and the broader world through *social media has quickly become a daily (and some would say necessary) experience for Americans of all ages*") emphasis added; *see also* SOCIAL MEDIA COLLECTIVE, *supra* note 151 (the leading comment on this article from user Steve Boland reads: "I did leave Facebook in a self-righteous huff, having had enough of how they treat their customers. I took the 'Don't like Facebook? Leave Facebook.' approach. Then I came crawling back, six months later. I was socially isolated. It was too difficult to keep [up] with [] people when I couldn't be reached as easily as other family and friends. The cost of not participating in the free service was too high"); *see also* Nicole B. Ellison, et al., *The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites*, 12 Journal of Computer-Mediated Communication 1143, 1164 Mich. St. U. 2007 (http://www.michelepolak.com/200fall11/Weekly_Schedule_files/Ellison.pdf) [https://perma.cc/NDN8-3HET] (research study illustrating Facebook's edge in cultivating friendship, concluding that "Internet use alone did not predict social capital accumulation, but intensive use of Facebook did.").

153. Evgeny Morozov, *Surfing the Surfer*, NY Times (June 1, 2010), http://www.nytimes.com/2010/06/02/opinion/02iht-edmorozov.html [https://perma.cc/96ZV-9NY5].

154. *Id*.

155. Comb v. Paypal, Inc., 218 F. Supp. 2d 1165, 1173 (N.D. Cal. 2002) (quoting *Dean Witter Reynolds*, 211 Cal. App. 3d at 772.

prolix printed form drafted by the party seeking to enforce the disputed terms."[156] The element of surprise is generally focused on the terms included in the agreement at issue.[157] Nowhere in Facebook's Terms of Service or Data Policy is the phrase "facial recognition technology" explicitly used.[158] Yet, upon careful review, facial recognition data collection from photos is assumedly included under what Facebook refers to as "IP Content,"[159] termed by Facebook to include things "like photos and videos."[160] In other words, users would need to be specifically searching on Facebook's Help Center, which is wholly separate from the company's Terms of Service or Data Policy, to find any information about the company's use of facial recognition technology.[161] Yet when signing up for the platform, users are prompted that by signing up they "agree to [the] Terms and that [they] have read [Facebook's] Data Policy,"[162] neither of which include the term facial recognition nor a description of how Facebook collects and uses that technology.[163] The problem, then, is that users consent to the Terms of Service and Data Policy – not to the Help Center – meaning that they simply cannot agree to something that is not there.

By tactfully omitting the term "facial recognition technology" from its Terms of Service and Data Policy, Facebook is taking advantage of unsuspecting users who simply do not know what they do not know.[164] Considering that the element of surprise in an unconscionability determination concerns whether certain terms are concealed or buried within the contract,[165] the omission of any reference to facial recognition technology is wholly significant. Facebook did not merely hide its right to collect and use facial recognition data in a shuffle of other terms in hopes that its users would not read the Terms of Service and Data Policy. Rather, the company flat-out failed to include any reference to facial recognition technology in its Terms of Service and Data Policy – the two agreements to which users are required

156. *A & M Produce Co.*,135 Cal. App. 3d at 486.

157. *Id*.

158. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122.

159. *Id*.

160. *Id*.

161. *See* https://www.facebook.com/help/122175507864081?helpref=faq_content for the lone search result for "facial recognition" on Facebook's Help Center (accessed Apr. 4, 2017).

162. Facebook home page, https://www.facebook.com/ (accessed Apr. 4, 2017).

163. *Id*.

164. *See* Yasamine Hashemi, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability,* 15 B.U. J SCI & TECH L. REV. 140, 158 (2009), https://www.bu.edu/jostl/files/2015/02/Hashemi_WEB_151.pdf (noting that "[t]here is evidence that most Facebook members do not read these documents in the first place . . . [which] could support an argument that they are unduly long and confusing, or that there is no possibility that they could bargain with Facebook to change the language into terms that are more member-friendly. This would support a finding of procedural unconscionability."). The author makes a strong argument that a user's failure to read Facebook's excessively lengthy terms could support a finding of procedural unconscionability.

165. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (citing M.P. Ellinghaus, *In Defense of Unconscionability* 78 YALE L.J. 757, 764–765 (1969)).

to assent in order to use the platform.[166] As such, even if users read the entirety of Facebook's terms and policies, there is no explicit information on facial recognition technology to which users can even contemplate consenting.[167]

Another surprise term is found in Facebook's Terms of Service, outlining that users grant to the company "a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content" posted "on or in connection with Facebook."[168] Essentially, this clause in the Terms of Service allows Facebook, carte blanche, to collect, use, and share any and all content at the company's discretion, without any payment or notice of such use or distribution to the impacted users.[169] In practice, not only does Facebook fail to offer adequate notice to its users upon sign-up about the company's facial recognition practices, but Facebook then reserves for itself the an explicit license to any biometric data subsequently collected for an undetermined and undisclosed period of time.[170]

With this in mind, California courts should find the exclusion of facial recognition terminology in the Terms of Service and Data Policy, coupled with the company's exclusive license to use such data, as a contractual surprise, thereby making any use and licensure of biometric data unconscionable and subsequently void.

---

166. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122 (providing no terminology or explanation regarding the company's practice of collecting and using facial recognition technology).

167. As of February 27, 2018, Facebook began issuing pop-up notices to some, not all, of its *existing* users, in which it described in very little detail the company's facial recognition practices. *See* Russell Brandom, *Facebook is starting to tell more users about facial recognition*, THE VERGE (Feb. 27, 2018), https://www.theverge.com/2018/2/27/17058268/facebook-facial-recognition-notification-opt-out. However, at the time of this note publication, Facebook still explicitly excludes any mention of facial recognition technology in its Terms of Service and Data Policy for *prospective* users. As a result, a prospective user would sign-up for Facebook with no notice of the company's facial recognition practices, and would subsequently be opted-in to Facebook's biometric data collection. Due to the sensitive nature of biometric data, it is simply not enough for Facebook to only notify *some* of its *existing* users about this technology: Facebook needs to provide explicit notice to its *prospective* users as well in either its Terms of Service or Data Policy.

168. *Terms of Service*, *supra* note 106.

169. *See* Oliver Smith, *Facebook terms and conditions: why you don't own your online life*, THE DAILY TELEGRAPH (Jan. 4, 2013), http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html ("Specifically for photos and video uploaded to the site, Facebook has a license to use your content in any way it sees fit, with a license that goes beyond merely covering the operation of the service in its current form. Facebook can transfer or sub-license its rights over a user's content to another company or organization if needed. Facebook's license does not end upon the deactivation or deletion of a user's account, content is only released from this license once all other users that have interacted with the content have also broken their ties with it.").

170. *See* Lynch, *supra* note 10, at 11 ("All of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large.").

a. *Merging Surprise with Failure to Read – How to Remedy and Address This Counterargument*

An important consideration is whether a user's failure to read terms and policies should be taken into consideration when asserting the defense of unconscionability.[171] The California Supreme Court has rejected "[t]he suggestion that a contract or clause cannot be unconscionable if it is accepted by a knowledgeable party."[172] Indeed, although there is commonly a duty and expectation to read a contract before assenting to it, California courts have recognized that "no authority is cited for a supposed rule that if a party reads an agreement he or she is barred from claiming it is unconscionable," adding that "[s]uch a rule would seriously undermine the unconscionability defense."[173]

Although, generally speaking, "'one who signs an instrument may not avoid the impact of its terms on the ground that he failed to read the instrument before signing it,'"[174] this general rule is applicable "only in the absence of 'overreaching'[175] or 'imposition.'"[176] In fact, failure to read a contract is actually deemed to be helpful in establishing "actual surprise."[177]

With respect to whether sufficient consent was given by a user who may or may not have read the terms, one expert in the area has said "[o]ne of the issues will be whether the consent was obtained under circumstances where people understand what they're agreeing to . . . [h]ow many times have you clicked through 'I consent' licenses on software and Web sites? I write those for a living, and I don't read them."[178] But even if a diligent user were to read the entirety of Facebook's terms and policies, there is no explicit information on facial recognition technology included therein to which the user could contemplate consenting.[179]

By failing to mention its use of facial recognition technology in its Terms of Service and Data Policy to prospective users, Facebook is collecting

---

171. For better or for worse, it is widely regarded that consumers often neither read nor understand the terms included in adhesion contracts. Instead, consumers misguidedly "trust to the good faith of the party using the form and to the tacit representation that like terms are being accepted regularly by others similarly situated." RESTATEMENT (SECOND) OF CONTRACTS, §211 cmt.b (Am. Law. Inst. 1981).

172. *Stirlen*, 51 Cal. App. 4th at 1534.

173. Higgins v. Superior Court, 140 Cal.App. 4th 1238, 1251 (Cal. App. 4th 2006).

174. Bruni v. Didion, 160 Cal. App. 4th 1272, 1291 (Cal. App. 4th 2008) (citation omitted).

175. *Bruni*, 160 Cal. App. 4th at 1291 (quoting Stewart v. Preston Pipeline Inc., 134 Cal.App. 4th 1565, 1588 (Cal. App. 4th 2005)).

176. *Bruni*, 160 Cal. App. 4th at 1291(quoting Jefferson v. Dep't of Youth Auth., 28 Cal. 4th 299, 303 (Cal. App. 4th 2002)).

177. *See Bruni*, 160 Cal. App. 4th at 1291 (quoting Patterson v. ITT Consumer Fin. Corp., 14 Cal.App. 4th 1659, 1666 (Cal. App. 4th 1993).

178. Caroline McCarthy, *Legally, are Facebook's Social ads Kosher?*, CNET NEWS (Nov. 15, 2007, 8:17 PM), http://www.news.com/8301-13577_3-9817421-36.html (quoting Brian Murphy, a partner at Frankfurt Kurnit Klein & Selz specializing in intellectual property issues and content licensure).

179. *See Terms of Service*, *supra* note 106.

biometric data wholly without consent.[180] This matters because "[f]acial recognition is one of those categories of data where a very prominent and a very clear consent is necessary."[181] Users cannot agree to something that is neither mentioned nor included in the terms presented, and in the case of Facebook's Terms of Service and Data policies, it is inconsequential whether or not a user reads or fails to read the terms and provisions because there is simply no mention of facial recognition technology whatsoever. The most careful reader would be unable to find mention of the term, meaning that there simply cannot be a failure to read when there is nothing in question to be read.[182]

Considering the adhesive nature of the contract, the unequal bargaining positions, the lack of meaningful choice, and the surprise, hidden contractual terms, it would be prudent for California courts to follow precedent and find that there is a sufficient showing of procedural unconscionability in Facebook's Terms of Service and Data Policy. The analysis would then turn to whether substantive unconscionability is also present.

C. The Standard for Substantive Unconscionability

Unlike procedural unconscionability, "[s]ubstantive unconscionability is less easily explained."[183] Substantive unconscionability often refers to an "allocation of risks or costs which is overly harsh or one-sided and is not justified by the circumstances in which the contract was made."[184] California courts are split as to the standard for substantive unconscionability: some require that substantive unconscionability rise to a level that "shock[s] the

180. Lynch, *supra* note 10, at 10 ("[I]t turned these features on by default. It first enrolled all its users in the system without prior consent and then continued to opt-in users every time they uploaded a photograph.").

181. Rachel Adams-Heard, *Facebook's Facial Recognition Software Draws Privacy Complaints*, *Lawsuit*, INSURANCE JOURNAL (July 30, 2015), http://www.insurancejournal.com/news/national/2015/07/30/376972.htm [https://perma.cc/6S9J-ZAZY] (quoting Alvaro Bedoya, executive director of Georgetown University's Center on Privacy & Technology).

182. Failure to read presents an interesting policy and moral question for California courts: should consumers be held liable for unconscionable adhesion contracts that they failed to read in full? In pondering this question, it is imperative to consider a July 2016 study which showed that, for the most part, users simply do not read Terms of Service Agreements and Privacy Policies. The experiment created a fictional social networking service and asked participants to read the Terms of Service Agreement and Privacy Policy. Aside from sharing all user data with the National Security Agency ("NSA") and the participant's employers, one of the clauses in the Terms of Service provided that participants would deliver their first-born child as payment for access to the social networking service. This sacrificial-child clause went unnoticed by 98% of the study's participants, with only 1.7% of the participants noticing and raising a concern with the clause. Jonathan A. Obar & Anne Oledorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, (Aug. 24, 2016), http://dx.doi.org/10.2139/ssrn.2757465.

183. *Stirlen*, 51 Cal. App. 4th at 1532.

184. Cal. Civ. Code § 1670.5 n.2 (2016); *see also A & M Produce Co.*, 135 Cal. App. 3d at 486; *Armendariz*, 24 Cal. 4th at 114.

conscience,"[185] while others require a less onerous showing of failure to act in "good faith and fair dealing."[186] Regardless, it is well-accepted that "a contractual term is substantively suspect if it reallocates the risks of the bargain in an objectively unreasonable or unexpected manner."[187]

In assessing substantive unconscionability, California courts often consider whether the contractual terms at issue "contravene the public interest or public policy,"[188] whether the questionable terms are included in the contract in "fine print,"[189] and whether the terms "seek to negate the reasonable expectations of the nondrafting party."[190] The Legislative Committee Comments to the California Civil Code on unconscionability state that courts can "police explicitly against the contracts or clauses which they find to be unconscionable" by examining whether the "clause is contrary to public policy or to the dominant purpose of the contract."[191]

Important to note, a showing of substantive unconscionability "requires a substantial degree of unfairness beyond 'a simple old-fashioned bad bargain.'"[192]

It is well understood by California courts that "[n]ot all one-sided contract provisions are unconscionable; hence the various intensifiers in [the California court] formulations: '*overly* harsh,' '*unduly* oppressive,' '*unreasonably* favorable.'"[193] As such, "[a] contract term is not substantively unconscionable when it merely gives one side a greater benefit."[194] Accordingly, as articulated in *Stirlen v. Supercuts, Inc.*, "a contract can provide a 'margin of safety' that provides the party with superior bargaining strength a type of extra protection for which it has a legitimate commercial need without being unconscionable." However, the *Stirlen* court clarified that "unless the 'business realities' that create the special need for such an advantage are explained in the contract itself [] [then] it must be factually established."[195]

185. *See* California Grocers Ass'n. v. Bank of Am., 22 Cal. App. 4th 205, 215 (Cal. Ct. App. 1994).

186. *See* Donovan v. Rrl Corp., 26 Cal. 4th 261, 290–91 (Cal. 2001).

187. *Stirlen*, 51 Cal. App. 4th at 1532.

188. *Loewen*, 129 F.Supp.3d at 952.

189. *Id*.

190. *Id*.

191. Cal. Civ. Code § 1670.5 commentary (2016).

192. Sonic-Calabasas A, Inc. v. Moreno, 57 Cal. 4th 1109, 1160 (Cal. 2013) (citation omitted).

193. Sanchez v. Valencia Holding Co., LLC, 61 Cal. 4th 899, 911 (Cal. 2015).

194. *Id*. (quoting Pinnacle Museum Tower Ass'n. v. Pinnacle Market Dev. (US), LLC, 55 Cal. 4th 223, 246 (Cal. 2012).

195. *Stirlen*, 51 Cal. App. 4th at 1536.

1. First Consideration: Facebook's Terms of Service and Data Policy Are Against California Public Policy and the Public Interest

Szetela v. Discover Bank provides the best illustration of a court deeming a contract term to be unconscionable due its contravention of established public policy. In the case, the court found a banking contract containing an adhesive arbitration provision to be substantively unconscionable because it "violate[d] public policy by granting Discover a 'get out of jail free' card while compromising important consumer rights."[196] The court reasoned that Discover had "essentially granted itself a license to push the boundaries of good business practices to their furthest limits, fully aware that relatively few, if any, customers will seek legal remedies, and that any remedies obtained will only pertain to that single customer without collateral estoppel effect."[197] In turn, the court found that the overwhelming advantages that the adhesive arbitration provision imparted on Discover contradicted "the California Legislature's stated policy of discouraging unfair and unlawful business practices."[198]

Facebook's non-consensual biometric data collection practices run afoul of Article I, Section I of the California Constitution, which prescribes an "inalienable right to privacy."[199] When California residents voted in 1972 to amend the state constitution to include an inalienable right to privacy, "the moving force behind the new constitutional provision was a more [focused] privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[200]

The same pamphlet enticed voters to support the privacy amendment by noting that "[f]undamental to [consumer] privacy is the ability to control circulation of personal information . . . [t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them."[201] These promises of privacy and the fears of simultaneous corporate and government overreaching are what charged California voters to amend their state constitution to explicitly include an inalienable right to privacy, a strong showing in favor of this highly important public policy.[202]

---

196. Szetela v. Discover Bank, 97 Cal. App. 4th 1094, 1101 (Cal. App. 4th 2002).
197. *Id*.
198. *Id*.
199. CAL. CONST. ART. I § 1.
200. White v. Davis, 13 Cal. 3d 757, 774 (Cal. 1975).
201. *Id*.
202. *Id*. (yet 42 years later, the driving factor behind the amendment remains true: "[a]t present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian").

If the privacy amendment was included to mitigate intrusive government data collection, as expressly recognized by the California Supreme Court,[203] then California courts need to take into account that over a mere six month period, Facebook complied with nearly 85% of domestic law enforcement requests for user data.[204] In fact, in a public-private surveillance quid pro quo of sorts, the government and Facebook have long worked together in pursuance of their respective agendas.[205] For example, where the U.S. Constitution may preclude the government from certain domestic surveillance measures, Facebook can supplement those deficiencies with datasets on its billion-plus users.[206] Similarly, where burdensome red-tape and regulations could limit the social media company's seemingly indomitable growth, the government can act to pave the way and knock down roadblocks standing in Facebook's way.[207]

This "you scratch my back, I'll scratch yours" partnership is facilitated by Facebook's Data Policy, which carves out a subjective standard for sharing user data with the government and law enforcement agencies.[208] By its very terms, Facebook's loose standard for deciding whether to access and share user data in response to a warrant, subpoena or other legal request is grounded in whether the company has "a good faith belief that the law requires [it] to do so."[209] Despite the fact that Facebook requires the government and law enforcement agencies to obtain a valid subpoena, search warrant, court order, or national security letter when seeking user data,[210] inclusion of the "good faith belief" catch-all significantly dismantles any purported legal privacy protections for Facebook users. "Good faith" is hardly a legal standard to which consumers or courts can look for sufficient clarity and guidance, and it does not adequately protect consumers' inalienable right to privacy as guaranteed by the California Constitution. Given the background behind

---

203. *See White*, 13 Cal. 3d at 761.

204. *See* FACEBOOK, Gov't Request Rep., https://govtrequests.facebook.com/country/United%20States/2016-H2/ (accessed July 27, 2017).

205. *Cf.* Bruce Schneier, *Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong*, THE ATLANTIC (Mar. 25, 2014), https://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/ and Cory Bennett, *Facebook accused of 'secretly lobbying' for cyber bill*, THE HILL (Oct. 26, 2015), http://thehill.com/policy/cybersecurity/258060-advocate-accuses-facebook-of-secretly-lobbying-for-cyber-bill (conflicting reports on whether Facebook lobbied Congress in support of the Cybersecurity Information Sharing Act (CISA), legislation which would have incentivized private companies to share data with the U.S. government on potential hacking threats).

206. *See* Bruce Schneier, The Public/Private Surveillance Partnership, Schneier on Security (Aug. 5, 2013), https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html.

207. *Id*. ("Corporations rely on the government to ensure that they have unfettered use of the data they collect.").

208. *Data Policy*, *supra* note 122.

209. *Id*.

210. *See* FACEBOOK, Law Enforcement Guidelines, https://www.facebook.com/safety/groups/law/guidelines/ (accessed July 10, 2017).

Article I, Section I, California courts need to recognize that Facebook's Terms of Service and Data Policy deliberately and utterly take away the rights of consumers to control the collection and dissemination of their biometric data.

2. Second Consideration: Facebook's Terms of Service and Data Policy Impose an Unreasonable and Unexpected Allocation of Risk

The overly harsh allocation of risk in Facebook's policies falls squarely on the back of consumers. Facebook reaps the overwhelming advantages of its collection of users biometric identifiers despite the company's Data Policy and Terms of Service being "unreasonably favorable to the more powerful party."[211] For example, Facebook's Data Policy states that the company can share user information within its 11 other Facebook-owned companies,[212] as well as any applications, websites and any third-party integrations on or using Facebook.[213] Facebook further states that "[i]f the ownership or control of all or part of our Services or their assets changes, [the company] may transfer your information to the new owner."[214] Even if a user simply deletes a photograph from his or her account, Facebook's Terms of Service states that any "removed content may persist in backup copies for a reasonable period of time (but will not be available to others)."[215] However, this provision conveniently seems to reason that users are only worried about other users having access to their removed content, rather than Facebook retaining the licensed right to use, distribute or sell any deleted user data to any entity or individual that Facebook so chooses.[216] But this conclusion is in contradiction with the summary findings below in Figure B, which demonstrate that, as a whole, consumers are more worried about how companies are collecting, distributing, and sharing their personal data.[217]

In fact, this 2015 study showed that the top two consumer privacy concerns are where and to whom data is sold and where data is kept.[218] Yet, despite such pervasive consumer privacy concerns, Facebook's Terms of Service and Data Policy artfully includes ambiguous phrases like "as long as" and "for a reasonable period" that essentially grant to the company

211. *See Loewen*, 129 F.Supp.3d at 952 (citing 8 Williston on Contracts (4th ed.2010) § 18.10, p. 91).

212. For a full list of Facebook's 11 owned companies, *see* FACEBOOK, https://www.facebook.com/help/111814505650678 (accessed Apr. 2, 2017).

213. *Data Policy*, *supra* note 122.

214. *Id*.

215. *Terms of Service*, *supra* note 106.

216. *See* Chirita, *supra* note 147, at 3 (noting that "personal data, which is economically relevant, could be misused, for instance, through it being shared with third parties, in order to maintain or strengthen a dominant market position").

217. *See* Stacey Higginbotham, *Companies need to share how they use our data. Here are some ideas*, FORTUNE MAGAZINE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy/ (citing Jessica Groopman, *Consumer Perceptions of Privacy in the Internet of Things*, ALTIMETER GROUP (2015), http://go.pardot.com/l/69102/2015-07-12/pxzlm).

218. *Id.*

indisputable and unbounded access to all user data, leaving users in the dark as to who has their information and who might get it next.[219] All things considered, a court would not be hard-pressed in finding that Facebook's Terms of Service and Data Policy contain unreasonably favorable terms for the company.

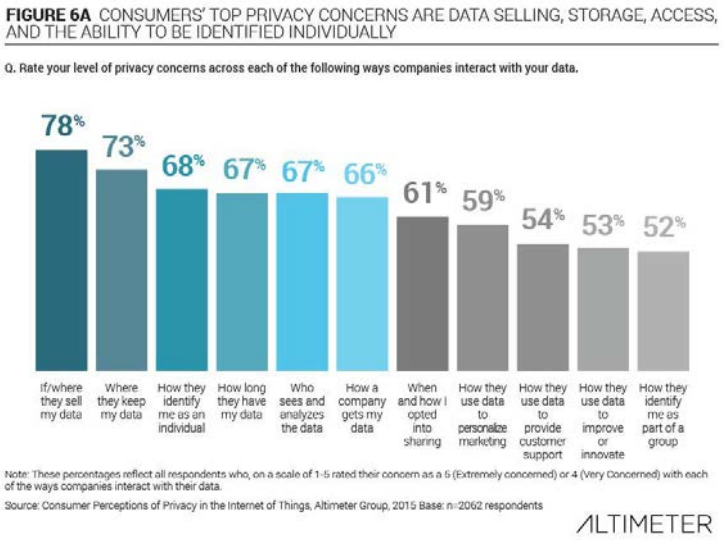

Figure B [220]

With no concrete justification, and operating only under conditions of self-restraint, Facebook's Terms of Service and Data Policy allow the company to continue to sweep in a massive amount of sensitive user data, seemingly just to have it.

Further, there is certainly an unexpected allocation of risk in the Terms of Service and Data Policy, as they seem to be written in a way that is advantageous solely to Facebook. What is troubling, then, is that

219. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122; *see also* Lynch, *supra* note 10, at 11 ("[a]ll of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large").

220. Higginbotham, *supra* note 217 (citing Jessica Groopman, *Consumer Perceptions of Privacy in the Internet of Things*, ALTIMETER GROUP (2015), http://go.pardot.com/l/69102/2015-07-12/pxzlm).

government,[221] law enforcement agencies,[222] app developers,[223] and advertisers[224] all have an interest in user information collected by Facebook. Similar to *Szetela*, Facebook's Terms of Service and Data Policy essentially grant the company a license to push the boundaries of sound business practices, as the company is retaining an alluring goldmine of data that can be shared or sold without user consent.[225] Considering that Facebook operates according to its own subjective standards of "good faith" and has historically failed to "maintain control over how user data is used by advertisers,"[226] the outside interest in the sheer amount of personal user data retained by Facebook and the company's reserved right to use it at its discretion lends support to a conclusion that the terms are unreasonably unfair and function only to the detriment of consumers.

For example, Facebook could potentially share or sell[227] its entire data set to the federal government, subjecting millions of users to unwarranted surveillance and inclusion in the FBI facial recognition database.[228] Facebook's dataset is attractive because even the FBI, through its Next Generation Identification ("NGI") facial recognition database, pales in

221. *See generally* John Lynch & Jenny Ellickson, U.S. Dep't of Justice, *Computer Crime and Intellectual Property Section, Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More*, (Mar. 2010), 17, http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.

222. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 19; *see also* Julie Masis, Is this Lawman your Facebook Friend?, BOSTON GLOBE, Jan. 11, 2009, http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend?mode=PF.

223. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 17–18.

224. *Id*.

225. *See* Weinstein, *supra* note 15 ("By clicking the 'I Agree' button, you blindly assent to hand over your life and interests to billion-dollar corporations to do with it what they may. Oftentimes, this means selling your information to the highest bidder or sharing it with your government. Most of us never even realize it. Our government does, Republicans and Democrats alike, but does nothing about it. After all, this data is a treasure trove they can access by simply reaching into the data candy bowl collected by Facebook, Google, and company.").

226. ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 18.

227. *See, e.g.*, Lauren Effron, *Facebook In Your Face: New Facial Recognition Feature Raises a Few Eyebrows*, ABC NEWS (June 10, 2011), http://abcnews.go.com/Technology/facebook-facial-recognition-feature-raises-eyebrows/story?id=13792666 (quoting Graham Cluely, a senior technology consultant at British Internet security firm Sophos: "Maybe in the future [Facebook] will sell this information to third parties . . . [t]here's so much information we've already given away willingly to Facebook. They have slowly eroded away our control over that data.").

228. Facebook further reserves the right to share user information in response to legal or governmental requests so long as the company has a "good faith belief" that the law requires their acquiescence. *See* Facebook https://www.facebook.com/about/privacy/ (accessed Apr. 5, 2017). Biometric identifiers collected through facial recognition are included in such requests, as the U.S. Department of Justice has indicated that the "standard data production" from Facebook contains "photoprint" and individual contact information, as well as "other data" available upon request, noting that Facebook is "often cooperative with emergency requests." Lynch & Ellickson, *supra* note 221, at 17.

comparison to Facebook's accuracy with facial recognition.[229] The difference in accuracy likely can be attributed to the fact that the FBI is often working with one frontal-facing photograph, usually in the form of a mug shot, passport photo, or driver's license photo,[230] while Facebook's algorithm is consistently being refined and improved each time a user uploads a photo and tags someone.[231] This is because each tag "shows the algorithm what someone looks like from different angles and in [a] different light[]."[232] So while other facial recognition systems struggle with adapting to aging subjects, inconsistent lighting, and single, front-facing photos,[233] Facebook's database and algorithm is uniquely precise because it is routinely updated and cultivated[234] by the company's 1.65 billion users.[235]

Yet, the glaring issue remains: Facebook's diligently developed facial recognition database is arguably lacking user consent, as there is no explicit mention of facial recognition technology included in the company's Terms of Service or Data Policy to which users could even contemplate consenting.[236] Consequently, users who click "I Agree" in a brief pop-up are agreeing to quite possibly be subject to inclusion in government surveillance or to have their sensitive biometric information shared and distributed with any other entity – at no risk or cost to Facebook whatsoever and without any prior notice to consumers.[237]

---

229. Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, ELECTRONIC FRONTIER FOUNDATION (Apr. 14, 2014), https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year (to illustrate, when given a particular face, NGI provides a list of 50 potential facial matches – but of those 50 possibilities, the FBI reports an unimpressive 85% accuracy in successful facial recognition).

230. *See* Jennifer Lynch, *New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos*, ELECTRONIC FRONTIER FOUNDATION (June 15, 2016) https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos; *see also* Naomi Lachance, *Facebook's Facial Recognition Software Is Different From The FBI's. Here's Why*, NATIONAL PUBLIC RADIO (May 18, 2016), (http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why.

231. *See* Naomi Lachance, *Facebook's Facial Recognition Software Is Different From The FBI's. Here's Why*, NATIONAL PUBLIC RADIO (May 18, 2016), http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why ("Every time you tag a photo, you're adding to an enormous, user-driven wealth of knowledge and data.").

232. *Id*.

233. Yue Liu, *supra* note 41, at 41.

234. *See, e.g.*, Martin Kaste, *A Look Into Facebook's Potential To Recognize Anybody's Face*, National Public Radio (Oct. 28, 2013), http://www.npr.org/sections/alltechconsidered/2013/10/28/228181778/a-look-into-facebooks-potential-to-recognize-anybodys-face ("Theoretically, every time you label faces by tagging a picture, you're chipping away at those two big challenges for universal facial recognition. First, you're helping to build a super-database of labeled faces. Second, you're uploading multiple versions of each person's face, which can improve a system's accuracy.").

235. Lachance, *supra* note 231.

236. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 116.

237. *See, e.g.*, Weinstein, *supra* note 15.

Several California courts have agreed that substantive unconscionability "turns not only on a 'one sided' result, but also on an absence of 'justification' for it."[238] The California Supreme Court has recognized that "lack of mutuality can be manifested as much by what the agreement does not provide as by what it does."[239] Outlined in *Armendariz v. Foundation Health Psychcare Services, Inc*., the California Supreme Court was receptive to the fact that even where a provision is not "expressly authorize[d]" in a contract, the Court can look to the "clear implication of the agreement" to establish a lack of mutuality.[240] Even in cases where there is a "reasonable justification for [a] lack of mutuality,"[241] California courts have found substantive unconscionability in contractual provisions where certain terms are fashioned unfairly and solely for "means of maximizing employer advantage."[242]

a. *Lack of Justification for the One-Sided Terms*

Because Facebook does not expressly mention facial recognition technology and its biometric data collection practices in its Terms of Service and Data Policy, a California court should then look to the "clear implication of the agreement"[243] to establish a lack of mutuality. It is unlikely that there would be any possible justification for the lack of mutuality in Facebook's failure to explicitly mention its use of facial recognition technology in the two agreements to which users are required to consent. The only time Facebook provided a justification regarding its implementation of facial recognition technology was during a congressional hearing, in which the company stated that it wanted to make photos "more social."[244] But users could manually tag photos, keeping the "social" aspect alive, prior to Facebook's introduction of facial recognition technology.[245] Facebook contends that "many people" told the company that "manually entering tags for each person in every photo required a great deal of time and effort."[246] But this was a bare assertion, as Facebook offered no surveys or inquiries demonstrating that a substantial

238. *Carboni*, 2 Cal. App. 4th at 84; *see also A & M Produce Co.*, 135 Cal. App. 3d at 487.

239. *Armendariz*, 24 Cal. 4th at 120.

240. *Id*.

241. Soltani v. W. & S. Life Ins. Co., 258 F.3d 1038, 1046 (9th Cir. 2001).

242. *Id*.

243. *Armendariz*, 24 Cal. 4th at 120.

244. *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (testimony of Richard Sherman, Manager of Privacy & Public Policy at Facebook), https://www.judiciary.senate.gov/imo/media/doc/12-7-18ShermanTestimony.pdf.

245. *Id*. at 4.

246. *Id*.

number of users were deeply opposed to manual tagging to warrant the implementation of facial recognition technology as the sole alternative.[247]

3. Third Consideration: The Lack of Mutuality in Facebook's Terms of Service and Data Policy Is Not Due to a Legitimate Commercial Need

One might argue that Facebook is not the only business operation imposing such broad and wide-reaching terms onto consumers, suggesting that the proper test for unconscionability might be whether the contract provisions are "so extreme as to appear unconscionable according to the mores and business practices of the time and place."[248] Although the current business practice for companies may be to write overreaching privacy policies for consumers by way of standardized agreements, that does not mean the business practice is ethically sound, nor that such privacy policies are necessarily immune from a finding of unconscionability.[249]

Moreover, Facebook is not acting like all other businesses with respect to how it operates its facial recognition data collection. Google also has a facial recognition feature, but unlike Facebook, Google intentionally leaves the recognition feature off by default and allows users to elect whether or not to opt-in.[250] Facebook could have set up its facial recognition system so that users would have to affirmatively opt-in, rather than opt-out of the feature, something which was suggested to the company in 2012.[251] But Facebook deliberately maintained the facial recognition collection as an opt-out program, meaning that biometric identifiers are collected by default unless

---

247. *Id*. at 5 (noting that "[t]ag suggestions has been enthusiastically embraced by millions of people" but offering no qualitative data on the public reception of tag suggestions). In fact, several articles were published after the initial rollout indicating that the suggestions were not enthusiastically embraced at all. *See, e.g.*, Lauren Effron, *Facebook In Your Face: New Facial Recognition Feature Raises a Few Eyebrows*, ABC NEWS (June 10, 2011), http://abcnews.go.com/Technology/facebook-facial-recognition-feature-raises-eyebrows/story?id=13792666 (quoting Graham Cluely, a senior technology consultant at British Internet security firm Sophos: "There's a huge backlash in response.... [Facebook users] don't really like the idea of Internet companies, Facebook in particular, gathering data of what we look like . . . it makes me uncomfortable...especially when they turn on features like this without even telling us"); *see also* Nathan Olivarez-Giles, *Facebook under scrutiny for face-recognition feature from privacy group, lawmakers*, L.A. TIMES (June 8, 2011), http://articles.latimes.com/2011/jun/08/business/la-fi-0609-facebook-faces-mobile.

248. 1 Corbin, *Contracts* (1963) § 128, 551.

249. *See* TERMS OF SERVICE; DIDN'T READ, https://tosdr.org/ [https://perma.cc/44TB-H6VC] (accessed Apr. 5, 2017) (rating various networking platforms and websites for consumers based on the broad, wide-reaching nature of company privacy policies, copyright licenses, and more).

250. *Facial Recognition Hearing*, *supra* note 49, at 26 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

251. *Id*. at 26. *See also* FTC, BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES iii (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/Q8FT-PTCZ].

and until the particular user manually changes his or her privacy settings.[252] Despite years of criticism and conversation, Facebook continues to collect its users biometric identifiers by default, meaning the company is unequivocally collecting this sensitive personal data absent explicit consent from well over a billion people.[253]

This note does not purport to say that Facebook should refrain from issuing standardized form agreements to its users, nor does it purport to say that Facebook should allow each user to negotiate the terms with the company. It would be preposterous to have Facebook negotiate its user agreements with each and every one of its billion-plus users. Standardized agreements undoubtedly offer "a degree of efficiency, simplicity, and stability," and they "appear to be a necessary concomitant of a sophisticated, mass-consumption economy."[254] However, "the obvious danger exists that the party who draws up the contract will do so unfairly to his or her advantage,"[255] which is what Facebook is currently doing to its users through the company's Terms of Service and Data Policy. As noted in *Stirlen*, there is no "legitimate commercial need" for Facebook to accrue its user's biometric data and subsequently take away any ownership right over that data from its users.

IV. SOLUTION: WITH MULTIPLE LEGAL CHANNELS AVAILABLE, CALIFORNIA COURTS ARE BEST POSITIONED TO STRIKE DOWN FACEBOOK'S PRIVACY-INVASIVE TERMS REGARDING THE COMPANY'S USE OF FACIAL RECOGNITION TECHNOLOGY

Pursuant to Section 15 of Facebook's Terms of Service, any claims related to Facebook are to be governed by California law and resolved "exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County."[256] Aside from being the mandated jurisdiction due to Facebook's forum and conflict of laws provision, the California judiciary is actually best positioned to take the lead in protecting consumer privacy rights from Facebook's overarching biometric data collection practices. The standing requirement to bring a claim in a California state court, such as San Mateo County, is very straightforward:

252. *See* Adams-Heard, *supra* note 181 ("The technology powers a photo feature called 'tag suggestions' that is automatically turned on when users sign up for a Facebook account . . . Users can opt-out at any time, Facebook said. But that requires that they [affirmatively act to] change their settings.").

253. *See* Graham Cluely, *Facebook changes privacy settings for millions of users – facial recognition is enabled*, SOPHOS (June 7, 2011), https://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/ [https://perma.cc/E6XQ-EADH].

254. *Sybert*, *supra* note 94, at 297–98.

255. *Id*.

256. *Terms of Service*, *supra* note 106.

Article VI, §10 of the state constitution grants Superior Courts power to hear relatively any cause of action.[257] The only threshold requirement is dictated by the California Code of Civil Procedure, which mandates that "every action must be prosecuted in the name of the real party in interest."[258] The U.S. District Court for the Northern District of California, on the other hand, is a federal court, meaning that a plaintiff would need to meet the standing requirements as imposed by Article III of the U.S. Constitution.[259] Regardless of the forum, California courts have the following three legal avenues available to strike down Facebook's privacy-invasive terms: state contract law, state constitutional law, and state tort law. Each possibility is discussed respectively below.

A. Option No. 1: Unconscionability

Based on the extensive reasoning in Section III above, California courts should find that Facebook's Terms of Service and Data Policy containing unconscionable terms with respect to the company's secretive and non-consensual biometric data collection practices under state law. Pursuant to the California Civil Code, "[i]f the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result."[260] The Code offers courts a great deal of flexibility in striking the proper balance between consumer privacy and Facebook's desire to further its utilization of new technologies. For example, rather than dismantling Facebook's Terms of Service and Data Policy in its entirety, California courts could begin by voiding the provisions providing or inferring unrestricted access to user's biometric data.[261]

In order for a California court to deem provisions within Facebook's Terms of Service and Data Policy unconscionable, a Facebook user would need to bring suit alleging that he or she was injured by Facebook's use of

257. CAL. CONST. Art. VI, §10.

258. Cal. Code Civ. Proc. §367 (2017).

259. "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

260. Cal Civ Code § 1670.5 (2016).

261. *See* Future of Privacy Forum, Privacy Principles for Facial Recognition Technology, Discussion Document (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf. (recommending that "companies should also set reasonable retention and disposal practices for facial recognition data. Facial recognition template data that can be used to personally identify an individual, as opposed to aggregate information or simple detection or classification data, should be retained no longer than necessary for legitimate business purposes, and deleted or destroyed in a secure manner").

facial recognition technology and collection of biometric data.[262] Likely, the critical issue that the litigation would turn on would be the question of whether the Facebook user suffered an injury. This determination would be based on whether the user was "sufficiently informed about how their Facebook data would be used"[263] and whether the user "gave permission or agreed to give consent to the company[] to collect, store and tag a photo of their face."[264]

One could argue that if or until Facebook actually does sell its facial recognition database, or until a significant biometric breach occurs, users have not suffered concrete harm or particularized injury under Article III[265] of the U.S. Constitution from the company's collection of biometric identifiers. However, in *Spokeo, Inc. v. Robins*, the U.S. Supreme Court acknowledged that the "risk of real harm" may satisfy the Article III concrete injury requirement where "harms may be difficult to prove or measure."[266] The *Spokeo* Court further acknowledged that "'[c]oncrete' is not . . . necessarily synonymous with 'tangible.'"[267]

Taking Article III and *Spokeo* into consideration, there are two apparent risks of real harm to Facebook users with regard to the company's utilization of facial recognition technology. First, operating with no restraint and with little regard for consumers, Facebook is already engaged in profiting off of user data and information.[268] Estimated to be responsible for roughly 38%[269] of all advertisement revenue growth in the United States, Facebook's wealth

---

262. *See* California Courts, *Filing a Lawsuit*, http://www.courts.ca.gov/9616.htm (accessed Apr. 5, 2017). This section presupposes that a consumer would bring suit in the Northern District of California, a federal court, solely based on the fact that the most recent and preeminent litigation involving Facebook and its users was brought in this court. *See* In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD at 1 (N.D. Cal. 2016) (discussed *infra*).

263. *See* Meg Graham, *What's Next Illinois Biometrics Lawsuits May Help Define Rules for Facebook, Google*, CHI. TRIB. (Nov. 26, 2017, 2:57 P.M.), http://www.chicagotribune.com/bluesky/originals/ct-biometric-illinois-privacy-whats-next-bsi-20170113-story.html.

264. *See* Kate MacArthur, *Facebook, Google track you, but how is data being shared?*, CHI. TRIB. (Apr. 20, 2016, 5:26 A.M.), http://www.chicagotribune.com/bluesky/originals/ct-carla-michelotti-biometric-tracking-bsi-20160420-story.html.

265. "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

266. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (citing *Clapper*, 133 S. Ct. 1138 (2013)).

267. *Spokeo*, 136 S. Ct. at 1549.

268. *See* MacLean, *supra* note 12, at 45 ("In the digital age, when private consumer data—through the wideopen 'back door'—is so freely captured, used, resold, reused, aggregated, and more, for profit alone and largely without the knowing and voluntary consent of the consumer subject of the data, our right to privacy has been eroded almost beyond repair").

269. *See* Jason Kint, *Google and Facebook devour the ad and data pie. Scraps for everyone else*, DIGITAL CONTENT NEXT (June 16, 2016), https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/.

of data that it has amassed on its billion-plus users results in an 89% accuracy rate for targeted advertisements.[270]

In 2015 alone, Facebook garnered a $4 billion profit from advertising revenues.[271] Due to the sheer magnitude of user data and its accuracy in targeted advertising services, Facebook is poised to remain an attractive choice for advertising sales. Yet the problem remains that due to the broad nature of its Terms of Service and Data Policy, Facebook fundamentally has no limitations on the extent to which it can go in selling[272] user data and information.[273] This problem is further enhanced by the fact that there is no accountability framework for Facebook, and consumers have relatively no possible way to trace their biometric data through any subsequent sale or distribution.

In Re Facebook Biometric Information Privacy Litigation, which is currently pending in the Northern District of California, signals a possible shift in the willingness of California courts to find that Facebook's collection and retention of face prints from uninformed consumers could suffice as a concrete injury for consumers.[274] Facebook filed a motion to dismiss the lawsuit arguing that under *Spokeo*, the plaintiffs failed to allege a concrete injury resulting from the company's facial recognition tagging practices.[275] Facebook's argument was "that the collection of biometric information without notice or consent can never support Article III standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.'"[276]

---

270. *See* FACEBOOK, *Reach new customers with your targeting*, https://www.facebook.com/business/a/online-sales/targeting-tips-basic (visited Feb. 8, 2017).

271. Kint, *supra* note 269.

272. *See, e.g.*, Jared Bennett, Center for Public Integrity, *Facebook: Your Face Belongs to Us*, The Daily Beast (July 31, 2017), https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition [https://perma.cc/DHJ4-AHRG] (quoting Larry Ponemon, founder of the Ponemon Institute: "The whole Facebook model is a commercial model . . . gathering information about people and then basically selling them products" based on that information).

273. Facebook is prone to acting first and dealing with the consequences later. For example, in 2013 Facebook settled a class-action lawsuit for roughly $20 million for sharing data with advertising companies on its users' "likes" without consent. Similarly, in 2016 the company came under fire for selling targeted advertisements based on race and ethnicity. *See* Sapna Maheshwari and Mike Isaac, *Facebook Will Stop Some Ads From Targeting Users by Race*, N.Y. TIMES (Nov. 11, 2016), https://www.nytimes.com/2016/11/12/business/media/facebook-will-stop-some-ads-from-targeting-users-by-race.html?_r=0.

274. *See* In Re Facebook Biometric Information Privacy Litigation, Case No. 15-cv-03747-JD (N.D. Cal. 2016) (the plaintiffs are suing Facebook for the company's facial recognition tagging practices under the Illinois' Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b) (2008), http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [https://perma.cc/NH9E-J5R3].

275. *See generally* In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD (N.D. Cal. Sept. 14, 2016) (Facebook, Inc.'s Motion to Dismiss for Lack of Subject-Matter Jurisdiction).

276. In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD, at 7 (N.D. Cal. Feb. 26, 2018) (Order Denying Facebook's Renewed Motion to Dismiss for Lack of Subject Matter Jurisdiction).

In a November 2017 hearing on the matter, U.S. District Judge James Donato seemed unconvinced by Facebook's *Spokeo* argument, stating that "[t]he right to say no is a valuable commodity," also adding that the litigation involves "the most personal aspects of your life: your face, your fingers, who you are to the world."[277] Judge Donato subsequently issued an order denying Facebook's motion to dismiss in February 2018. Quoting the *Spokeo* Supreme Court, Judge Donato delineated the elements required to establish standing, stating that "a plaintiff must demonstrate standing to sue by alleging the 'irreducible constitutional minimum' of (1) an 'injury in fact' (2) that is 'fairly traceable to the challenged conduct of the defendants' and (3) 'likely to be redressed by a favorable judicial decision.'"[278] Importantly, Judge Donato reiterated that "[t]he specific element of injury in fact is satisfied when the plaintiff has 'suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."'"[279] Judge Donato further explained that although "*Spokeo* []refers to Congress, [] state legislatures are equally well-positioned to determine when an intangible harm is a concrete injury."[280]

Of course, *In Re Facebook Biometric Information Privacy Litigation* is unique in the sense that involves a very particularized Illinois state statute. This case is predicated upon Illinois' Biometric Information Privacy Act, which "codifie[s] a right of privacy in personal biometric information" in order to give "Illinois residents the right to control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent."[281] As a result, "[w]hen an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air."[282] As Judge Donato concluded, "[] the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt."[283]

Although California does not have a biometric privacy law on point that resembles Illinois', the California Civil Code provides California residents with other statutorily created interests that can and should be protected against Facebook's intrusive facial recognition technology practices. Judge Donato explicitly mentioned that the Ninth Circuit had previously established that

277. Joel Rosenblatt, *Facebook Judge Frowns on Bid to Toss Biometric Face Print Suit*, Bloomberg (Nov. 30, 2017), https://www.bloomberg.com/news/articles/2017-11-30/facebook-judge-frowns-on-bid-to-toss-biometric-face-print-suit [https://perma.cc/M3GH-HANY] (concluding "[t]he point is Illinois gave its citizens the right to say no . . . [t]he allegation is Facebook usurped that right. That is not a mere technicality in my view.").

278. *See* Case No. 15-cv-03747-JD, at 3 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

279. *Id.* at 3–4 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

280. *Id.*at 4.

281. *Id.* at 6.

282. *Id.*

283. *Id.*

"'state law can create interests that support standing in federal courts. If that were not so, there would not be Article III standing in most diversity cases, including run-of-the-mill contract and property disputes. State statutes constitute state law that can create such interests.'"[284] That being said, California courts can use the state's civil code[285] to plausibly render Facebook's Terms of Service and Data Policy unconscionable for automatically opting users into its facial recognition technology programs after failing to explicitly state that the company collects its users' biometric data upon sign-up.

Consumers could face an uphill battle in California, however, as state judges have remarked that "even though injury-in-fact may not generally be Mount Everest . . . in data privacy cases in the Northern District of California, the doctrine might still reasonably be described as Kilimanjaro."[286] However true that might be, Judge Donato's recent ruling is promising for consumer privacy efforts with respect to facial recognition technology.

The second risk of harm stems from the fact that Facebook disclaims relatively all liability for any ensuing privacy and security implications that might follow in the event of a biometric data breach. This risk is derived from the company's significantly broad inclusion of an exculpatory clause, essentially carving out any liability for Facebook in the event that anything happens to user biometric data that is later sold or accessed by third parties.[287]

This free-trade, zero-liability exception that Facebook has reserved for itself raises an unprecedented risk to consumers, as "it could be difficult or impossible for [consumers] to determine what data has been collected about them, how it is being used, who it has been shared with, and to request access to correct errors or delete the information."[288] Due to "the fact that face images can be captured without [detection] and in public,"[289] the risk of real harm to consumers is undeniable. The reality is that "[a]ll of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large."[290]

Accordingly, another way California courts could limit the offending terms is by explicitly excluding facial recognition data from the scope of Facebook's exculpatory clause. For decades now, several California courts have invalidated contracts containing exculpatory clauses that "affect[] the

---

284. *Id*. at 4 (quoting Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001)).

285. Cal Civ Code § 1670.5 (2016).

286. In re Google, Inc. Privacy Policy Litig., 2013 U.S. Dist. LEXIS 171124, at *13 (N.D. Cal. Dec. 3, 2013).

287. *See* Facebook Terms of Service, https://www.facebook.com/terms.php (accessed July 31, 2017).

288. Future of Privacy Forum, Privacy Principles for Facial Recognition Technology, Discussion Document (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

289. Lynch, *supra* note 10, at 16.

290. *Id.*

public interest."[291] Included in its Terms of Service, the exculpatory clause releases Facebook from any liability resulting from abusive data practices or bad-faith actions from third parties, such as advertisers.[292] This is troubling because "Facebook is one of the most well-known businesses that mine our personal information and sell it to third party companies who use the information in their behavioral advertising strategies."[293] Because the consequences of a biometric data breach can have massive and potentially permanent security consequences, California courts would be well served to invalidate the applicability of Facebook's exculpatory clause to facial recognition data.[294]

Adhesion contracts, like Facebook's, do not have to be completely eradicated in order to better protect consumers; rather, California courts simply need to be more proactive in shielding consumers from overbearing adhesion contracts containing overzealous and unconscionable terms, especially when something as significant as biometric data is on the line. If presented with the opportunity, California courts should decline to enforce Facebook's current Terms of Service and Data Policy on the grounds of unconscionability. Facebook should then be required to revise its Terms of Service and Data Policy so that prospective users are provided with full and explicit notice of the company's biometric data collection practices, including a retention and destruction schedule for such data, before creating an account. Additionally, California courts should require Facebook to operate its tag suggestions exclusively as an opt-in program so that the company has no opportunity to automatically accumulate and hold onto sensitive biometric data. If ever presented with the opportunity to do so, there are a number of sound ways for California courts to limit the unconscionable provisions included in Facebook's Terms of Service and Data Policy without invalidating the entirety of these user agreements.

---

291. *See* Tunkl v. Regents of Univ. of Cal., 60 Cal. 2d 92, 98 (Cal. 1963) (stated best by the California Supreme Court, "[n]o definition of the concept of public interest can be contained within the four corners of a formula. The concept, always the subject of great debate, has ranged over the whole course of the common law"); *see also* Hiroshima v. Bank of Italy, 78 Cal. App. 362 (1926); Union Constr. Co. v. Western Union Tel. Co., 163 Cal. 298 (Cal. 1912)).

292. *See* Facebook Terms of Service, https://www.facebook.com/terms.php (accessed July 31, 2017) (the exculpatory clause reads: "WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES").

293. Justin McHugh, *I Know Who You Are and I Saw What You Did [Social Networks and The Death of Privacy*, 31 SYRACUSE SCI. & TECH. L. REP. 132, 137 (2015) (citing Lori Andrews, I Know Who You Are and I Saw What You Did (Free Press ed., 2011) at 19.

294. *See, e.g.*, Future of Privacy Forum, *supra* note 261 ("social networks and other large databases of identified individual images could increasingly become the targets of access by unauthorized individuals, leading to consumers' facial recognition data being used in ways that consumers cannot anticipate or control, and without their knowledge.").

B. Option No. 2: California State Constitution and Public Policy

If California courts are dissuaded from finding that Facebook's Terms of Service and Data Policy to constitute an unconscionable contract, state courts should still find Facebook's terms independently unlawful, as they clearly violate well-established California public policy as indicated in the state constitution. The First Amendment of the California State Constitution explicitly prescribes a right to privacy, stating:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[295]

Although the right to privacy is not absolute,[296] several California courts have found the state constitution's explicit inclusion of an inalienable right to privacy to be a sufficiently stated interest.[297] Under California law, contacts are void as contrary to public policy where they violate or implicate larger social constructs and concerns.[298] The concept of invalidating contracts on public policy grounds is far from novel to the California judiciary. For example, as far back as 1928, California's 1st District Court of Appeal stated: "public policy means the public good. Anything which tends to undermine that sense of security for individual rights, whether of personal liberty or private property, which any citizen ought to feel is against public policy."[299]

An argument that consumers waive their right to privacy when accepting Facebook's Terms of Service and Data Policy is thwarted by Cal. Civil Code § 3513, which states: "any one may waive the advantage of a law intended solely for his benefit. But a law established for a public reason cannot be contravened by a private agreement."[300] In determining whether a law was intended for personal or public benefit, California courts have historically found that a "law has been established 'for a public reason' only if it has been enacted for the protection of the public generally, i.e., if its tendency is to promote the welfare of the general public rather than a small percentage of citizens."[301]

It is plain from looking at the legislative history behind Article 1 Section 1 of the California Constitution that the inalienable right to privacy was included for the public benefit. The bill's sponsor "was concerned about

---

295. CAL. CONST. ART. I § 1 (emphasis added).

296. *See* CAL. CONST. ART. I § 1.

297. *See, e.g.*, In re Carrier IQ, Inc., Consumer Privacy Litig., 78 F. Supp. 3d 1051, 1117 (N.D. Cal. 2015); *White*, 13 Cal. 3d at 773–74 (Cal. 1975).

298. *See* 2-18 MB Practice Guide: CA Contract Litigation 18.10.

299. Noble v. Palo Alto, 89 Cal. App. 47, 51 (Cal. App. 1928).

300. Cal. Civ. Code § 3513 (2016).

301. *See* Benane v. Int'l Harvester Co., 142 Cal. App. 2d Supp. 874, 878 (Cal. App. 1956); *accord* In re Application of Kazas, 22 Cal. App. 2d 161, 172 (Cap. App. 1937); Cal. Bank v. Stimson, 89 Cal. App. 2d 552, 554 (Cal. App. 1949); Winklemen v. Sides, 31 Cal. App. 2d 387 (Cal. App. 1939).

the evils associated with the growing tendency of the government to collect large amounts of private information about people . . . perceiv[ing] [the] government's collection and use of such information as part and parcel of a shrinking orbit of privacy."[302] Perhaps more telling, the legislative history reveals that the bill was introduced due to concern around "government cooperation with private business in the widespread dissemination of private information" as well as concern about "private businesses knowing private facts about private people."[303] As the legislative history illustrates, privacy rights were incorporated into the state constitution for the public welfare. Therefore, California courts should find that Article 1 Section 1 cannot be circumvented by a private agreement between Facebook and its users. Moreover, the fact that the California judiciary holds that "courts should indulge every reasonable presumption against a waiver of a constitutional right"[304] lends support to a pro-consumer, pro-privacy finding with respect to Facebook's Terms of Service and Data Policy.

Even supposing that a court were to assume that Facebook users waived their state constitutional right to privacy, it is well-established in California case law that "[w]aiver always rests upon intent. Waiver is the intentional relinquishment of a known right after knowledge of the facts."[305] Facebook users simply cannot have relinquished their inalienable right to privacy because, in doing so, they would have needed to know the full extent of how Facebook was using their biometric data, what state privacy rights they had, and what relinquishment of those privacy rights actually entailed. California courts have previously accepted invasion of privacy as a valid public policy concern and there is no reason why the courts should shy away from protecting consumers from Facebook's most recent privacy-invasive practices with facial recognition.[306]

When the legislature sought to amend the state constitution in 1972, California residents received a state election pamphlet which stated that the inalienable right to privacy was included to "prevent[] government and business interests from collecting and stockpiling unnecessary information about [consumers] and from misusing information gathered for one purpose in order to serve other purposes or to embarrass [consumers]."[307] Analogous

---

302. *See* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 2, 418 (1992), http://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1631&context=plr.

303. *Id*.

304. *See* People v. Houston, 10 Cal. App. 3d 894, 900 (Cal. App. 1970).

305. *See* Kay v. Kay, 188 Cal. App. 2d 214, 218 (Cal. App. 1961) (quoting Wienke v. Smith, 179 Cal. 220, 226 (Cal. 1918)) (citing Alden v. Mayfield, 164 Cal. 6, 11 (Cal. 1912) (finding no valid waiver where one attempts "surreptitiously to do something which might in some way advantage him")); *see also* Freshko Produce Servs. v. Produce Delights, LLC, 2017 U.S. Dist. LEXIS 57004 at *4 (C.D. Cal. Apr. 13, 2017).

306. *See, e.g.*, In re Carrier IQ, Inc., Consumer Privacy Litig., 78 F. Supp. 3d 1051, 1117 (N.D. Cal. 2015); Pioneer Elec. (USA), Inc. v. Superior Court, 40 Cal. 4th 360, 370 (Cal. 2007) ("the right of privacy protects the individual's *reasonable* expectation of privacy against a *serious* invasion").

307. White v. Davis, 13 Cal. 3d 757, 774 (Cal. 1975).

to Judge Donato's reasoning used in *In Re Facebook Biometric Information Privacy Litigation*, the California legislature clearly intended to protect consumers against the kind of intrusive and sweeping data collection practiced by Facebook.[308] Since it is well-regarded that "'state law can create interests that support standing in federal courts,'"[309] California courts can use the California State Constitution's inalienable right to privacy in order to protect consumer privacy rights against Facebook's intrusive biometric data collection practices.

By ignoring the will of the people who voted to include an inalienable right to privacy in the now long-standing Constitutional principle, California courts will be engaging in an unprecedented level of judicial activism, with the burden falling squarely on the backs of consumers.

C. State Tort Law: Intrusion Upon Seclusion

Lastly, this issue could potentially be addressed from a tortious conduct standpoint by focusing on the state tort of intrusion upon seclusion. California has adopted the elements for an intrusion upon seclusion claim as articulated in *Miller v. National Broadcasting Co.* and the Restatement Second of Torts.[310] Accordingly, "[u]nder California law, a claim for intrusion upon seclusion has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person."[311] The first element is satisfied when the individual claiming an invasion of privacy can show that they have "an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source."[312]

Although an individual "cannot have a reasonable expectation of privacy if she consented to the intrusion,"[313] it is well-accepted under California law that "consent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and

308. In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD, at 6 (N.D. Cal. Feb. 26, 2018) ("As the Illinois legislature found, these procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers -- identifiers that cannot be changed if compromised or misused. When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.").

309. No.: 3:15-CV-03747-JD, at 4 (quoting Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001)).

310. *See* Miller v. Nat'l Broadcasting Co., 187 Cal. App. 3d 1463, 1482 (Cal. App. 1986); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

311. Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (citing Shulman v. Group W Prod., Inc., 18 Cal. 4th 200, 231 (Cal. 1998)).

312. *Id.*

313. *Opperman*, 205 F. Supp. 3d at 1072 (N.D. Cal. 2016) (citing *Hill v. Nat'l Collegiate Athletic Ass'n.*, 7 Cal. 4th 1, 26 (Cal. 1994)).

if the alleged tortfeasor did not exceed the scope of that consent."[314] *Opperman v. Path, Inc.* illustrates consent in intrusion upon seclusion claim.

Opperman involved the adequacy of consumer consent and notice within Yelp's Privacy Policy.[315] Due to an ambiguity in the Privacy Policy, the question in *Opperman* was whether consumer consent to allow Yelp to "find friends" also implies "consent to upload that data to Yelp's servers."[316] The Northern District of California denied Yelp's motion for summary judgment and dismissal, noting that "a reasonable jury could find that Yelp's Privacy Policy provisions do not explicitly address—and thus do not obtain knowing consent" for purposes beyond what was stated in the Privacy Policy.[317] Facebook's Terms of Service and Data Policy are analogous to the consent issues with Yelp's Privacy Policy in *Opperman*, as consumers cannot knowingly consent to something of which they are unaware. Specifically, Facebook users cannot consent to the company collecting their biometric data, since the inclusion of facial recognition technology is not stated in the Terms of Service or Data Policy to which users are required to consent. As such, under an intrusion upon seclusion claim, it would be plausible for California courts to find that Facebook users could not possibly have consented to Facebook's facial recognition data collection from the outset, and that the company exceeded the scope of any proffered consumer consent that it received.

As to the second element of an intrusion upon seclusion claim, "the intrusion must also be 'highly offensive to a reasonable person and sufficiently serious and unwarranted as to constitute an egregious breach of the social norms.'"[318] Significantly, California courts have noted that "[a] 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms."[319] Moreover, California courts have clarified that "community norms" entails that "'[t]he protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.'"[320] For example, in *Opperman*, the Northern District of California said that data collected through invasive or unwanted means needs to be "more private than a person's mailing address" and that the collection needs to be outside of the scope of "routine commercial

314. *Opperman*, 205 F. Supp. 3d at 1072 (quoting RESTATEMENT (SECOND) OF TORTS § 892A, §§ 2(b), 4 (1979)).

315. Opperman v. Path, Inc., 205 F. Supp. 3d 1064 (N.D. Cal. 2016).

316. *Id*. at 1075–76.

317. *Id*. at 1074.

318. *See Opperman*, 205 F. Supp. 3d at 1077 (quoting Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 295 (Cal. 2009)); *see also* Miller v. Nat'l Broadcasting. Co., 187 Cal. App. 3d 1463, 1483–84 (Cal. App. 1986) ("A court determining the existence of 'offensiveness' would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.").

319. *Opperman*, 205 F. Supp. 3d at 1079 (quoting *Hill*, 7 Cal. 4th at 37).

320. *Opperman*, 205 F. Supp. 3d at 1079 (quoting In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014).

behavior."[321] Certainly biometric data is more private than a mailing address, because although you can move and change your address, "you cannot change your fingerprint, and you cannot change your face."[322]

Facebook has far surpassed any kind of "routine commercial behavior" with respect to its facial recognition capabilities, and the company's seemingly endless patent requests using the technology seem to go far beyond any kind of routine commercial activity as well.[323] Of paramount concern is an August 2015 patent filing in which Facebook sought to "utilize passive imaging information" by visually tracking user's emotions and facial expressions across "social networks, news articles, video, audio, or other digital content."[324] The stated purpose of this patent is essentially to bring in advertising revenue, as the patent filing specifies that "advertisement delivery may be customized based upon a user's detected emotions."[325] If offensiveness is truly determined by widely-held community values, then California courts must take into account the fact that despite 93% of Americans reporting the importance of controlling who can access their personal information, only a mere 9% actually feel in control of the extent of information collected about them.[326] Accounting for the 68% of American adults who use Facebook daily,[327] it seems farfetched to believe that allowing highly invasive practices would be considered the social norm. The Northern District of California recently noted that "[t]hose customs and habits are very much in flux,"[328] meaning that California courts can put a stop to Facebook's vastly overstepping of the bounds of consumer consent and privacy before any further irreversible escalation.

It is plain that there are numerous ways for California courts to protect consumers from invasions of privacy without hindering Facebook's foray into more innovative uses for facial recognition technology. California courts have the legal tools available to shift the course and create a pro-privacy and pro-consumer landscape. As continued failure to act will present insurmountable challenges for consumer privacy, Facebook's current facial recognition

---

321. *Opperman*, 205 F. Supp. 3d at 1078 (citation omitted).

322. *Facial Recognition Hearing*, *supra* note 49, at 1 (opening statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

323. *See, e.g.*, U.S. Patent No. 20170140214 (filed May 18, 2017) (seeking to capture facial data points in order to generate an emoji based on the user's current facial emotion); U.S. Patent No. 20160127360 (filed May 5, 2016) (seeking to use facial recognition data and speech recognition data for access and authentication into the social media site); U.S. Patent No. 20150242679 (filed Aug. 27, 2015) (discussed *infra*, note 290).

324. *See generally* U.S. Patent No. 20150242679 (filed Aug. 27, 2015) (Facebook is looking to "include emotions or expressions such as a smile, joy, humor, amazement, excitement, surprise, a frown, sadness, disappointment, confusion, jealously, indifference, boredom, anger, depression, or pain").

325. *See* U.S. Patent No. 20150242679 (filed Aug. 27, 2015).

326. *See* George Gao, *What Americans think about NSA, surveillance, national security and privacy*, PEW RESEARCH CENTER (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

327. PEW RESEARCH CENTER, Social Media Fact Sheet (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/social-media/.

328. *Opperman*, 205 F. Supp. 3d at 1079.

practices necessitate significantly overdue judicial intervention from the California judiciary.

V. CONCLUSION

As written, Facebook's Terms of Service and Data Policy wrongfully allows unrestricted collection, disclosure, and use of sensitive biometric identifiers in ways that its users neither understand nor explicitly consent to. California courts would be wise to accept that "[o]paque privacy waivers that consumers merely click through without understanding are no substitute for real and substantive consumer privacy protections in the digital age. Forced consent is not consent at all."[329] Acknowledging that Facebook has everything to gain, and consumer privacy rights have everything to lose, California courts should recognize the very real risk of harm to consumers by Facebook's accumulation and handling of biometric data. Pro-consumer intervention can be achieved under California law through any of the three legal avenues discussed in this note. A pro-consumer privacy holding from California will hopefully spark meaningful policy and legislative changes on both the state and federal levels to adequately address the possible privacy implications from unregulated facial recognition technology. Facebook controls the narrative, but it is not too late for the California judiciary to step in and lead the way by preventing the company from unequivocally controlling consumer privacy, both now and in the future. Without action and interference, there is nothing to stop Facebook from expanding its collection, use and distribution of images in its facial recognition database – all at the expense of over one billion innocent and non-consenting users.[330]

329. *See* MacLean, *supra* note 12, at 46.

330. The author would like to draw attention to a 2010 article featured in The New Yorker, in which it was revealed that Facebook founder Mark Zuckerberg once called the social media site users "dumb fucks" for trusting him with their personal data. *See* Jose Antonio Vargas, *The Face of Facebook*, THE NEW YORKER (Sept. 20, 2010), http://www.newyorker.com/magazine/2010/09/20/the-face-of-facebook [https://perma.cc/LYW9-82FN].

Where in the World is Your Data? Who Can Access It?

Katherine Grabar *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. B.A., Political Science and Law, History, and Culture, University of Southern California, May 2015. The author would like to thank James Brecher for teaching her about legal writing, analysis, and advocacy. She dedicates this note to her parents and grandparents who gave her the instrumental gift of education.

I. INTRODUCTION

People take pictures on their Apple iPhones, save documents to Google Drive, or send emails using Microsoft's Outlook.com. Companies, like Microsoft, Apple, and Google, make these services available to their users and store the user-created data on their own servers, as opposed to on the device used to create the work product.[1] This storage function is called the "cloud."[2] Customers using the cloud can access their data from any Internet-enabled device and share the data with others while preventing data loss.[3] The cloud is a large number of grounded servers located across the globe, and in the United States alone, the cloud is responsible for two percent of the country's electricity usage.[4] The servers powering the cloud must be stored at a location with a low temperature because if they overheat, the servers will crash.[5] When these servers, hosted in data centers, overheat, users' devices cannot access the content they need.[6] In response, Microsoft developed Project Natick to solve this problem of overheated servers by operating data centers in the ocean.[7] The ocean keeps the data centers cool so consumers can access their data without delay, and the technology companies furnishing the servers save money on their electricity bill.[8]

The Stored Communications Act ("SCA"), which is part of Title II of the Electronic Communications Privacy Act ("ECPA"), is the "primary law governing government and private actor access to our stored online communications" written in 1986.[9] Courts differ on how to interpret the anachronistic statute, some choosing to protect electronic communications that did not exist at the time of the SCA's passage, like data stored in the

---

1. *See* David Goldman, *What is the cloud?*, CNN (Sept. 14, 2014, 9:05 AM), http://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/index.html [https://perma.cc/3T7L-QZBU]. Businesses use similar storage services for medical and financial data, work product, and trade secrets. *See* Reuven Choen, *The Could Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*, FORBES (Apr. 16, 2013, 9:23 AM), https://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing [https://perma.cc/Z2AF-AE6].

2. *See* Jess Fee, *The Beginner's Guide to the Cloud*, MASHABLE (August 26, 2013), https://mashable.com/2013/08/26/what-is-the-cloud/ [https://perma.cc/W2UL-ZG4G].

3. *See* Nicole A. Ozer & Chris Conley, *Cloud Computing: Storm Warning for Privacy?*, ACLU NORTHERN CAL. (Jan. 2010), https://www.aclunc.org/sites/default/files/privacy_and_free_speech_it's_good_for_business,_2nd_edition.pdf [https://perma.cc/RV44-RR99].

4. Goldman, *supra* note 1.

5. *See* John Markoff, *Microsoft Plumbs Ocean's Depths to Test Underwater Data Center*, N.Y. TIMES (Jan. 31, 2016), https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html [https://perma.cc/H2W9-D2LA].

6. *See id.*

7. *Id.*

8. *Id.*

9. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2015).

cloud, while others fail to modernize their interpretation.[10] Without legal protection, the technological process will be inhibited if consumers and businesses do not have confidence that their data will be secure in new technologies like the cloud.[11]

The Second Circuit recently grappled with the SCA's applicability to cloud data stored in Dublin in a Microsoft data center.[12] The Court denied the government's search warrant application to access data in the Dublin data center because the SCA did not specifically mention that the law governs data extraterritorially.[13] An obsolete SCA thus produces an environment where online cloud data does not possess the same privacy protections as data stored on a home computer or in a filing cabinet.[14]

Congress has repeatedly failed to update the SCA to govern privacy rights in the massive amounts of data consumers store in the cloud.[15] This creates an even larger challenge when applied to the underwater data centers Microsoft is developing. The Second Circuit held that the United States does not have jurisdiction to access data that is not stored domestically.[16] Accordingly, the United States likely does not have jurisdiction over data stored at sea in places like underwater data servers in Microsoft's Project Natick.

Congress must amend the SCA to protect privacy interests and empower the government to engage in effective investigative searches. Law enforcement, armed with a search warrant, needs the ability to access the data of United States citizens stored on domestically and internationally. Companies that operate their own cloud services should not be able to store data wherever they please, based on a company policy designed to avoid potential government seizure. An updated Stored Communications Act should include: (i) jurisdiction to search overseas data of United States citizens; (ii) jurisdiction to search data physically stored in the United States; and (iii) a warrant and notice requirement for search of any electronic

---

10. *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-76 (9th Cir. 2004) (concluding messages stored on a web server are included in the definition of electronic communications of the Stored Communications Act), *with* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994) (holding once communications are received they are no longer in electronic transmission) ("[T]he ECPA's legislative history makes it crystal clear that Congress did not intend to change the definition of "intercept" as it existed at the time of the amendment.").

11. *See* Elizabeth MacDonald, *NSA Leaks Slam Could Computing Industry*, FOX BUSINESS (Aug. 9, 2013), http://www.foxbusiness.com/politics/2013/08/09/nsa-leaks-slam-cloud-computing-industry.html [https://perma.cc/MDS5-279B] (revealing the billions of dollars potentially lost from the fallout of NSA spying programs).

12. *See* Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), https://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html [https://perma.cc/XM38-4XGH].

13. *See* Brian Jacobs, *The Microsoft Warrant Case: Unintended Consequences of the Second Circuit's Ruling*, FORBES (Aug. 2, 2016, 5:04 PM), https://www.forbes.com/sites/insider/2016/08/02/the-microsoft-warrant-case-unintended-consequences-of-the-second-circuits-ruling/#3b3b5ca52f28 [https://perma.cc/D2MM-FT3Z].

14. *See* Ozer & Conley, *supra* note 3.

15. *See* THOMPSON & COLE, *supra* note 9, at 8-15.

16. *See* Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d. Cir. 2016).

communications. These solutions are necessary to create clear procedures for searches and search warrant applications to protect law enforcement investigations, individual privacy, and the business of technology companies.

This Note proceeds in three parts. Part II outlines the text and legislative history of the Stored Communications Act and the Second Circuit's interpretation of the SCA in *Microsoft Corp. v. United States*. Part III addresses the consequences of inaction through a review of the lack of law enforcement search tools abroad without extraterritorial application of the SCA, Microsoft's development of underwater data servers, and a review of proposed and unsuccessful legislation to amend the SCA. Part IV proposes jurisdictional and privacy amendments to the SCA that provide law enforcement with the ability to search data with a warrant based on probable cause for electronically stored data of any United States citizen or data geographically stored within the United States. This proposed jurisdictional power is balanced with a warrant requirement for any stored data and notification requirement to any user whose data is seized.

II. THE STORED COMMUNICATIONS ACT: AN OUTDATED STATUTE APPLIED TO A MODERN-DAY DISPUTE

The Stored Communications Act was enacted to protect electronic communications from unreasonable searches and seizures.[17] However, the law has not been substantively updated in the thirty years since it was introduced.[18] An outdated law, in combination with developing technology, yields uncertain privacy protection for individuals over data stored using cloud technology.[19] The SCA inhibits an individual's attempt to protect data and law enforcement's endeavors to engage in lawful searches of data to investigate unlawful activity.[20] The Second Circuit interpreted the Stored Communications Act and concluded that the law does not authorize application of a United States search warrant to data stored overseas.[21] According to the Second Circuit's interpretation, the statute failed to grant law enforcement the power to search data overseas because there was no explicit provision discussing extraterritorial application or cloud data.[22] This outdated statute creates ambiguity as to an individual's privacy rights such that a corporation's decision of where to store data determines whether the data receives Fourth Amendment protections.[23]

17. *See* THOMPSON & COLE, *supra* note 9, at 1.
18. *See* Henning, *supra* note 12.
19. *See* Ozer & Conley, *supra* note 3, at 7.
20. *Id.*
21. *Microsoft*, 829 F.3d at 220.
22. *Id.* at 206, 211.
23. *Id.* at 224 (Lynch, J. concurring).

A. The Problem: The Outdated Text of the Stored Communications Act

Congress enacted the ECPA and the SCA to extend the application of the Fourth Amendment privacy right to electronic communications.[24] Before the statute, there was no explicit regulation governing who could access electronically stored data and when access was granted.[25] The statute outlines with whom network providers may share a customer's data, since customers may not store their own data when using electronic services.[26] The SCA instructs providers of electronic communication services on when they can share customers' information and communications[27] and dictates the proper standards for law enforcement to gain access to this data.[28] Service providers undertake the obligation to protect users and their data, with the exception of subpoenas and warrants based on probable cause.[29] The statute "allows law-enforcement agencies to obtain stored e-mail, account records, or subscriber information from a service provider."[30] Even though the statute has not been meaningfully updated since its passage, courts now interpret the SCA to govern electronic content, such as emails, YouTube videos, Facebook messages, and metadata related to Internet transactions.[31]

Under the SCA, an administrative subpoena can grant the government access to basic subscriber and transactional information.[32] However, law enforcement needs more than just a subpoena to access the actual content of stored communications because the SCA requires a warrant for "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less."[33]

---

24. *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U.L. REV. 267, 276 (2013).

25. *Id.* at 274-76.

26. *Id.* at 277.

27. According to the ECPA and the SCA, an electronic communication is any communication that is not a wire or oral communication. For example, an email is an electronic communication. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIV., INFO., AND TECH. 149 (3d. ed. 2011). Federal courts corroborate this interpretation. *See Theofel*, 359 F.3d 1066 (recognizing storage of copy of emails falls within jurisdiction of the SCA); Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 108 (3d Cir. 2003) (examining emails stored via backup methods).

28. *See* THOMPSON & COLE, *supra* note 9, at 3. Congress differentiated between the two categories of data because in 1986, users would download the emails onto their own machines instead of storing them with third-party providers and the copies the provider had were akin to business records. Serrin A. Turner, *Are Changes in Store for the Stored Communications Act?*, 2-6 PRATT'S PRIV. & CYBERSECURITY L. REP. 04 (2016).

29. *See* Samantha V. Ettari et al., *Second Circuit Rules That the U.S. Government Cannot Use a Search Warrant to Access Overseas Data*, 277-279 PRATT'S PRIV. & CYBERSECURITY L. REP. 03 (2016); Nora Ellingsen, *The Microsoft Ireland Case: A Brief Summary*, LAWFARE (July 15, 2016, 10:34 AM), https://www.lawfareblog.com/microsoft-ireland-case-brief-summary [https://perma.cc/6C5M-86V4].

30. Jessica R. Herrera-Flanigan, CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 317 (Bert-Jaap Koops & Susan W. Brenner eds., 2006).

31. THOMPSON & COLE, *supra* note 9, at Introduction.

32. 18 U.S.C. § 2703(c)(2).

33. *See* § 2703(a).

For any communications older than 180 days, the government must notify the subscriber or customer, or obtain a warrant.[34] Classifications within the statute dictate different protections for the same email if it is in transit, opened and stored in remote storage, stored on a home computer, unopened and stored for 180 days or less in remote storage, or in remote storage for more than 180 days while unopened.[35]

B. The Stored Communications Act: Too Old to Regulate the Microsoft Cloud and the Data Within It

On December 4, 2013, Magistrate Judge James C. Francis IV granted the United States government's warrant, in accordance with the SCA, for data stored by the Microsoft Corporation ("Microsoft") for a criminal narcotics investigation.[36] Microsoft stored most of the data relating to the government's request in one of its data centers in Dublin, and the rest in the United States.[37] Believing the warrant only authorized seizure of data located in the United States, Microsoft only provided the data stored domestically.[38] Judge Francis disagreed with Microsoft's interpretation, and decided that seizure of any relevant data was proper because the location where the government would review the data was "the relevant place of seizure," not the location the data was stored.[39] The District Court denied its motion to quash the government's warrant, and as a result, Microsoft appealed the decision to the Second Circuit Court of Appeals.[40]

The government's search of this data was problematic because data moves between Microsoft's servers in data centers around the world based on Microsoft's policy of placing data in a data center closest to a user's country code set by the user's stated preference.[41] In *Microsoft*, the country code dictated the data move to Microsoft's Dublin data center.[42] Once the data was transferred, all the data left remaining on the original server, here, a United States server, was non-content email information, some of the user's address book, and basic account information.[43]

The Second Circuit found that Congress enacted the SCA in order to provide the privacy protections of the Fourth Amendment to users of electronic communication services.[44] The technological knowledge Congress

34. § 2703(b)(1)(A)-(B).

35. *See* Electronic Communications Privacy Act (ECPA), ELECTRONIC PRIV. INFO. CENTER, https://epic.org/privacy/ecpa/ [https://perma.cc/Z8XG-QXEH], (last visited Dec. 14, 2016) (demonstrating a warrant is required to access an email in transit while an opened email stored remotely only requires a subpoena).

36. *Microsoft*, 829 F.3d at 203; Ettari et al., *supra* note 29, at 03.

37. *See Microsoft*, 829 F.3d at 204.

38. *Id*.

39. *Id.*

40. *Id*. at 200.

41. *Id.* at 203.

42. *Id*.

43. *Id*.

44. *Id.* at 206; *see also* S. COMM. ON JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, S. REP. NO. 99-541, at 5 (1986).

possessed thirty years ago when it passed the ECPA is considerably different from today because of the great advances in the industry.[45] "[A] globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy."[46]

The Second Circuit interpreted Supreme Court precedent to mandate that unless Congress specifically states otherwise, there is a presumption against applying United States law extraterritorially.[47] The SCA makes no such mention of extraterritorial application.[48] Even without the explicit mention of extraterritorial application, the Second Circuit noted that the "far-reaching state court authority" laid out in the SCA would inevitably conflict with foreign laws if applied outside of the United States.[49]

Drawing on this interpretation, the Court found that, "[b]ecause the content subject to the [w]arrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States."[50] The lack of explicit authorization for such action caused the Second Circuit's reversal of the District Court.[51] Microsoft would have to inevitably interact with a non-domestic data server in order to execute the search warrant.[52] The Second Circuit held that Microsoft adequately complied with the search warrant for the data stored domestically and had no further obligations to law enforcement.[53]

Judge Lynch wrote a concurring opinion to illustrate the practical consequences of the Court's decision and the apparent need to modernize the SCA.[54] The opinion emphasized how the court's holding was not actually a win for privacy interests generally; rather, only those who lived abroad or claimed to live abroad gained any additional protection from the court's holding.[55] This application of the SCA permits an American user to misrepresent where she is located solely to evade potential seizure and it likewise permits Microsoft and companies like it to move data in order to evade government searches.[56] According to Judge Lynch, a "sensible" resolution of the court's decision would be nuanced, accounting for more than

45. *See Microsoft*, 829 F.3d at 205-06.

46. *Id*. at 206 (citing Craig Partridge, *The Technical Development of Internet Email*, IEEE ANNALS OF THE HIST. OF COMPUTING 3, 4 (Apr.-June 2008)).

47. *See Microsoft*, 829 F.3d at 210 (citing Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010)). The Supreme Court recognizes that Congress typically legislates on domestic matters rather than foreign ones and that Congress is a governmental entity more fit to make decisions regarding international relations than are the courts. *Microsoft*, 829 F.3d at 210.

48. *Id*. at 211. *Contra* Weiss v. National Westminster Bank PLC, 768 F.3d 202, 207 & n.5 (2d Cir. 2014); United States v. Weingarten, 632 F. 3d 60, 65 (2d Cir. 2011).

49. *See* Microsoft, 829 F.3d at 211.

50. *Id.* at 220.

51. *Id*. at 222.

52. *Id*. at 220.

53. *Id*. at 222.

54. *Id*. (Lynch, J., concurring).

55. *Id.* at 224. (Lynch, J., concurring).

56. *Id.* at 230 (Lynch, J., concurring).

just what Congress anticipated in 1986.[57] "Our decision today is thus ultimately the application of a default rule of a statutory interpretation to a statute that does not provide an explicit answer to the question before us."[58]

III. *MICROSOFT CORP. V. UNITED STATES*: ONE OF MANY REASONS THE STORED COMMUNICATIONS ACT REQUIRES AN UPDATE

Without a law to authorize searches extraterritorially, United States law enforcement can only obtain overseas data by a mutual legal assistance treaty.[59] International law governs the parameters of a search for a law enforcement investigation and inhibits law enforcement from doing their job.[60] Underwater data centers will only worsen the ambiguity surrounding searches since these centers are not necessarily located in any jurisdiction to which a mutual legal assistance treaty would apply. Law enforcement, under the SCA interpretation in *Microsoft*, would not have any recourse to search the data. Congressional attempts to amend the SCA in recent legislative sessions have been unsuccessful and Congress has been unable to create complete and effective solutions to any of these issues.[61]

A. Ramifications of Microsoft Corp. v. United States Beyond One Search Warrant

The Second Circuit is one of many courts across the globe grappling with jurisdictional questions about electronically stored data.[62] Treaties and the lack thereof cause a "jurisdictional headache" for courts where companies like Microsoft have "headquarters in one country, servers in another, and users all around the world."[63] United States law enforcement and governmental entities have to submit a request to a country with which it in a mutual legal assistance treaty ("MLAT") and must follow the outlined

57. *See id*. at 231 (Lynch, J., concurring). *See also* Henning, *supra* note 12 (quoting the concurrence "[T]here is no evidence that Congress has ever weighed the costs and benefits of authorizing court orders of the sort at issue in this case").

58. *See Microsoft*, 829 F.3d at 232 (Lynch, J., concurring). Judge Lynch asserted at oral argument that it "would be helpful if Congress would engage" in the task of updating the statute, while acknowledging that speed is not Congress' strength. Alex Ely, *Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview*, LAWFARE (Sept. 10, 2015, 5:08 PM), https://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview [https://perma.cc/CWX2-CXPA].

59. *See Microsoft*, 829 F.3d at 221.

60. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 409 (2014); *see also* U.S. Dep't of State, Treaties, Agreements and Asset Sharing (2014), https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm [https://perma.cc/GE6Q-YKRK].

61. *See* Kerr, *supra* note 60, at 373; *see, e.g.*, Email Privacy Act, H.R. 699, 114th Cong. (2015).

62. Kerr, *supra* note 60, at 376.

63. *Id*.

procedures.[64] The parties to the treaty consult with the Office of International Affairs at the Department of Justice to obtain data on a foreign server pursuant to the MLAT.[65] The MLAT does not necessarily describe the complete process; a combination of national laws govern the procedure.[66] United States law enforcement seeking the information is therefore at the mercy of the partner country to respond to the request, if the country responds at all.[67] If the country does respond, the typical international response takes months, not days.[68] The MLAT does not require a response when "the execution of such [a] request would be prejudicial to the state's security or public interest; the request relates to a political offense; there is an absence of reasonable grounds; the request does not conform to the MLAT's provisions; or the request is incompatible with the requested state's law."[69] Where the United States has not signed a MLAT with the country, the United States government has no formal way to conduct searches of data centers abroad.[70]

Certain countries who reject the MLAT approach mandate forced data localization to exercise control over data and ensure their own access by "requir[ing] the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs . . . for both providers and consumers."[71] However, these requirements are difficult to enforce and drive potential wrongdoers to engage in more secretive practices.[72] These policies can affect privacy, security, economic

64. *See* Microsoft, 829 F.3d at 221; Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE (July 15, 2016, 7:21 AM), https://www.lawfareblog.com/reactions-microsoft-warrant-case [https://perma.cc/GE7R-SZ27]. A MLAT is a bilateral agreement between the United States and another country to aid in criminal investigations. Thomas G. Snow, *Prosecuting White-Collar Crime: The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them*, 11 WM. & MARY BILL OF RTS. J. 209, 223-25 (2002).

65. *See* Herrera-Flanigan, *supra* note 30, at 324.

66. *See* Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. FOR INTERNET AND SOC'Y BLOG (Feb. 23, 2015, 1:06 PM), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [https://perma.cc/A3VT-8K89].

67. *See* Susan W. Brenner et al., *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 384 (2002).

68. *See* United Nations Office on Drugs and Crime, Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector, U.N. Doc. No. UNODC/CCPCJ/EG.4/2013/2 (Jan. 23, 2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf [https://perma.cc/36UV-PWWQ].

69. *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 734 (2015).

70. *See Microsoft*, 829 F.3d at 221. As of 2014, the United States only had mutual legal assistance treaties with 57 nations. *See* U.S. DEPARTMENT OF STATE, TREATIES, AGREEMENTS AND ASSET SHARING (2014), https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm [https://perma.cc/GE6Q-YKRK]. Ultimately this note focuses solely on the domestic statutory analysis and not the international framework. A larger discussion of law enforcement access to information on the international level would further delve into an MLAT and Privacy Shield discussion that would frankly overwhelm and distract from this note's purpose.

71. *See* Chander & Le, *supra* note 69, at 681.

72. *Id*. at 732.

development, international trade, and innovation.[73] MLATs reduce the risk of countries requiring data localization requirements and avoid an even bigger jurisdictional headache for extraterritorial data searches.[74]

B. Cloud Innovation: Microsoft Underwater Data Center

Many individuals already engage in most of their work through the cloud.[75] A majority of technology experts agree that most people will access and share information through cloud computing by 2020.[76] Webmail services, like that Microsoft provides, is one of the most prevalent of the cloud services offered.[77]

In order for customers to utilize email, engage in social networking, and stream video all while on the cloud, companies like Microsoft need data servers that do not overheat, and plenty of space to store the data servers.[78] If the servers reach too high of temperatures, they crash.[79] Current data centers are built far away from users and hubs because they require large spaces to be built and are costly to maintain.[80] Microsoft developed Project Natick to solve these problems; the Project aims to operate data centers in the ocean, possibly on the sea floor, or in containers beneath the surface and connected to land by a fiber-optic cable.[81] These aquatic data centers promise to transmit data faster than current data centers are capable of because "half of the world's population lives within 120 miles of the sea" so the data centers will be much closer to the users they serve.[82]

Microsoft engaged in a successful 105-day trial of a steel capsule containing a data center 30 feet underwater in the Pacific Ocean and 30 kilometers from shore.[83] The capsule was connected to land through a cable,

---

73. *Id*. at 681.

74. *See* Int'l Chamber of Commerce, *Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures* 3 (2012), https://www.iccwbo.be/wp-content/uploads/2016/03/20120912-ICC-policy-statement-on-MLAT.pdf [https://perma.cc/43HY-B4UB].

75. *See* Janna Anderson & Lee Rainie, *The future of cloud computing*, PEW RESEARCH CTR. (June 11, 2010), http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/ [https://perma.cc/EAF8-HHFU].

76. *See id*.

77. *See id*.

78. *See* Markoff, *supra* note 5. Microsoft is not the only company innovating to decrease the burden of data storage; Nautilus Data Technologies is building the first commercial data center on water. *See* George Leopold, *Navy backs development of first 'data barge'*, DEFENSE SYSTEMS (Nov. 19, 2015), https://defensesystems.com/articles/2015/11/19/navy-nautilus-floating-data-barge.aspx [https://perma.cc/TRN9-HHFQ]. The company discussed the product and selling it to "the industry's leading technology companies." *Id*.

79. *See* Markoff, *supra* note 5.

80. *Id*.

81. *Id*.

82. *See* James Eng, *Project Natick: Microsoft Tests Putting Data Centers Under the Sea*, NBC NEWS (Feb. 1, 2016, 4:59 PM), https://www.nbcnews.com/tech/innovation/project-natick-microsoft-tests-putting-data-centers-under-sea-n508946 [https://perma.cc/S5MX-BU5M].

83. *See* Markoff, *supra* note 5.

which was then connected to the Internet to transmit data.[84] According to Microsoft, the results of the test run thus far are "promising."[85] Because of these promising results, Microsoft expects to develop underwater data centers that last up to five years without significant maintenance.[86] Microsoft engages in this innovation to respond to the increasing demand for mass amounts of data storage at a faster speed as opposed to the typical storage on a user's device.[87]

C. Congress' Lack of Impactful Action Leaves the SCA in the Twentieth Century

Congress first attempted to amend the ECPA and SCA in 2011 after technology companies, academics, and privacy advocates lobbied to communicate the importance of an update to the statutes.[88] The technology community recognized that, "the ECPA is an anachronistic statute, one ill-suited to contemporary law enforcement and global electronic communications."[89] Most Congressional proposals merely tinkered with the 1986 statute, even though the ECPA requires drastic reform to adapt to the changes in technology and the Internet since 1986.[90] Congress presented solutions by recommending a requirement for a warrant for any seizure regardless of the age of the communication, enforcement of a blanket prohibition on any voluntary disclosure of customer data, and a notice requirement for the customer's data searched by law enforcement.[91] No Congressional attempt, thus far, has been successful at achieving any meaningful change.[92] The following two attempts illustrate this lack of success and examine how the statutes could have held up in the *Microsoft* case instead of the archaic SCA.

The Email Privacy Act was the most successful Congressional attempt to amend the ECPA. The House Judiciary Committee unanimously voted it out of Committee and it passed the House of Representatives with unanimous approval as well.[93] Under the Act, the provider of an electronic communication service, the technology company and host of the cloud had to

---

84. *See Project Natick*, MICROSOFT, https://news.microsoft.com/natick/ [https://perma.cc/PA7J-9CX9] (last visited Dec. 13, 2016).

85. *See* Eng, *supra* note 82.

86. *See id.*

87. *See* Markoff, *supra* note 5.

88. *See* THOMPSON & COLE, *supra* note 9, at 8.

89. *See* Ely, *supra* note 58.

90. *See* Kerr, *supra* note 60, at 373, 375 (suggesting repeal of the ECPA and law to replace it).

91. *See* THOMPSON & COLE, *supra* note 9, at 8-15.

92. *Id*. at 8.

93. *See* Turner, *supra* note 28, at 04; Sophia Cope, *House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform*, ELEC. FRONTIER FOUND. (Apr. 27, 2016), https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform [https://perma.cc/QXF3-F66F]; *see also* Eric Geller, *Major online privacy bill easily clears first vote in Congress*, THE DAILY DOT (Apr. 13, 2016, 12:00 PM), https://www.dailydot.com/layer8/email-privacy-act-house-judiciary-committee-passage/ [https://perma.cc/GEJ2-H2QJ].

disclose data "that is in electronic storage with or otherwise stored, held, or maintained" when law enforcement was armed with a proper warrant.[94] Any government search or seizure of emails required a search warrant; stored documents only required a subpoena.[95] However, the Email Privacy Act did not differentiate between emails and stored communications older or newer than 180 days, as the current SCA does, so any email search required a warrant.[96] If the government entity was a law enforcement entity, they had to give notice to the consumer if it accessed the consumer's data within ten days, and within three days for any non-law enforcement governmental entity.[97]

The Email Privacy Act would not have actually impacted the warrant requirement for data seizure if it had been enacted. Since the Sixth Circuit decided *United States v. Warshak* in 2010, the Department of Justice's policy already enforced a warrant requirement for electronic data stored with electronic service providers, regardless of the 180 and non-180 day requirements of the SCA.[98] Therefore, this change would have merely codified what the federal government was already doing, and thus maintained the status quo.[99] Modern email storage renders most emails stored in data centers older than 180 days anyway; for example, Google stores about 17,000 emails for the average Gmail user.[100] The notification requirements of three and ten days in the Act only notified a customer after data is seized.[101] Customers would be left to trust the technology company to fight for their rights because they have no recourse before the search occurs. The technology company only risks reputational harm if it does not fight for a customer's rights; for the customer, however, the damage caused could be loss of his confidential communications or work product, and the consequences could be his livelihood or even freedom.

Another Congressional attempt to reform the ECPA, The Law Enforcement Access to Data Stored Abroad Act, recognized the jurisdictional issue that created the holding of the *Microsoft* case, "[N]either ECPA nor subsequent amendments extended the warrant power of courts in the United States beyond the territorial reach of the United States."[102] According to the Act, the location of the data did not matter; instead, the government could properly obtain any data with an adequate warrant if it was for a United States'

94. *See* Email Privacy Act, H.R. 699, 114th Cong. § 3 (2015).

95. *See* Geller, *supra* note 93.

96. *See* THOMPSON & COLE, *supra* note 9, at 9.

97. *Id*. Law enforcement can request a notification delay of not more than 180 days; any other government entity can request a delay of no more than 90 days. *Id* at 10.

98. The Sixth Circuit held email accounts in the purview of third-party services have Fourth Amendment protections and require a warrant for seizure. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); Turner, *supra* note 28, at 04.

99. *See id*.

100. *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, WIRED (July 25, 2012), https://www.wired.com/insights/2012/07/gmail-account-worth/ [https://perma.cc/4S3K-RYVX].

101. *See* THOMPSON & COLE, *supra* note 9, at 10.

102. *See* Law Enforcement Access to Data Stored Abroad Act, S.2871, 113th Cong. § 2 (2014).

citizen.[103] But the court of proper jurisdiction would modify or vacate the warrant if the provider had to violate the laws of a foreign country by giving the United States government the data.[104] Congress recognized that service providers could store customer data in multiple locations and the user is not always in the same country as the data.[105] While the Act did not grant jurisdiction to law enforcement, it did allow the Department of Justice and United States Attorney General to streamline MLAT requests, inventory requests sent and received, and review the data of what is actually received and sent.[106] Unfortunately, the Law Enforcement Access to Data Stored Abroad Act never left the Senate Judiciary Committee.[107] Had the bill made it out of Committee, law enforcement, network providers, and individuals could have more clarity about what determined whether United States law enforcement could search their data. This law clearly allowed United States law enforcement to search the data of any United States citizen, regardless of where the data would be stored.[108] The Law Enforcement Access to Data Stored Abroad Act attempted to address the issue of jurisdiction in contention in *Microsoft*.[109] However, the Act only allows seizure of data of United States citizens subject to legal privacy regimes in other countries.[110]

IV. SUGGESTED AMENDMENTS TO MODERNIZE THE STORED COMMUNICATIONS ACT

The Internet of 1986 only slightly resembles the Internet used today.[111] The drafters of the SCA would not have contemplated regulating cloud storage as a means of storing mass amounts of user data because the public did not have universal access to the Internet in 1986.[112] Now with cloud data, electronic service providers can store customer data at their own discretion, to such an extreme that the data could be fragmented around the world and only legible with the assembly of every single piece.[113] Additionally, at the time of the SCA's enactment, the cost of electronic storage was too high to

103. *See id.*; *see also* Patrick Maines, *The LEADS Act and cloud computing*, THE HILL (March 30, 2015), http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing [https://perma.cc/QG2L-EKS9].

104. *See* S.2871, 113th Cong. § 3 (2014).

105. *See* THOMPSON & COLE, *supra* note 9, at 14.

106. *See* S.2871, 113th Cong. § 4 (2014).

107. *See S.2871 - The Law Enforcement Access to Data Stored Abroad Act*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/senate-bill/2871/committees?q=%7B%22search%22%3A%5B%22Law+Enforcement+Access+to+Data+Stored+Abroad+Act%22%5D%7D&r=1 [https://perma.cc/436J-LURK] (last visited Nov. 19, 2016).

108. *See* S.2871, 113th Cong. § 3 (2014).

109. *See* CONGRESS.GOV, *supra* note 107.

110. *See* THOMPSON & COLE, *supra* note 9, at 14.

111. *See* Kerr, *supra* note 60, at 376.

112. *See* Ellingsen, *supra* note 29.

113. *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CON. L. HEIGHT. SCRUTINY 11, 20-21 (2012) (illustrating Google and Amazon's tendency to fragment consumer data).

contemplate regulating it.[114] In the thirty years since then, costs of storage plummeted and technology companies evolved to turn a profit by charging for electronic storage on their own servers.[115]

The Second Circuit reserved the issue of regulation of data in the cloud for Congress to resolve based on Supreme Court precedent and the lack of explicit law enforcement power to search data overseas in the SCA. Law enforcement does not have any domestic law that specifically guides them in searches of cloud data stored overseas.[116] Individuals are likewise left in the dark as to how the data they entrust to a third party will be stored and when it will be turned over to law enforcement. Network providers have to muddle through interpreting a twentieth century law in a twenty-first century technological world. Until Congress acts, the Supreme Court must grapple with the possible creation of a judicial solution to a legislative problem when *Microsoft* comes for argument before the Court.[117]

An underwater data center solution to the need for data storage can only exacerbate the demand for a legislative update to the SCA. At least with the data stored in Dublin, law enforcement could adhere to an MLAT to search the data.[118] For data stored at sea, there is no means to access the data.

These amendments focus on assuring an informed and consistent law for users and businesses located in the United States to solve the jurisdictional problems presented by the *Microsoft* case and Microsoft's underwater servers.[119] Any changes to the statute should also simplify the structure to enable it to evolve with developments of technology.[120]

A. First Proposed Amendment: United States Law Enforcement Has Jurisdiction Over United States Citizen's Data

United States privacy regulations should follow the data of a United States citizen, regardless of the data location.[121] This clear rule assures and informs United States users that their own domestic law would apply in any search and seizure scenario.[122] Making a citizen subject to the law of his or her own country makes logical sense and likely meets consumer expectations

114. *See* Kerr, *supra* note 60, at 376; *see also* R.J.T. Morris & B.J. Truskowsi, *The Evolution of Storage Systems*, 42 IBM SYS. J. 205, 205-06 (2003) (reviewing the development of electronic storage methods).

115. Kerr, *supra* note 60, at 376.

116. *See Microsoft*, 829 F.3d at 210

117. *See* Jose Pagliery, *Supreme Court to rule if Microsoft must turn over emails stored overseas*, CNN (Oct. 16, 2017, 10:17 AM), http://money.cnn.com/2017/10/16/technology/business/supreme-court-microsoft/index.html?sr=twtech101617supreme-court-microsoft0223PMVODtopLink&linkId=43551689 [https://perma.cc/G37X-J9RH].

118. *See Microsoft*, 829 F.3d at 221.

119. *See* Medina, *supra* note 24, at 292-93.

120. *See id.* at 292.

121. *See* Kerr, *supra* note 60, at 417.

122. *Id.*

since these laws were enacted by their own elected representatives.[123] Data of United States citizens should be subject to search by the United States according to United States law, even if it is stored abroad, as long as the warrant satisfies probable cause.

This proposed amendment would not be a new concept in Congress. The Law Enforcement Access to Data Stored Abroad Act proposed a similar requirement but allowed for other countries' laws to dictate whether the search could proceed.[124] The intent of a uniform rule is laudable, however, another country interfering with an investigation of a United States citizen by United States law enforcement only creates more ambiguity. The bureaucratic hold-up multiplies with the approach in the Law Enforcement Access to Data Stored Abroad Act because law enforcement must garner approval for the warrant and have the judge interpret the laws of the country in which the data is physically located to determine whether the search would be lawful.[125] A clear rule, free of any other country's privacy laws, will create transparency for law enforcement, individuals, and businesses.

For example, laws governing computer crimes grant United States law enforcement jurisdiction abroad despite geographic boundaries.[126] These laws permit United States law enforcement to "pursue not only international cases that originate or conclude in the United States, but also those cases where networks or computers in the United States are merely used as pass-throughs."[127] This broad jurisdiction could lead Congress to adopt similar language to pursue cases against United States citizens, regardless of their personal or technological location. That the same principle and definition exists in a current law should allow for seamless adaptation to the SCA.

This proposed amendment would not burden technology companies that host data centers. *Microsoft* was not about whether Microsoft could transfer the data; the issue centered on whether the SCA compelled Microsoft to do so.[128] The servers used for cloud data storage are designed to quickly transmit data around the world regardless of their location. Technology companies build these servers to make the data transfer even faster and withstand the increase in cloud computing demand.[129] Microsoft can easily

123. *See* Marketa Trimble, *Second Circuit's Decision In Microsoft v. U.S. (Data Stored in Ireland): Good News For Internet Users?*, TECH. & MKTG. LAW BLOG (Aug. 1, 2016), https://blog.ericgoldman.org/archives/2016/08/second-circuits-decision-in-microsoft-v-u-s-data-stored-in-ireland-good-news-for-internet-users-guest-blog-post.htm [https://perma.cc/6VC2-JXJK].

124. *See* S.2871, 113th Cong. § 3 (2014).

125. *See* CONGRESS.GOV, *supra* note 107 ("A court issuing a warrant pursuant to this subsection, on a motion made promptly by the service provider, shall modify or vacate such warrant if the court finds that the warrant would require the provider of an electronic communications or remote computing service to violate the laws of a foreign country.").

126. *See* Herrera-Flanigan, *supra* note 30, at 320 (including the National Information Infrastructure Protection Act, the U.S.A. Patriot Act and the Computer Fraud and Abuse Act, which amended the definition of "protected computer" to include those involved in interstate or *foreign* commerce).

127. *Id*. at 325.

128. *See* Henning, *supra* note 12.

129. *See* Markoff, *supra* note 5.

transfer its data across the globe with a keystroke when compelled to do so by a warrant or MLAT agreement.[130]

However, this amendment will inevitably cause controversy within countries from which the data seizure occurs. For example, all member states in the European Union ("EU") classify privacy as a fundamental right-the United States does not hold privacy in such a high regard.[131] The United States and the EU have already clashed on the movement of data overseas.[132] There will inevitably be another disagreement of privacy rights with this amendment's enactment. However, the amendment impacts only those who are United States citizens. The amendment gives no authority for seizure of data from other countries' citizens that may maintain different privacy expectations. Further, countries like Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, and the United Kingdom cannot conflict with the United States over this amendment because their laws already empower them to access data stored outside their own borders.[133]

B. Second Proposed Amendment: United States Law Enforcement Has Jurisdiction Over Data Physically Stored in the United States

Congress should impose jurisdiction over data stored in data centers located in the United States.[134] This way, courts assert jurisdiction over companies because of the location of the data and, more than likely, this data is for users in the United States who may not be citizens or cannot be identified as such.[135] This improves the customer experience by assuring the quick delivery of their data.[136]

Without this amendment, electronic service providers could evade civil and criminal investigations and charge consumers a premium for their privacy

130. *See* Henning, *supra* note 12.

131. *See* Steven S. McCarty-Snead & Anne Titus Htlby, *Research Guide to European Data Protection Law*, 42 INT'L J. LEGAL INFO. 348, 350 (2014) (maintaining the fundamental privacy right through the European Convention for Human Rights and the Charter of Fundamental Rights); *see also* Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661, 671 (1999).

132. *See* Mark Scott, *In Europe-U.S. Clash on Privacy, a Longstanding Schism*, N.Y. TIMES (Oct. 7, 2015), https://www.nytimes.com/2015/10/08/technology/in-europe-us-clash-on-privacy-a-longstanding-schism.html?mtrref=www.google.com&gwh=4540E44F9CD47CA4B0CD0E2F8086A12A&gwt=pay [https://perma.cc/63LG-VFA5].

133. *See* Winston Maxwell & Christopher Wolf, *A Global Reality: Government Access to Data in the Cloud* (May 23, 2012), https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf [https://perma.cc/Y5QR-Y8QD].

134. *See* Trimble, *supra* note 123. The government argued for this interpretation of the SCA in *Microsoft Corp. v. United States*. Ely, *supra* note 58.

135. *See* Trimble, *supra* note 123.

136. Companies like Microsoft store data close to the user to increase the speed at which it is delivered. *See Microsoft*, 829 F.3d at 202; Markoff, *supra* note 5.

and security.[137] This creates a massive loophole that does not exist in physical data.[138] The United States government, just like in *Microsoft*, would be unable to access data when pertinent in an attempt to prosecute for illicit activity, despite the physical location of the data, without this amendment.[139]

In the alternative, Congress could amend the SCA to mandate data localization, company servers' location in the United States, and simultaneously gain jurisdiction.[140] This leaves great power with the government so that companies cannot dictate their own policy about the cloud and consumer data.[141] Yet, a mandate like this is increasingly unfeasible in the global Internet landscape and would increase costs greatly for technology companies.[142] A proposal like this is unlikely to succeed after recent progress by the EU to fight forced data localization.[143] Further, considering the power of technology companies to lobby Congress, mandating that all servers for United States companies must be stored in the United States is impracticable.[144] The alternative, for jurisdiction to search any data servers within the United States with a warrant based on probable cause, is much more realistic.

C. Third Proposed Amendment: Law Enforcement Needs a Search Warrant and Notice Requirement for Search of Any Electronic Communications

State and federal law require a governmental entity and law enforcement to have a warrant in order to search a suspect's home.[145] Currently, the SCA provides lower privacy protections for data stored through cloud computing than the protections afforded to data on an individual's physical computer or hard drive.[146] The SCA only enforces a warrant requirement in some cases, but not in others.[147] This proposed amendment

---

137. *See* Henning, *supra* note 12 (discussing the potential profit in "Crim Mail", a hypothetical service that would charge customers a premium to hide their data around the globe so as to deny feasibility in government searches).

138. *See Microsoft*, 829 F.3d at 220-21.

139. *See id.* at 221.

140. *See* Trimble, *supra* note 123.

141. *Id.*

142. *See* Woods, *supra* note 64 (questioning whether the cost would actually matter for a flush company like Google).

143. *See* Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17, 2017, 3:19 PM), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/3YWM-W5EH]; *see also* Trade in Service Agreement (TiSA) Annex on [Electronic Commerce] (Sept. 16, 2013), https://wikileaks.org/tisa/document/201505_Annex-on-Electronic-Commerce/201505_Annex-on-Electronic-Commerce.pdf [https://perma.cc/H7A6-W2E7].

144. *See* Trimble, *supra* note 123.

145. *See* Ozer & Conley, *supra* note 3.

146. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 43 (2013).

147. *See* Kerr, *supra* note 60, at 387 (discussing limits of the SCA such as warrant requirement based on timing and provider status).

ensures protection for old emails and data stored through services, like Google Drive, while the current statute fails to protect the data with a warrant on both counts.[148] The age of data is not a relevant barometer in evaluating the level of protections it should be afforded.[149] With almost 250 million Americans on the Internet, the lack of required data protections is concerning.[150] The government must have a warrant to access these users' electronic communications.[151] The Email Privacy Act and the Law Enforcement Access to Data Stored Abroad Act called for similar warrant protections for data so that a mere subpoena did not grant law enforcement access to electronically stored data because of the age of the data.[152]

Building on existing privacy protection, this amendment mandates probable cause for a warrant, ensuring that law enforcement cannot seize a United States citizen's data by requesting it from a country that does not hold privacy rights to such a high bar. Otherwise, users have no guarantee about the existence or quality of other countries' surveillance laws that govern access to data stored within that country's physical jurisdiction.[153] These laws are also subject to change depending on power shifts and developing technology and could therefore leave users with a lower standard than probable cause to protect their data from government seizure.[154]

Google discloses to users the number of subpoenas and warrants requested under the ECPA and fulfilled by Google for United States law enforcement.[155] There were 8,182 subpoena requests from law enforcement to Google from January to July of 2016.[156] The number of requested search warrants are only about half that, 4,246, for that time period.[157] Google fulfilled 76% and 85% of these requests, respectively.[158] Google notifies the user that law enforcement has requested their data unless the request is pursuant to an emergency request or a gag order.[159] Fifteen of the twenty-four companies surveyed by the Electronic Frontier Foundation always notify a

148. *Id*.

149. *Id.* at 393.

150. *See United States*, ICT DEVELOPMENT INDEX 2016, http://www.itu.int/net4/ITU-D/idi/2017/index.html [https://perma.cc/64WJ-CJ9B] (last visited Feb. 17, 2018).

151. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299-300 (2004).

152. *See* THOMPSON & COLE, *supra* note 9, at 9, 13-15.

153. *See* Jennifer Granick, *The Microsoft Ireland Case and the Future of Digital Privacy*, JUST SEC. (July 18, 2016, 12:46 PM), https://www.justsecurity.org/32076/Microsoft-ireland-case-future-digital-privacy/ [https://perma.cc/A2DR-EQ8T].

154. *Id*.

155. *See Transparency Report: United States*, GOOGLE, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US [https://perma.cc/PTU2-BTNF] (last visited Feb. 17, 2018).

156. *Transparency Report: United States*, GOOGLE, https://perma.cc/V9SJ-T332 (last visited Dec. 13, 2016).

157. *Id*.

158. *Id*.

159. *See Transparency Report: Legal process*, GOOGLE, https://perma.cc/9SSS-24L7 (last visited Dec. 13, 2016).

user when the government submits any kind of data request.[160] These few technology companies invest in user notice because a governmental entity is not required by the SCA to always notify the subscriber or customer of the subpoena or search warrant execution.[161] Even where notification is required, law enforcement can delay fulfilling the requirement.[162] This practice is fundamentally unfair and undermines an individual's right to due process if the person is not notified or receives delayed notification through an SCA loophole. Individuals are left to trust technology companies to protect their data and fight for their rights, despite such companies' main incentive to protect their consumer base.

D. Amendment Application to Microsoft Corp. v. United States and Microsoft's Underwater Data Centers

The United States never disclosed the citizenship of the suspect in *Microsoft*.[163] Thus, this note proceeds in hypotheticals to determine the effectiveness of the above proposals. Microsoft stores customer data in the "general" area of which the customer is located, based on a customer's selected location preference.[164] If the customer is a United States citizen, the first proposed amendment would circumvent the preferred location to grant law enforcement access to search the data with a valid search warrant. None of the proposed amendments would help the investigation if the customer was not a United States citizen unless Microsoft stored his data on a United States server. This country's law enforcement does not need the power to search everyone's data, nor should they. United States citizens and businesses understand our country's laws and make a conscious choice to retain citizenship and do work here, and therefore, are subject to United States law.

The second suggested amendment provides United States courts and law enforcement jurisdiction over the underwater data centers that connect to the United States. Each data center, whether it floats in the ocean or rests on the ocean floor, must connect to the mainland to transmit the data to the company or the user.[165] Since the data center needs to link to an office and control center, the company operating the data center needs to maintain a physical presence within the geographical borders of the United States, thus giving the underwater data centers a geographic location for searches.

The third amendment does not solve the issues presented by *Microsoft* or the underwater data servers. However, it would protect customers in this

160. Who Has Your Back?, ELEC. FRONTIER FOUND., https://perma.cc/N4M6-34PU (last visited Dec. 13, 2016).

161. *See* 18 U.S.C. § 2703(b).

162. *See* Orin S. Kerr, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act: Surveillance Law: Reshaping the Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233-34 (2004).

163. *See Microsoft*, 829 F.3d at 203 (revealing the warrant only asked for the email address).

164. *Id*. at 202.

165. *See* Markoff, *supra* note 5.

constantly evolving world of technology by holding the government to a probable cause standard no matter the type or age of the data.[166] The Internet and the cloud will inevitably evolve to allow for more storage for various types of data, to the point where it will be a user's main use of electronic storage.[167] This mass of data should be protected like a physical data and should not be discriminated against because it may be easier to access.

V. CONCLUSION

The Stored Communications Act revolutionized the privacy laws of the Internet in 1986. Yet, the rapid development of the world of technology and the lack of modernization to the law curtailed its effectiveness. Judge Lynch recognized that the *Microsoft* decision was the byproduct of an ineffective statute to govern that particular set of facts. Law enforcement should not have access to all data stored around the world, but Congress needs to empower, not hamper, them in doing their jobs effectively by allowing them access to the data of United States citizens. The current Stored Communications Act does the former. Recent Congressional attempts have similarly been insufficient to amend this foundational statute. Even though the Supreme Court granted *certiorari* to hear the case, Congress must act to create a thorough legislative solution to deal with the domestic and international issues posed in *Microsoft*.

The record of *Microsoft* is silent as to the citizenship of the suspect. If he was a United States citizen, the first proposed amendment in this note would govern the proper seizure of the data based on probable cause. The underwater data centers would fall under the jurisdiction of United States jurisdictions in accordance with the first and second proposals. Whether the data is anchored to the sea floor or floating off the California coast, it is operated by a United States company and likely contains the data of United States citizens living close to the coast.

The legal landscape surrounding data, Congress, and law enforcement in this area is complicated. There are a number of players and considerations to factor in on the domestic and international levels. The proposed amendments in this note are not exhaustive in the mission to fully rectify the Stored Communications Act. There is much more to contemplate regarding differentiating data types, international ramifications, and surveying the methodologies of cloud storage companies for an impactful and nuanced solution. Congress must update the Stored Communications Act to balance the interests of users, United States citizens, international implications, and law enforcement.

166. These ideas of data distinction and age are further discussed in Kerr, *supra* note 60, at 376.

167. *See* Anderson & Rainie, *supra* note 75.

Taxing the Nontaxable: Are State and Local Governments Allowed to Tax Internet Streaming Service Providers?

Michael Wallace *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. A native Arkansan, I attended Harding University for my undergraduate studies, where I graduated magna cum laude with a B.S. in Public Administration. I would like to thank Jodie Griffin for her feedback and guidance regarding this note. Last, but not least, I would like to thank my father, Robert Wallace, and mother, Cynthia Wallace, for all of their support and encouragement throughout my life and academic career.

I. INTRODUCTION

For Netflix, Hulu, and other Internet streaming service providers ("ISSPs"), the years 2015 through 2017 have been filled with confusion and frustration. ISSPs are required to collect and remit varying tax amounts from customers based on state and local governments' sales and use tax codes.[1] Yet, imposing such taxes violates the Permanent Internet Tax Freedom Act, burdens interstate commerce in violation of the Commerce Clause by requiring the ISSP to sort through hundreds of tax codes, and possibly violates the Due Process Clause of the Fourteenth Amendment by enforcing statutes and regulations on companies that are not under the state or local government's jurisdiction.

The application of existing state and local governments' sales and use tax codes imposes a substantial burden on ISSPs. According to the Federal Communications Commission ("FCC"), "the current patchwork of state and local laws and regulations relating to taxation of digital goods and services . . . may hinder new investment and business models,"[2] thus hindering interstate commerce. For example, a double or triple taxation issue could arise if a resident of Washington, D.C. streams a video through an ISSP based in California during a layover at Dallas Fort Worth International Airport, and each jurisdiction claimed a right to tax the streamed video.[3] Adding to the complexity and confusion, "some [state and local governments] tax [online sales] as part of the sales tax imposed on tangible personal property; others tax them as a separate category of services."[4] Furthermore, each taxing jurisdiction differs on the content and products that are subject to be tax.[5]

Various sources of law, however, suggest that it is impermissible to require ISSPs to collect and remit sales and use taxes.[6] The United States Congress enacted the Internet Tax Freedom Act in 1998, which prohibited the

---

1. *See generally* Jason Henry, *Pasadena Will Tax Netflix, Hulu and Your City Might be Next*, SAN GABRIEL VALLEY TRIBUNE (Sept. 27, 2016) http://www.mercurynews.com/2016/09/27/pasadena-will-tax-netflix-hulu-and-your-city-might-be-next/ [https://perma.cc/N8S8-WYRZ]; *see generally* Jennifer Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*, PwC (Sept. 9, 2015) http://ebiz.pwc.com/2015/09/us-the-disparate-state-and-local-tax-treatment-of-digital-streaming-services-2/ [https://perma.cc/7ERV-JYE6]; *see generally* Vidya Kauri, *'Netflix Tax' On Digital Downloads Takes Effect in Pa.*, LAW 360 (Aug. 3, 2016) https://www.law360.com/articles/824535/print?section=corporate [https://perma.cc/TG7F-2QL5].

2. FCC, *Connecting America: The National Broadband Plan* (2014), at 58, https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

3. *See* Jeremy Bui, The Permanent Internet Tax Freedom Act, H.R. 3086, 113th Congress (2014), 23 COMM. LAW CONSPECTUS 536, 537 (2014).

4. Delta, George B. and Matsuura, Jeffrey H., *Law of the Internet: State Taxation of Electronic Commerce*, Aspen Publishers, §15.06(B)(1) (2016).

5. *Id.*

6. *See e.g.*, Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, §922(b), 130 Stat. 122, 281 (2016); *Quill Corp. v. North Dakota*, 504 U.S. 298, 317 (1992).

introduction of new taxes on Internet access.[7] In 2016, Congress passed the Trade Facilitation and Trade Enforcement Act, which extended the Internet Tax Freedom Act's applicability to 2020.[8] Importantly, ISSPs fall within the category of "Internet access" as defined by the Internet Tax Freedom Act.[9] Further, a state or local government violates the Commerce Clause by requiring an ISSP to collect and remit sales and use taxes, unless the ISSP has a "substantial nexus" with the taxing jurisdiction.[10] Finally, the exercise of jurisdiction over ISSPs by state and local governments may also violate the Due Process Clause.[11]

A. Internet Streaming Service Providers Are Faced with A Confusing Web of Conflicting Consumer Taxation Laws

ISSPs are in a state of confusion regarding its tax obligations for online streaming services. State and local governments have passed and implemented legislation and regulations that require ISSPs to collect and remit sales and use taxes.[12] However, Congress intended to prevent the taxation of Internet access when it permanently extended the Internet Tax Freedom Act in 2016.[13] In addition, the Commerce Clause and the Due Process Clause limit the actions of state and local governments.[14] In 1992, the United States Supreme Court held that a "substantial nexus" is required for states to force out-of-state sellers to collect and remit taxes from customers, formulating a test for imposing sales and use taxes on out-of-state companies.[15] In order for a state or local government to tax an ISSP, the Due Process Clause requires the company to be "physically present" in the jurisdiction or "purposefully direct[] its activities" at residents of the jurisdiction.[16] Yet, state and local jurisdictions continue to pass legislation

7. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 (2012); Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999, Pub. L. No. 105-277, § 1101(a)(1), 112 Stat. 2681, 2681-719 (1998).

8. *See* Trade Facilitation and Trade Enforcement Act of 2015 § 922(b).

9. 47 U.S.C. 231

10. *See id.*; *Quill*, 504 U.S. at 313.

11. *See* U.S. CONST. amend. XIV, § 1.

12. *See* Kauri, *'Netflix Tax' On Digital Downloads Takes Effect in Pa.*, *supra* note 1; Sales, Use & Hotel Occupancy Tax Bulletin 16-001, PENNSYLVANIA DEPARTMENT OF REVENUE (July 21, 2016), http://www.revenue.pa.gov/GeneralTaxInformation/TaxLawPolicies BulletinsNotices/Documents/Tax%20Bulletins/SUT/st_bulletin_16-001.pdf; Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*, *supra* note 1; Henry, *Pasadena Will Tax Netflix, Hulu and Your City Might be Next*, *supra* note 1.

13. *See* Trade Facilitation and Trade Enforcement Act of 2015, at Sec. 922; Internet Tax Freedom Act, *supra* note 7.

14. *See* U.S. CONST. Art. 1, § 8, cl. 3 (2016); U.S. CONST. amend. XIV, at § 1.

15. *See e.g.*, *Quill v. North Dakota*, 504 U.S. 298. To note, *South Dakota v. Wayfair, Inc.*, a case challenging the "substantial nexus" test developed in *Quill*, is currently before the U.S. Supreme Court, with a decision to be issued by the end of the term, June 2018.

16. *See* Quill v. North Dakota, 504 U.S. at 306-08.

that subject ISSPs to various and differing sales and use taxes.[17] ISSPs are therefore uncertain as to whether they are required to collect and remit sales and use taxes. With all of this confusion, what should ISSPs do? The answer to this question rests on how the courts interpret the interplay of the Permanent Internet Tax Freedom Act, the "substantial nexus" requirement of the Commerce Clause, and the Due Process Clause.[18] This Note argues that state and local governments are not permitted to require ISSPs to collect and remit sales and use taxes because doing so would violate the Permanent Internet Tax Freedom Act, the Commerce Clause, and possibly the Due Process Clause.

This Note looks at past and present legislation, case law, congressional intent, and agency and commission recommendations to conclude that state and local governments are not permitted to require ISSPs to collect and remit sales and use taxes. In doing so, this Note explores how courts should address the issue of multiple and differing methods of taxation, and the overall burden on interstate commerce that arises by the taxation of ISSPs by state and local governments. Part II provides a brief background on the developments affecting the taxation of ISSPs. Part III outlines a three-part argument as to why courts should prohibit state and local governments from requiring ISSPs to collect and remit sales and use taxes. The contentions are (1) the Permanent Internet Tax Freedom Act prohibits ISSP taxation, (2) such taxation violates the Commerce Clause by placing an undue burden on interstate commerce, and (3) the imposition of such tax laws on ISSPs may violate the Due Process Clause.

II. THE CONFUSION AND COMPLEXITY FACING INTERNET STREAMING SERVICE PROVIDERS

With the advent of Internet video streaming in the late 2000's, cities and states have tried to recuperate some of their lost tax revenue by taxing ISSPs.[19] For example, Netflix was founded in 1997, but it was not until 2007 that Netflix started providing online streaming service in the United States.[20] Hulu, another ISSP, launched its streaming services in 2008.[21] Because of

17. *See* Kauri, *'Netflix Tax' On Digital Downloads Takes Effect in Pa.*, *supra* note 11; *see* Sales, Use & Hotel Occupancy Tax Bulletin 16-001, *supra* note 11; *see* Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*; *see* Henry, *Pasadena Will Tax Netflix, Hulu and Your City Might be Next*, *supra* note 11.

18. *See* Trade Facilitation and Trade Enforcement Act of 2015 at Sec. 922; *see generally* Quill v. North Dakota, 504 U.S. 298; *see* U.S. Constitution Art. 1, § 8, cl. 3; *see* U.S. Constitution Amend. XIV, § 1.

19. *See* Mary Benton and Zach Gladney, *From the Litigators' Desks: The Future in State Taxation of the Cloud and an Enduring Guiding Principle*, 26 J. MULTISTATE TAX'N AND INCENTIVES, 14, 14 (2016).

20. *See Netflix's View: Internet TV is Replacing Linear TV*, NETFLIX, https://ir.netflix.com/long-term-view.cfm [https://perma.cc/J5HS-88MK] (last updated Jan. 18, 2017).

21. *See About Hulu*, HULU, https://www.hulu.com/press/about [https://perma.cc/6T6N-YV4M] (last visited Nov. 12, 2017).

these technologies, the traditional tax bases, including cable video services and in-store video rentals, are diminishing, thereby increasing the pressure on state and local governments to expand their tax reach.[22]

Therefore, cities and states are rapidly, and increasingly, passing new statutes and regulations levying various taxes on ISSPs.[23] Some cities and states tax ISSPs under their general sales tax. Searcy, Arkansas, for example, applies a sales tax rate of 9.5% on Internet video streaming.[24] In Pennsylvania, on the other hand, ISSPs are required to charge customers "a 6[%]sales tax on digital downloads."[25] The "digital tax" went into effect August 1, 2016, and required sellers to "collect [sales] tax on digitally or electronically delivered or streamed video," therefore adding an additional six percent to their monthly fee.[26]

Another method of taxing ISSPs is through use and excise taxes.[27]Washington State passed an act in 2009 amending its existing excise taxation policy to include the taxation of digital products.[28] This amendment permitted the taxation of digital goods to "protect the sales and use tax base [of the state]."[29] The city of Chicago implemented an amusement tax on ISSPs in September 2015.[30] The Chicago Department of Finance specified that "the [city's] amusement tax applies to charges for the privilege to witness, view,

---

22. *See* Benton and Gladney, *supra* note 18, at 14; *see also Catherine* Chen, *Taxation of Digital Goods and Services*, 70 N.Y.U. ANN. SURV. AM. L. 421, 422-24 (2015).

23. *See* Kauri, *'Netflix Tax' On Digital Downloads Takes Effect in Pa.*; *see generally* Engrossed Substitute House Bill, 2075 § 101, 61st Washington State Legislature (2009); *see* Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*; *see* Henry, *Pasadena Will Tax Netflix, Hulu and Your City Might be Next*.

24. *See State Tax Rates*, ARKANSAS DEPARTMENT OF FINANCE AND ADMINISTRATION, http://www.dfa.arkansas.gov/offices/exciseTax/salesanduse/Pages/StateTaxRates.aspx [https://perma.cc/MM9F-6QT8] (last visited Mar. 3, 2018); see List of Cities and Counties with Local Sales and Use Tax, ARKANSAS DEPARTMENT OF FINANCE AND ADMINISTRATION, http://www.dfa.arkansas.gov/offices/exciseTax/salesanduse/Documents/cityCountyTaxTable.pdf [https://perma.cc/G73P-HRS7] (last visited Mar. 3, 2018). *See also* https://www.arktimes.com/ArkansasBlog/archives/2017/02/10/amazon-set-to-begin-collecting-sales-tax-on-arkansas-purchases-in-march [https://perma.cc/X29P-6KJD] (last visited Mar. 3, 2018).

25. *See* Kauri, *'Netflix Tax' On Digital Downloads Takes Effect in Pa.*; *see also* Sales, Use & Hotel Occupancy Tax Bulletin 16-001.

26. *See* Sales, Use & Hotel Occupancy Tax Bulletin 16-001.

27. A use tax is a "tax on purchases made outside one's state of residence on taxable items that will be used, stored or consumed in one's state of residence and on which no tax was collected in the state of purchase. https://www.investopedia.com/terms/u/use-tax.asp [https://perma.cc/Q6L3-ZKSU] (last visited Mar. 3, 2018); An excise tax is "an indirect tax charged on the sale of a particular good [that] is not directly paid by an individual consumer; instead, the Internal Revenue Service levies the tax on the producer or merchant, who passes the tax onto the consumer by including it in the product's price." https://www.investopedia.com/terms/e/excisetax.asp [https://perma.cc/X6QS-V5LD} (last visited Mar. 3, 2018).

28. *See generally* Engrossed Substitute House Bill.

29. *Id.* at § 101(3)(a).

30. *See* Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*.

or participate in an amusement either in person or *electronically delivered*."[31] Therefore, citizens of Chicago now pay a nine percent amusement tax on top of the membership fee Netflix, Hulu, and other ISSPs charge.[32] Chicago requires the ISSPs to collect and remit the tax if the customer's residential street address or primary business address is in Chicago"[33] Chicago consumers have challenged the city's amusement tax on ISSPs by claiming that the application of the amusement tax on Internet streaming services violates the Permanent Internet Tax Freedom Act and the Commerce Clause.[34]

Other cities and states tax ISSPs under service taxes. In California, ISSPs may be subject to the service tax rate applied to cable providers in up to 46 cities in the near future.[35] One of those cities, Pasadena, decided that an existing "9.[%] tax on 'video services' [will apply] to subscribers of streaming video providers."[36] On the other side of the country, the state of Florida currently taxes ISSPs under "Florida's communications services tax."[37]

In sharp contrast, some states do not tax ISSPs at all. The state of Idaho, for example, clarified that "streaming services are not subject to tax."[38] Similarly, Alabama briefly considered enacting a streaming tax, but abandoned the measure after pressure from its citizens.[39] As a result, ISSPs are faced with the burden of interpreting, applying, collecting, and remitting taxes according to multiple state and local governments' sales and use tax codes.

III. STATE AND LOCAL GOVERNMENTS CANNOT REQUIRE INTERNET STREAMING SERVICE PROVIDERS TO COLLECT AND REMIT SALES AND USE TAXES

The Permanent Internet Tax Freedom Act, the Commerce Clause, and possibly the Due Process Clause prohibit state and local governments from requiring ISSPs to collect and remit sales and use taxes. The Permanent Internet Tax Freedom Act prohibits the taxation of Internet access.[40] The Commerce Clause allows the U.S. Congress to regulate commerce "among the several states;" thus regulation of commerce by states and localities that

31. *Id.* (emphasis added).
32. *See id.*
33. *Id.*
34. *See generally* Labell v. Chicago, Case No. 2015 CH 13399 (Cir. Ct. Cook Cty. Ill. July 21, 2016) (opinion and order on motion to dismiss).
35. *See* Henry, *Pasadena Will Tax Netflix, Hulu and Your City Might be Next*.
36. *Id.*; *see also* Pasadena, Cal. Code of Ordinances 4.56.070 (2017); https://www.municode.com/library/ca/pasadena/codes/code_of_ordinances?nodeId=TIT4REFI_CH4.56UTUSTA.
37. *See* Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*.
38. *Id.*
39. *See id.*
40. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 Note at Sec. 1101(a).

affects interstate commerce would violate Congress's constitutional right to regulate interstate commerce.[41] The Due Process Clause prohibits the taxation of a company that is not physically present in the jurisdiction or does not "purposefully direct[] its activities" at residents of the jurisdiction.[42] Therefore, state and local governments are prohibited from requiring ISSPs to collect and remit ales and use taxes. Due to the already existing legislation and Constitutional requirements, there is no need for legislative reform if the courts apply these requirements correctly.

A. The Permanent Internet Tax Freedom Act

In 1998, Congress prohibited state and local governments from taxing Internet access by passing the Internet Tax Freedom Act.[43] The Internet Tax Freedom Act specifically stated that:

> No State or political subdivision thereof shall impose any of the following taxes during the period beginning on October 1, 1998, and ending 3 years after the date of the enactment of this Act – (1) taxes on Internet access, unless such tax was generally imposed and actually enforced prior to October 1, 1998; and [(2)] multiple or discriminatory taxes on electronic commerce.[44]

The Internet Tax Freedom Act was extended a total of five times before Congress decided to enact the permanent moratorium in 2016.[45]

The Permanent Internet Tax Freedom Act made the moratorium on the taxation of Internet access created by the Internet Tax Freedom Act permanent.[46] The permanent moratorium effectively prohibits all state and local governments from creating and applying sales and use taxes to ISSPs because of the applicability and purpose of the Permanent Internet Tax Freedom Act.[47]

The Permanent Internet Tax Freedom Act maintained the same language as the Internet Tax Freedom Act.[48] Accordingly, the Permanent Internet Tax Freedom Act also defined Internet access service as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet and may also include access to proprietary

41. *See* U.S. Constitution Art. 1, § 8, cl. 3.

42. *See* Quill v. North Dakota, 504 U.S. at 306-08 (citing Miller Brothers Co. v. Maryland, 347 U.S. 340, 344-45 (1954)).

43. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 Note.

44. *See id.* at Sec. 1101(a).

45. *See* "The Permanent Internet Tax Freedom Act," 23 COMM. LAW CONSPECTUS at 537; Trade Facilitation and Trade Enforcement Act of 2015 at Sec. 922.

46. *See* Trade Facilitation and Trade Enforcement Act of 2015 at Sec. 922.

47. 47.U.S.C. §151 Note at Sec. 1101(a).

48. *See* "The Permanent Internet Tax Freedom Act," 23 Comm. Law Conspectus at 537; Trade Facilitation and Trade Enforcement Act of 2015 at Sec. 922.

content, information, and other services as part of a package of services offered to consumers."[49]

Of note, during the 114th Congress, the Marketplace Fairness Act of 2015 and the Digital Goods and Services Tax Fairness Act of 2015 were introduced into the Senate.[50] The Marketplace Fairness Act would "require all sellers . . . to collect and remit sales and use taxes with respect to remote sales . . . "[51] The Digital Goods and Services Tax Fairness Act would require a seller to "be responsible for collecting and remitting the correct amount of tax for the State and local jurisdictions whose territorial limits encompass the customer tax address . . . ."[52] However, neither of these proposed pieces of legislation have moved out of committee, and therefore, are not applicable.[53]

1. Applicability of the Permanent Internet Tax Freedom Act

The Permanent Internet Tax Freedom Act explicitly preempts state and local government laws that permit taxing ISSPs In cases where federal law conflicts with state law, courts have held that preemption under the Supremacy Clause applies when the federal law explicitly says so.[54] In *English v. General Electric Company*, the United States Supreme Court emphasized that state law is preempted by federal law "when Congress has made its intent known through explicit statutory language…."[55] Congress's explicit direction that "[n]o State or political subdivision thereof may impose any . . . [t]axes on Internet access . . . or discriminatory taxes on electronic commerce" demonstrates that the Permanent Internet Tax Freedom Act is meant to preempt any state or local law establishing such taxes.[56] Therefore, state and local tax laws that conflict with the Permanent Internet Tax Freedom Act are preempted and impermissible.

Further, ISSPs fall under the protection of the Permanent Internet Tax Freedom Act according to the explicit statutory language. The Permanent Internet Tax Freedom Act defines Internet access service as "a service that enables users to access content, information . . . or other services offered over the Internet and may also include access to proprietary content, information, and other services as part of a package of services…."[57] Netflix, for example,

---

49. Internet Tax Freedom Act, 47 U.S.C. § 151 Note, at Sec. 1101(d)(3)(D).

50. *See* S. 698 – Marketplace Fairness Act of 2015, 114th Congress, https://www.congress.gov/bill/114th-congress/senate-bill/698; S. 851 – Digital Goods and Services Tax Fairness Act of 2015, 114th Congress, https://www.congress.gov/bill/114th-congress/senate-bill/851

51. *See* S. 698 - Marketplace Fairness Act of 2015.

52. S. 851 – Digital Goods and Services Tax Fairness Act of 2015.

53. *See* S. 698 - Marketplace Fairness Act of 2015; *see* S. 851 – Digital Goods and Services Tax Fairness Act of 2015.

54. *See* Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 95-98 (1983).

55. English v. General Elec. Co., 496 U.S. 72, 78-79 (1990).

56. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 Note at Sec. 1101(a).

57. *Id.* at Sec. 1101(e)(3)(D).

offers video streaming services over the Internet, allowing "[m]embers [to] watch as much [videos] as they want, anytime, anywhere, on nearly any Internet-connected screen."[58] Netflix thus provides a "service that enables users to access content . . . offered over the Internet," and should be classified under Internet access.[59] Therefore, Netflix and similar ISSPs are encompassed within the statutory definition of Internet access service and should be protected by the tax prohibition created by the Permanent Internet Tax Freedom Act.

Proponents of taxing ISSPs might argue that ISSPs are comparable to cable providers and should be classified and taxed as such.[60] However, such a comparison is flawed because ISSPs do not meet the definition of a cable system as defined by statute and interpreted by courts. Because the Permanent Internet Tax Freedom Act does not deal with cable systems, this Note looks to other statutes for the definition of a cable system. According to the Copyright Act

> A "cable system" is a facility, located in any State, territory, trust territory, or possession of the United States, that in whole or in part receives signals transmitted or programs broadcast by one or more television broadcast stations licensed by the Federal Communications Commission, and makes secondary transmissions of such signals or programs by wires, cables, microwave, or other communications channels to subscribing members of the public who pay for such service.[61]

ISSPs do not clearly fit within the definition of a cable system established by Congress and thus, they cannot be classified as such. ISSPs do not "receive signals transmitted or programs broadcast by one or more television broadcast stations."[62] Netflix, for example, acquires its content through licensing deals with owners and suppliers, as well as by creating its own content.[63] Netflix does not receive its content from transmitted signals or broadcast programs and, accordingly, is not a cable system. Furthermore, Netflix transmits all of its content on its "Open Connect" system, which is comprised of a network of servers accessed through Internet service

58. *See generally* Netflix Media Center, *About Netflix: Netflix Has Been Leading the Way for Digital Content Since 1997*, https://media.netflix.com/en/about-netflix [https://perma.cc/LNC2-ZEM9] (accessed Dec. 28, 2016). According to the website, "Netflix is the world's leading *Internet* television network…."

59. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 Note at Sec. 1101(e)(3)(D).

60. *See, e.g.*, *Netflix, Inc. v. Finance and Administration Cabinet Dep't of Revenue*, Order No. K-24900 at 2 (Kentucky Bd. Tax App. Sept. 23, 2015).

61. 17 U.S.C. § 111(f)(3) (2012).

62. *Id.*

63. *See Netflix's View: Internet TV is Replacing Linear TV*, NETFLIX, https://ir.netflix.com/long-term-view.cfm (updated April 18, 2016).

providers.[64] Netflix is not transmitting "such signals or programs by wires, cables, microwave, or other communications channels," but is simply allowing access to the content on the servers.[65] As a result, Netflix and other ISSPs cannot properly be classified as cable systems because they do not meet any applicable statutory definition.

Courts have also held that ISSPs fail to satisfy the definition of a cable system contained in the Copyright Act. In *Fox Television Stations, Inc. v. FIlmOn X, LLC*, a case regarding broadcast licensing, the District Court for the District of Columbia held that a company that uses the Internet to transmit content is not a cable system.[66] The Court's reasoning centered around the fact that, "cable companies . . . receive the signals and directly retransmit them by coaxial cable, wires, or microwave links to their subscribers[; and] the Internet is not a physical 'facility[] located in any State.'"[67] Unlike cable companies, ISSPs do not receive their content from signals or broadcasts, or retransmit their content over coaxial cable, wires, or microwave links.[68] For example, Netflix receives its content through licensing deals, and allows customers to access the content on its servers via the Internet.[69] Therefore, Netflix and similar ISSPs are not receiving signals or retransmitting them, but simply allowing access to content via the Internet.

Another reason that ISSPs should not be treated like cable systems is that they fail to meet the physical facility requirement. According to the court in *FIlmOn X*, a cable system must have a physical facility that retransmits the signal.[70] Arguably, in order to have a physical facility, an ISSP would have to have a physical presence. The Court of Appeals of New York held "physical presence is not typically associated with the Internet in that many websites are designed to reach a national or even a global audience from a single server whose location is of minimal import."[71] Hence, because it is Internet-based, an ISSP has neither a physical presence nor a physical facility that retransmits the signal. For the above reasons, an ISSP is not a cable system and should not be classified or taxed as such.

64. *See* Niccolai, James, *Behind the Curtain: How Netflix Streams Movies to Your TV*, TECHHIVE (May 22, 2014) http://www.techhive.com/article/2158040/how-netflix-streams-movies-to-your-tv.html.

65. 17 U.S.C. § 111(f)(3); *see id.*

66. *See* Fox Television Stations, Inc. v. FIlmOn X, LLC., 150 F. Supp. 3d. 1, 20 (D.D.C. 2015).

67. *Id*. at 19.

68. *See, e.g.*, *Netflix's View: Internet TV is replacing linear TV*, *supra* note 58.

69. *See Id.*

70. *See* Fox Television Stations, Inc. v. FIlmOn X, LLC., 150 F. Supp. 3d. at 19.

71. Overstock.com, Inc. v. New York Department of Taxation and Finance, 987 N.E.2d 621, 626 (N.Y. 2013).

2. The Purpose of the Permanent Internet Tax Freedom Act

The taxation of ISSPs by state and local governments runs contrary to the purpose of the Permanent Internet Tax Freedom Act, which is to prevent the taxation of Internet access and promote the growth of the Internet.[72] In determining the purpose of the Permanent Internet Tax Freedom Act, one should look at the plain language of the statute and Congressional intent.[73]

The Permanent Internet Tax Freedom Act explicitly states that Internet access remain tax-free: "It is the sense of Congress that no new Federal taxes similar to [taxes on Internet access and multiple or discriminatory taxes on electronic commerce] should be enacted with respect to the Internet and Internet access…."[74] Therefore, Congress intended Internet access, and thus ISSPs, to remain tax-free from state and local governments.

The purpose of the Permanent Internet Tax Freedom Act can also be determined by reviewing the Congressional intent. The Congressional Record evidences that Congress's purpose in passing the Act was to protect Internet access from taxation and to promote the growth of the Internet. Congressman Robert Goodlatte (R-VA) asserted that the Permanent Internet Tax Freedom Act protects Americans from a substantial tax burden, but also "maintains unfettered access to [the Internet]," and promotes the growth of the Internet by creating a permanent tax ban to enhance predictability for investors.[75] Similarly, Congressman Steven Chabot (R-OH) believed Internet access needed to be protected from taxation because Americans use it every day "to run small businesses, to do research, to apply for jobs, to listen to music, to communicate with friends and family . . . and for so many other things."[76] Therefore, the Congressional Record demonstrates that in passing the Permanent Internet Tax Freedom Act, Congress intended to protect Internet access, including ISSPs, from taxation, as well as to promote the growth of the Internet.

Congress could not have intended that ISSPs be subject to taxation because such a requirement would hinder the statute's purpose.[77] According to opponents of taxing Internet access, "allowing states to impose tax[es] on internet access would hurt the growth of the wireless industry and price out

72. *See* Internet Tax Freedom Act, 47 U.S.C. § 151 Note at Sec. 1101(a); *see also* House Congressional Record, H3952 (June 9, 2015) (stating "Congress has worked assiduously for 16 years to keep Internet access tax-free.").

73. *See* Miller v. French, 530 U.S. 327, 336 (2000) (stating "[w]here Congress has made its intent clear, '[the court] must give effect to that intent.'" (quoting Sinclair Refining Co. v. Atkinson, 370 U.S. 195, 215 (1962)).

74. Internet Tax Freedom Act, 47 U.S.C. § 281 Note at Sec. 1201.

75. *See* House Congressional Record at H3952.

76. *See id.* at H3952 (emphasis added).

77. *See id.* at H3952.

lower-income customers," which would thereby "impose an unnecessary burden on consumers and providers."[78]

Based on the above arguments that the Permanent Internet Tax Freedom Act preempts state and local taxing authority, that ISSPs fall under the statutory definition of Internet access, and the congressional intent in passing the Permanent Internet Tax Freedom Act, is a clear indicator that ISSPs should not be subject to state and local sales and use taxes.

B. The Commerce Clause

The Commerce Clause gives Congress the power to regulate interstate commerce and prohibits state and local governments from enacting regulations that place an unconstitutional burden on interstate commerce.[79] In 1992, the United States Supreme Court addressed the issue of requiring an out-of-state vendor to collect and remit sales and use taxes in *Quill Corp. v. North Dakota*.[80] The Court held that physical presence in the taxing jurisdiction was required for an entity to have a substantial nexus with the taxing jurisdiction as required by the Commerce Clause.[81] Accordingly,, the Court reasoned that a business that "deliver[ed] all of its merchandise to its North Dakota customers by mail or a common carrier from out of state locations" did not meet the required substantial nexus with the taxing state of North Dakota.[82] Therefore, "[u]nless the remote seller has a 'nexus,' that is, some type of contact or connection, with the state in which the customer is located, the seller has no obligation to collect and remit the state's sales or use tax."[83] As a result, the issue of whether a business has the required nexus "has become one of the most contentious issues between states and out-of-state vendors."[84]

---

78. *See* Sarah McGahan, and Troy Young, *Extended Yet Again: The Debate Over State Taxation of Internet Access Will be One for the 114th Congress*, THE TAX ADVISER (Mar. 1, 2015), http://www.thetaxadviser.com/issues/2015/mar/salt-mar2015.html [https://perma.cc/5NKU-PJ4P]; *see also* House Congressional Record at H3952 (Congressman Goodlatte states "[Taxing Internet access] is regressive. Low-income households pay 10 times as much in communication taxes as high-income households as a share of income.").

79. *See* Granholm v. Heald, 544 U.S. 460, 493 (2005) (Stevens, J., dissent) (stating that "a state law may violate the unwritten rules described as the "dormant Commerce Clause" [] by imposing an undue burden on both out-of-state and local producers engaged in interstate activities…"); *see also* U.S. Constitution Art. 1, § 8, cl. 3 (2016).

80. *See generally* Quill v. North Dakota, 504 U.S. 298.

81. *See id.* at 313-14.

82. *See id.* at 302; *see also National Bella Hess v. Department of Revenue*, 386 U.S. 753, 755 (holding that a company, with only a contact through "the United States mail or common carrier" with the state, was not required to "collect and pay…the tax imposed by [the state] upon consumers who purchase the company's goods for use within the State.").

83. *See* Delta and Matsuura, *Law of the Internet: State Taxation of Electronic Commerce*.

84. *Id.*

1. The Taxation of ISSPs by State and Local Governments' Fails to Satisfy the Substantial Nexus Test Required by the Commerce Clause

State and local governments' requirements that ISSPs collect and remit sales and use taxes violate the Commerce Clause because the taxation places an undue burden on interstate commerce. To determine whether a state or local government's imposition of sales and use taxes on ISSPs are an undue burden on interstate commerce, courts should look at the "substantial nexus" requirement.[85] The test to determine "substantial nexus" with the taxing jurisdiction is whether a company has a physical presence in the jurisdiction.[86] Without this connection, the requirement that ISSPs collect and remit sales and use taxes creates an undue burden on interstate commerce.

ISSPs do not satisfy the "substantial nexus" test with the taxing jurisdictions because the content is accessed via the Internet, a common carrier. In *Quill*, the Supreme Court held that an out-of-state vendor whose only connection to customers in the taxing state was through "mail or common carrier as part of a general interstate business" could not be required to collect and remit taxes due to a lack of "substantial nexus" because it would be an undue burden on interstate commerce.[87] ISSPs, as in *Quill*, deliver their merchandise and products through a common carrier, the Internet.[88] Therefore, like in *Quill* and *National Bella Hess, Inc. v. Department of Revenue*, where the company was not subject to collecting and remitting sales and use taxes by the state because its only contact was through a common carrier, ISSPs should not be subject to taxation by governments in which their only connection is Internet access service, a common carriage service.[89]

To note, there is the possibility that the Internet's classification as a common carrier will change.[90] However, the potential reclassification will not change the conclusion that ISSPs do not satisfy the "substantial nexus" requirement established by *Quill*. The Supreme Court's use of the phrase

85. The exceptions being cases where the ISSP has physical offices or headquarters in the jurisdiction.

86. *See* Quill v. North Dakota, 504 U.S. at 298; *see* National Bella Hess, Inc. v. Department of Revenue, 386 U.S. 754, 759-60 (1967).

87. *See* Quill v. North Dakota, 504 U.S. at 302, 307.

88. *See* United States Telecom Association, et al., v. Federal Communications Commission, 825 F.3d 674, 711 (D.C. Cir. 2016) (upholding the FCC's classification of the Internet as a common carrier).

89. This would not be the case for ISSPs headquartered or with physical offices in jurisdictions. In those cases, ISSPs could be taxed by the jurisdiction.

90. *See generally* Restoring Internet Freedom, *Notice of Proposed Rulemaking*, FCC 17-60 (2017), https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1.pdf [https://perma.cc/PXE5-ADE6]; *see generally* Marc S. Martin and Michael A. Sherling, *Net Neutrality and Broadband Privacy Under The New FCC*, LAW 360 (Feb. 13, 2017); *see generally* Jenna Ebersole, *4 Clues From The FCC Chairman On Net Neutrality's Fate*, LAW 360 (March 10, 2017).

"mail or common carrier as part of a general interstate business"[91] suggests that the Court was applying the lay definition of "common carrier" because it used the phrase to include other methods of transportation, in addition to standard mail. It would be a stretch to conclude that the Court used the phrase "common carrier," as defined by the Communications Act of 1934,[92] when it was discussing sending packages via the United States Postal Service.[93] Therefore, the Court was likely using the lay definition of a "common carrier," which is "a business or agency that is available to the public for transportation of persons, goods, or messages."[94] The Internet is an entity "available to the public for the transportation of . . . goods or messages."[95] Therefore, the Internet meets the criteria of a common carrier for the "substantial nexus" test, regardless of its classification for regulatory purposes.

Furthermore, ISSPs do not have the required "substantial nexus" with the taxing jurisdictions because the content is accessed via the Internet, without the ISSP maintaining an actual physical presence in the taxing jurisdiction. ISSPs provide services to customers via the Internet, which, as the District Court for the District of Columbia concluded, is not a physical facility.[96] Therefore, ISSPs do not have a physical presence in the taxing states and localities because the Internet does not count as a physical facility; thus, there is not substantial nexus.

ISSPs also do not have the required substantial nexus with the taxing jurisdiction because "physical presence is not typically associated with the Internet in that many websites are designed to reach a national or even a global audience from a single server whose location is of minimal import."[97] Netflix and other similar ISSPs use content delivery networks, which are comprised of a system of servers.[98] According to the court in *Overstock.com v. New York*, the locations of servers are "of minimal import," and therefore, the mere presence of a server does not satisfy the "substantial nexus" requirement.[99] This argument is further supported by the fact that the State of Washington explicitly excluded the use of servers from the "substantial nexus" requirement for taxation.[100] As a result, the only jurisdictions that should be

91. *See* Quill v. North Dakota, 504 U.S. at 307 (citing to National Bella Hess, Inc., 386 U.S. 758).

92. *See* Communications Act of 1934, 47 U.S.C. § 153(11) (2016) (defining a common carrier as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this Act; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier").

93. *See generally* Quill v. North Dakota, 504 U.S. 298.

94. "Common Carrier." *Merriam-Webster.com*. Merriam-Webster, n.d. Web. 6 Apr. 2017.

95. *Id.*

96. *See* Fox Television Stations v. FilmOn X, 150 F. Supp. 3d. at 19.

97. *See* Overstock.com v. New York, 987 N.E.2d at 626.

98. *See* Niccolai, *Behind the Curtain: How Netflix Streams Movies to Your TV*.

99. *See* Overstock.com v. New York, 987 N.E.2d at 626.

100. *See* Engrossed Substitute House Bill, at § 101(4)(b).

allowed to tax ISSPs are the jurisdictions in which the ISSPs are headquartered or have offices because this would meet the "substantial nexus" requirement. Nevertheless, the majority of state and local governments do not satisfy the "substantial nexus" required to force ISSPs to collect and remit sales and use taxes.

The United States Supreme Court in *Quill* emphasized that the "Commerce Clause and its nexus requirement are informed . . . by structural concerns about the effects of state regulation on the national economy."[101] The Court first laid out these structural concerns in *Bella Hess, Inc.*, holding that if a state or local jurisdiction was allowed to tax out of state businesses without a substantial nexus, then every other jurisdiction throughout the United States with the "power to impose sales and use taxes" would be allowed to tax the business too.[102] This would place an extreme burden on businesses and interstate commerce by subjecting businesses, such as ISSPs, to a multitude of differing tax rates, exemptions, and "record-keeping requirements" imposed by a jurisdiction with "no legitimate claim to impose 'a fair share of the cost of the local government.'"[103] Therefore, the taxation of ISSPs by states, localities, and other political subdivisions is not only impermissible because of the burden it places on interstate commerce; it is also unfair to ISSPs with no substantial nexus to the taxing jurisdiction because these companies should not be expected to share the cost of governments from which they receive no benefits or protections.

One could argue that the pleasure of doing business in the taxing jurisdiction is a benefit that justifies taxation; however, the Supreme Court of Florida has implied otherwise.[104] The Court identified some of these benefits, such as fire and police protection and the jurisdiction's "maintenance of a civilized society."[105] Based on the court's list of "benefits" or "protections," the pleasure of doing business in the taxing jurisdiction does not seem to fall into the "benefits" or "protections" the courts consider in these instances.[106] Proponents may also argue that ISSPs benefit from the provision of the Internet infrastructure provided by state and local governments. However, this is a stretch. The Internet infrastructure that ISSPs rely on is not provided by state and local governments, but instead is installed and maintained by private companies. Therefore, ISSPs do not enjoy the benefits or protections identified by the courts from the majority of taxing jurisdictions and should not be subject to collecting and remitting their sales and use taxes.

---

101. *See* Quill v. North Dakota, 504 U.S. at 312.

102. *See* National Bella Hess v. Department of Revenue, 386 U.S. at 759-60 (stating "the very purpose of the Commerce Clause was to ensure a national economy free from such unjustifiable local entanglements").

103. *Id.*

104. *See generally,* Florida Dep't of Revenue v. American Business USA Corp., 191 So.3d 906 (Fla. S. Ct. 2016)

105. *See id*. at 916 (quoting *Oklahoma Tax Comm'n v. Jefferson Lines, Inc.*, 514 U.S. 175, 200 (1995).

106. *Id.* at 916-17 (quoting *Delta Air Lines, Inc. v. Dep't of Revenue*, 455 So.2d 317, 323 (Fla. 1984)).

Not only do United States Supreme Court decisions discussed above indicate that the taxing of ISSPs by state and local governments places a burden on interstate commerce, the Federal Communications Commission ("FCC") and proponents of taxing ISSPs have also asserted that the imposition of various taxation systems is overly burdensome to ISSPs.[107] In its National Broadband Plan, the FCC stated, "a national framework for digital goods and services taxation would reduce uncertainty and remove one barrier to online entrepreneurship and investment." [108] Furthermore, the Advisory Committee on Electronic Commerce proposed that "[s]tate[] and local governments [ ] work . . . to draft a uniform sales and use tax act that would simplify State and local sales and uses systems…"[109] The Advisory Committee's recommendation to simplify the taxing systems of state and local governments' sales and use tax systems implies that subjecting any company that does interstate business over the Internet to taxation by various state and local governments would be a burden to interstate commerce. In fact, even proponents of taxing ISSPs admit that the subjection of a company to the multitude of state and local sales tax systems would be an undue burden on commerce.[110] Therefore, requiring ISSPs to collect and remit sales and use taxes based on a multitude of differing tax codes is a violation of the Commerce Clause because the regulations "unduly burden interstate commerce."[111]

The taxation of ISSPs by state and local governments violates the Commerce Clause because the requirements would place an undue burden on interstate commerce. The taxation of ISSPs by multiple state and local governments causes an undue burden on interstate commerce because ISSPs do not satisfy the "substantial nexus" requirement established by the Supreme Court in *Quill*.[112] Furthermore, major proponents of taxing ISSPs agree that subjecting ISSPs to the multitude of state and local tax codes would be an

107. FCC, *Connecting America: The National Broadband Plan* 58 (2010); STAFF OF JOINT COMM. ON TAXATION, 107TH CONG., *Overview of Issues Related to the Internet Tax Freedom Act and of Proposals to Extend or Modify the Act Scheduled for a Hearing Before the Senate Committee on Finance on August 1, 2001* 6 (Comm. Print 2001) WL 36044176.

108. See *Connecting America: The National Broadband Plan* at 58.

109. See Overview of Issues Related to the Internet Tax Freedom Act and of Proposals to Extend or Modify the Act Scheduled for a Hearing Before the Senate Committee on Finance on August 1, 2001, JOINT COMMITTEE ON TAXATION (July 30, 2001) 2001 WL 36044176 at *6.

110. *See What is The Marketplace Fairness Act*, MARKETPLACEFAIRNESS.ORG (last visited Mar. 4, 2018) http://marketplacefairness.org/what-is-the-marketplace-fairness-act/ [https://perma.cc/XP8W-5DRV].

111. Quill v. North Dakota, 504 U.S. at 312.

112. *See* Quill Corp. v. North Dakota, 504 U.S. at 298; *see* National Bellas Hess v. Department of Revenue, 386 U.S. at 759-60

undue burden on interstate commerce.[113] Therefore, requiring ISSPs to collect and remit sales and use taxes violates the Commerce Clause.

2. Counter Arguments Raised by Proponents of Taxing ISSPs Violate the Commerce Clause

This section addresses counter arguments that proponents of taxing ISSPs could raise, and how those arguments fail to meet the substantial nexus requirement of the Commerce Clause, thus placing an undue burden on interstate commerce.

Proponents of taxing ISSPs will argue that *Overstock.com, Inc.* should guide the courts, which held that in-state independent contractors satisfied the substantial nexus requirement.[114] The Court of Appeals of New York reasoned that having in-state independent contractors who provide links to an Internet company's website for the purpose of purchasing items qualifies as 'active, in-state solicitation;' and therefore, the company has a physical presence in the state.[115] This, however, was a clear example of judicial activism in which the court came to a conclusion without a rational basis, according to the dissenting opinion of Justice Smith.[116] Smith criticized the majority's opinion, claiming that such logic was "so strained as not to have a reasonable relation to the circumstances of life as we know them."[117]

Furthermore, the majority opinion in *Overstock.com* partly supports the assertion of this Note, that is, ISSPs should not be subject to state and local governments' sales and use taxes. The Court stated the physical presence requirement "need not be substantial," but "must be demonstrably more than a 'slight[] presence.'"[118] Based on the District Court for the District of Columbia's statement that the Internet is not a physical facility, a company that is solely based on the Internet would not have even a slight presence in the taxing jurisdiction.[119] Therefore, an ISSP, which is a company that provides services via the Internet, does not even have a slight presence in the majority of states and municipalities, because the Internet is not a physical facility.[120] As a result, ISSPs should not be subject to state and local governments' sales and use taxes because they do not have even a slight physical presence, and therefore, do not satisfy the "substantial nexus" test.

---

113. *See What is The Marketplace Fairness Act*; *see generally see generally* The Streamlined Sales and Use Tax Agreement, STREAMLINEDSALESTAX.ORG, http://www.streamlinedsalestax.org/uploads/downloads/Archive/SSUTA/SSUTA%20As%20Amended%2012-16-16.pdf [https://perma.cc/RM49-LPM2].

114. *See* Overstock.com v. New York, 987 N.E.2d at 623, 626.

115. *Id.*

116. Overstock.com v. New York, 987 N.E.2d at 629 (Smith, J. dissenting).

117. *Id.*

118. *See* Overstock.com v. New York, 987 N.E.2d at 625 (*quoting, Orvis Co. v. Tax Appeals Tribunal of State of N.Y.*, 86 N.Y.2d 165, 178 (1995)).

119. *See Fox Television Stations v. FIlmOn X*, 150 F. Supp. 3d. at 19

120. *See id.* at 19; Overstock.com v. New York, 987 N.E.2d at 626.

Proponents of requiring ISSPs to collect and remit state and local governments' sales and use taxes also argue that the Marketplace Fairness Act will avoid this undue burden on interstate commerce because it would simplify state and local sales and use tax codes.[121] The Marketplace Fairness Act provides states with two options to simplify their relevant tax codes:

> (1) [adopt the Streamlined Sales and Use Tax Agreement, or (2)] agree to notify retailers in advance of any rate changes within the state; designate a single state organization to handle sales tax registrations, filings, and audits; establish a uniform sales tax base for use throughout the state; use destination sourcing to determine sales tax rates for out-of-state purchases . . . ; [and] provide software and/or services for managing sales tax compliance, and hold retailers harmless for any errors that result from relying on state-provided systems and data.[122]

As of April 2017, twenty-four states have adopted the Streamlined Sales and Use Tax Agreement.[123] Therefore, even though the Marketplace Fairness Act claims to solve the undue burden problem, it fails to do so because it could still subject companies to the burden of complying with twenty-seven different state tax codes, not to mention the multitude of local tax codes.

C. The Due Process Clause

The taxation of ISSPs may violate the Due Process Clause by failing to satisfy its "physical presence" or "purposefully directing" requirements.[124] However, this argument is not likely to be successful. The United States Supreme Court has held that for a jurisdiction to be able to tax a company, the company must be "physically present" in the jurisdiction or "purposefully direct[] its activities" at residents of the jurisdiction, analogizing to personal jurisdiction.[125] The *Quill* Court looked to *International Shoe*, which held that the Due Process Clause requires a defendant to have "certain minimum contacts with [the jurisdiction] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[126] In doing so, the Court concluded a company satisfied this minimum contacts test by "purposefully direct[ing] its activities" at residents of the taxing jurisdiction.[127] Therefore, for a state or local government to require an ISSP to collect and remit sales and use taxes without violating due process, the ISSP

121. *See What is The Marketplace Fairness Act*.
122. *See id.*; *see generally* The Streamlined Sales and Use Tax Agreement.
123. *See What is The Marketplace Fairness Act*.
124. *See* Quill Corp. v. North Dakota, 504 U.S. at 306-08.
125. *See id.*
126. *See* International Shoe Co. v. Washington, 326 U.S. 310, 316 (citing Milliken v. Meyer, 311 U.S. 457, 63 (1940)); *see also* U.S. Constitution Amend. XIV, § 1.
127. *See* Quill v. North Dakota, 504 U.S. at 306-08.

has to be physically present in the state or municipality, or have "purposefully directed its activities" at residents.

However, ISSPs are not physically present in jurisdictions where they do not have a physical facility. As previously discussed, the Internet is not a "physical facility," therefore, unless the ISSP has an actual facility in the taxing jurisdiction, the ISSP is not physically present in the state or municipality.[128] Rather, the real question is what counts as a physical facility.

Proponents of taxing ISSPs could argue that a server counts as a facility; however, judicial precedence implies the contrary. According to *Overstock.com, Inc.*, "physical presence is not typically associated with the Internet in that many websites are designed to reach a national or even a global audience from a single server whose location is of minimal import."[129] Netflix and other ISSPs use content delivery networks, which are comprised of a system of servers.[130] According to the Court of Appeals of New York, the location of the servers is "of minimal import," and therefore, the presence of a server does not count as a facility sufficient to satisfy the physical presence requirement of the Due Process Clause.[131] As a result, state and local governments cannot require ISSPs to collect and remit sales and use taxes relying on the physical presence of a server.

All ISSPs, however, most likely satisfy the "purposefully directing" prong of the test, possibly allowing state and local governments to require them to collect and remit sales and use taxes under the Due Process Clause. According to *Quill*, a company satisfies the minimum contacts requirement by "purposefully direct[ing] its activities" at residents of the jurisdiction.[132] For example, the Supreme Court has held that a state can exercise jurisdiction over a national magazine company because the magazine is bought and distributed on a national scale with a "substantial number of copies [ ] regularly sold and distributed" in the state.[133] ISSPs likely satisfy this test because access to their content is sold and distributed to customers throughout the United States. Therefore, their services are "purposefully directed" at residents of every taxing jurisdiction. As a result, state and local governments do not violate due process by requiring ISSPs to collect and remit sales and use taxes so long as the ISSPs "purposefully directed" their activities at residents of the taxing jurisdiction.

ISSPs could argue that state and local jurisdictions should not be allowed to require them to collect and remit sales and use taxes because the only connection they have with the taxing jurisdiction is the customer. In *Walden v. Fiore*, the Supreme Court held that Nevada could not exercise jurisdiction over a police officer in Georgia for seizing personal property from

---

128. *See* Fox Television Stations, Inc. v. FilmOn X LLC, 150 F. Supp. 3d. 1, 19 (D.D.C. 2015).

129. See Overstock.com v. New York, 987 N.E.2d at 626.

130. *See* Niccolai, *Behind the Curtain: How Netflix Streams Movies to Your TV*.

131. *See* Overstock.com, *supra* note 123, at 626.

132. *See Quill v. North Dakota*, 504 U.S. at 306-08 (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985)).

133. *See* Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 781 (1984).

two people during their layover from San Juan to Las Vegas, finding "the plaintiff cannot be the only link between the defendant and the forum."[134] Yet, the city of Chicago is attempting to force ISSPs to collect and remit an amusement tax from Illinois residents who purchase their streaming services.[135] This would appear to violate the due process principle from *Walden* because the only connection between the taxing state and the ISSP is the customer. Therefore, ISSPs could argue state and local governments violate due process when they require ISSPs to collect and remit sales and use taxes; however, this is not likely to succeed because of the "purposefully directing" test.[136] Therefore, state and local governments most likely do not violate the Due Process Clause by requiring ISSPs to collect and remit sales and use taxes, because ISSPs "purposefully direct [their] activities" at residents of the taxing jurisdiction.[137]

IV. CONCLUSION

With the permanent extension of the Internet Tax Freedom Act by the Permanent Internet Tax Freedom Act of 2016, coupled with the Commerce Clause and the Due Process Clause, ISSPs have a defense against state and local regulations requiring the collection and remittance of sales and use taxes. And when the courts decide whether to uphold such tax schemes, it should draw upon Congress's clear intent that Internet access remain unburdened by state and local taxes and the Commerce Clause prohibiting undue burdens on interstate commerce. Therefore, ISSPs should challenge the legality of these taxes in the courts on the basis of the above reasons, with courts ideally striking down state and local tax regulations that violate any of the above requirement.

134. *See* Walden v. Fiore, 134 S.Ct. 1115, 1122 (2014).

135. *See* Jensen, *US – The Disparate State and Local Tax Treatment of Digital Streaming Services*.

136. *See* Quill v. North Dakota, 504 U.S. at 308.

137. *Id.*