EDITOR'S NOTE

Welcome to the third and final issue of Volume 70 of the *Federal Communications Law Journal* ("*Journal*"), the official journal of the Federal Communications Bar Association ("FCBA"). This summer has been an exciting transition period for the *Journal*, as the Class of 2018 members at The George Washington University Law School graduated, and incoming Volume 71 board and staff members were selected. Both outgoing and incoming members have dedicated their summer months to produce this issue, which provides noteworthy perspectives on topics ranging from drone regulation, zero-rating, to cyber harassment. As this is our Annual Review issue, we are also very proud to present nine case briefs, penned by incoming *Journal* board members, of legal disputes that were in the spotlight in the communications field last year.

This issue features a Guest Comment written by Lisa Li, who is a recent graduate from The George Washington University Law School, and a current Legal & Government Affairs Associate at Pondera International LLC. In her Comment, Ms. Li denotes the problem arising from diverging foci of current cyber-harassment laws; as a result, perpetrators and victims of cyber stalking and harassment in the Washington D.C. metropolitan area may face difficulties in determining their legal rights. Ms. Li highlights the need for new federal laws that directly deals with doxing and swatting issues, to govern actions that result from online harassment.

The first Student Note is written by McKenzie Schnell, who proposes that the most effective means to curb discriminatory zero-rating practices is to make the legal argument that certain zero-rated contracts are harmful to the public interest under the Mobile-Sierra Doctrine. The second Student Note is written by Samantha Dorsey, who points to the lack of regulation on the use of drones in the commercial market; Ms. Dorsey suggests a two-fold regulatory framework that would constrain the means of which data is collected and provide non-participants with opt-out options. Last but not least, the third Student Note is written by Bethany Krystek, who underscores the need for improved risk management in Computer-Assisted Dispatch systems for large cities with high rates of crime, so that chances of violent Post-Traumatic Stress Disorder triggers and use of excessive force are minimized.

Finally, the outgoing *Journal* members would like to thank the FCBA and The George Washington University Law School for the opportunity to serve the *Journal* this year. It was truly an honor. As a team, we worked hard to produce both qualitative and quantitative content for our esteemed colleagues of the FCBA, and we leave both proud and humbled by the experience. As we turn the reigns over to the talented Volume 71 members, we wish the team the best of luck in the new academic year!

We welcome your feedback or questions to fclj@law.gwu.edu and we ask that article submission be sent to fcljarticles@law.gwu.edu. The Annual Review issue and our archive will be available at www.fclj.org.

Jane Lee
Editor-in-Chief

Federal Communications Law Journal

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

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,500 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 3

SEPTEMBER 2018

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLES

NOTES

Zero-rating is an increasingly hot-button issue because of previous ambiguity, on behalf of the Federal Communications Commission (FCC), in how it should be regulated. While many consumers and conglomerate broadband providers are proponents of zero-rating, opponents contend that the practice violates the tenets of net neutrality. Prior to the new Republican administration, zero-rating was regulated on a case-by-case basis but was not banned entirely. However, through a 2016 investigation by the FCC into zero-rating practices, it became apparent that some zero-rating structures were seemingly discriminatory, namely AT&T and Verizon's.

Upon designation as Commissioner of the FCC, Ajit Pai dismissed all investigations into AT&T and Verizon's zero-rating programs and is unlikely to regulate the practice at all. This should be alarming to the public because these discriminatory practices will persist and likely, expand. Thus, the best mechanism for remedying discriminatory zero-rating practices is a lawsuit arguing that, pursuant to the Mobile-Sierra Doctrine, zero-rated contracts like those between AT&T, Verizon, and their affiliated providers are harmful to the public interest.

Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting

Lisa Bei Li *

TABLE OF CONTENTS

* J.D., May 2018, The George Washington University Law School; B.S., Finance and International Business, May 2010, New York University Stern School of Business. Thank you to the staff of the Federal Communications Law Journal (the "FCLJ") for their contribution and assistance with publication.

I. INTRODUCTION

Although online harassment encompasses many activities, including cyberbullying and cyberstalking, ever-increasing "troll storms" lead to two unique phenomena: doxing[1] and swatting.[2] Doxing is when someone's personal information is shared on the Internet without their consent[3] and swatting is when someone makes a fictitious report to the police that leads armed officers to come to an unknowing "victim's" home.[4] In these instances, an online "troll," defined as an inflammatory Internet user[5], calls to action other trolls to cause a "storm" that incites the group to disseminate victims' private information and hail armed forces to victims' homes as acts of terrorization.[6]

Every Internet user is subject to potential doxing. As a form of harassment, perpetrators reveal victims' personal information without permission.[7] The information shared is usually sensitive, like one's social security number, medical records, and personal messages or photos.[8] Even elderly individuals, who take care to lead private lives, are sometimes "doxed."[9]

Victims of online harassment are also subject to swatting. Swatters make fraudulent calls to the police who then send SWAT teams[10] to victims' allegedly dangerous homes to remove them at gunpoint. According to the New York Times, "[t]he FBI has estimated that about 400 cases of swatting occur nationwide every year, but anecdotal reports suggest the numbers are far higher than that . . . ."[11]

---

1. Also commonly spelled "doxxing."

2. *See generally* Andrew Quodling, *Doxxing, Swatting and the New Trends in Online Harassment*, THE CONVERSATION (Apr. 21, 2015), https://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234 [https://perma.cc/QV7F-KFWN].

3. *Id.*

4. *Id.*

5. *See generally* Elise Moreau, *10 Types of Internet Trolls You'll Meet Online*, LIFEWIRE (June 22, 2018), https://www.lifewire.com/types-of-internet-trolls-3485894 [https://perma.cc/YHW8-7WJY].

6. *See id.*

7. *See* Joel Stein, *How Trolls Are Ruining the Internet*, TIME (Aug. 18, 2016), http://time.com/magazine/us/4457098/august-29th-2016-vol-188-no-8-u-s/ [https://perma.cc/48D2-K43G].

8. *See, e.g.*, Jason Fagone, *The Serial Swatter*, N.Y. TIMES (Nov. 24, 2015), https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html [https://perma.cc/5NFU-Q9CN].

9. *See, e.g.*, C.S-W., *The Economist Explains What Doxxing Is, and Why It Matters*, THE ECONOMIST (Mar. 10, 2014), https://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9 [https://perma.cc/3BSV-QHEC].

10. SWAT teams are "Special Weapons And Tactics" units of the police force.

11. Anna North, *When a SWAT Team Comes to Your House*, N.Y. TIMES (July 6, 2017), https://www.nytimes.com/2017/07/06/opinion/swatting-fbi.html [https://perma.cc/7H9J-J7X2].

While online harassment comes in many forms, abuse of the Internet and its resulting harms can be curbed if the government focuses on the aspects of harassment that the law can regulate, particularly with regards to data privacy. This would require targeting the conduct related to and resulting from online harassment, such as doxing and swatting. While speech and expression may not be easily restrained, the manipulative and unauthorized use of others' data and the deception of police forces can be prevented. If these goals of "troll storms" are eliminated, trolls will be less likely to disrupt others both on and off the Internet.

II. BACKGROUND

In 2016, Andrew Anglin, the infamous neo-Nazi host of conservative website *The Daily Stormer*,[12] launched a "troll storm campaign" against Tanya Gersh, a Jewish real estate agent living in Montana.[13] In his campaign, Anglin called for readers to "make [their] opinions known against the Jewish people of Montana.[14] Although he explicitly incited the resulting 700 threatening anti-Semitic phone calls, emails, and text messages sent to Gersh,[15] Anglin also posted that he was not advocating for "violence or threats of violence."[16] Thus, Anglin's campaign, on its face, could be categorized as involving hate speech, but likely not more.[17] As the below Analysis will show, hate speech and other online communication is difficult to regulate, and existing laws do not provide the restraint required to curb harassing activities such as doxing and swatting.

This Comment covers examples of online harassment related to doxing and swatting, the conduct of doxing and swatting separate from hate speech, the difficulty of regulating hate speech and online communications, and the current laws available to restrain doxing and swatting. This Comment further asserts the inadequacy of existing laws covering cyber-harassment activity. Finally, this Comment recommends specific changes to federal laws that could be lobbied for in Congress to regulate doxing and swatting.

---

12. *See* Andrew Anglin, SOUTHERN POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/individual/andrew-anglin [https://perma.cc/6W46-U8SP] (last visited July 25, 2017).

13. *See* Complaint at 2, Gersh v. Anglin, No. 9:17-cv-00050-DLC-JCL (D. Mont. Apr. 18, 2017), ECF No. 1.

14. *See id.* at Complaint at 7.

15. *See id.* at Complaint at 20.

16. *See* Lois Beckett, *Jewish Woman in Montana Sues over 'Troll Storm' of Neo-Nazi Harassment*, THE GUARDIAN (Apr. 18, 2017), https://www.theguardian.com/us-news/2017/apr/18/montana-jewish-woman-sues-troll-storm-neo-nazi-harassment [https://perma.cc/2UCW-RNSU].

17. *See* Suzanne Nossel, *No, Hateful Speech Is Not the Same Thing as Violence*, WASH. POST (June 22, 2017), https://www.washingtonpost.com/outlook/no-hateful-speech-is-not-the-same-thing-as-violence/2017/06/22/63c2c07a-5137-11e7-be25-3a519335381c_story.html?utm_term=.3a3a29086274 [https://perma.cc/9HHR-9GCX].

III. ANALYSIS

A. *Hate Speech is Often Protected by the First Amendment*

As case law has established, hate speech targeting racist and other agendas is, on its own, protected[18] by the First Amendment's guarantee of "freedom of speech."[19] But, the First Amendment does not protect against otherwise illegal conduct that involves speech.[20] For example, once expression incites "imminent lawless action,"[21] "fighting words,"[22] or a "true threat,"[23] then the speech is no longer protected and the speaker may be subject to other criminal or civil laws.[24] Unfortunately, the bar for reaching such levels of speech is quite high.

The First Amendment generally restricts government regulation of content-based and/or viewpoint-based language,[25] even if the language amounts to offensive communication.[26] This applies not only to hate speech, but also to other intimidating and/or threatening conversations initiated online.[27]

In contrast, doxing and swatting are concrete actions associated with online harassment and trolling.[28] Doxing and swatting are conduct, and conduct is generally not protected by the First Amendment.[29] Therefore, given the constitutional challenges of regulating speech and expression, the best way to mitigate online harassment would be to focus on the conduct associated with and caused by harassment, instead of focusing on the harassing communication itself.

---

18. *See* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969); *see also* Dawson v. Delaware, 503 U.S. 159, 167 (1992).

19. *See* U.S. CONST. amend. I.

20. *See G*eorge L. Blum, *Validity, Construction, and Application of State and Municipal Criminal and Civil Cyberbullying Laws*, 26 A.L.R.7th Art. 4 § 4 (2017) ("It has never been deemed an abridgment of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated or carried out by means of language.").

21. *See* Brandenburg, 395 U.S. at 447.

22. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words — those which by their very utterance inflict injury or tend to incite an immediate breach of the peace.").

23. *See* Watts v. United States, 394 U.S. 705, 708 (1969).

24. *See, e.g.*, CAL. PENAL CODE § 415; D.C. ST § 22-1321.

25. Content and viewpoint-based speech regulations must satisfy the court's "strict scrutiny" test whereas content-neutral laws are only subject to "intermediate scrutiny." *See* George L. Blum, *Validity, Construction, and Application of State and Municipal Criminal and Civil Cyberbullying Laws*, 26 A.L.R.7th Art. 4 § 3 (2017).

26. *See* Aimee Fukuchi, *A Balance of Convenience: The Use of Burden-Shifting Devices in Criminal Cyberharassment Law*, 52 B.C. L. REV. 289, 304 (2011).

27. *See id.* at 295.

28. *See supra*, Introduction.

29. *See* United States v. O'Brien, 391 U.S. 376, 377 (1996).

B. Online Harassment Initially Involves Communication, Which is Difficult to Regulate

Almost all online harassment involves communication, whether the medium is through a social media post, on a forum, or in a chatroom.[30] Online communication and its many forms make online harassment an increasingly important issue for lawmakers to address.[31] Unfortunately, current focus on the communication aspect of harassment makes it subject to challenges, both constitutional and practical. Constitutional issues present a roadblock for victims attempting to obtain redress either under statutes or under common law. Applications of existing criminal and civil statutes are often challenged in court by defendants asserting First Amendment defenses.[32] As previously identified, "cyber[-]harassment statutes remain vulnerable to constitutional challenges for substantial over[-]breadth or vagueness due to their potential restrictions on protected speech."[33] Victims bringing suit pursuant to a common law tort offense, such as the Intentional Infliction of Emotional Distress ("IIED"), must also be able to maneuver the procedural hurdles of litigation.[34]

On the other hand, defendants can use the Fourth and Fifth Amendments as affirmative defenses, protecting against search and seizure and against self-incrimination, respectively.[35] Therefore, even if a victim is able to bring the case to court, the alleged harasser has multiple constitutional defenses that he or she could assert, making an already time-consuming and expensive process even harder for the victim pursuing litigation. Due to these difficulties, bringing a case based on threating or harassing speech is a difficult route to take for online harassment victims. Instead, the law is more amenable to regulating harassing conduct, like doxing and swatting, which

---

30. *See generally* U.S. DEP'T OF JUST., CYBER MISBEHAVIOR (May 2016), https://www.justice.gov/usao/file/851856/download [https://perma.cc/P4WM-EPTB]; *cf.* Kate E. Schwartz, *Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Victimization*, 87 WASH. U. L. REV. 407, 421 (2009) (presenting statistics of the number of people affected by cybercrime and internet victimization).

31. *See generally Online Harassment: A Comparative policy Analysis for Hollaback*, DLA PIPER 37 (Nov. 2016), https://www.ihollaback.org/app/uploads/2016/12/Online-Harassment-Comparative-Policy-Analysis-DLA-Piper-for-Hollaback.pdf [https://perma.cc/DY84-Q839].

32. *See* Rathod Mohamedbhali, LLC, *Using the First Amendment as a Defense in a Criminal Case*, RM (Oct. 8, 2013), https://www.rmlawyers.com/using-the-first-amendment-as-a-defense-in-criminal-cases/ [https://perma.cc/VRY5-DP62].

33. *See* Fukuchi, *supra* note 26 at 300.

34. *See* Schwartz, *supra* note 30 at 427 (discussing the timing needs for "fresh" evidence and the separate affirmative defenses available to defendants).

35. *See* David Gray, *Fighting Cybercrime After United States v. Jones*, 103 J. CRIM L. & CRIMINOLOGY 745, 745–46 (2013) (discussing Fourth Amendment search and seizure defenses by defendant who was prosecuted for cybercrime); In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1341 (involving defense presented by defendant asserting that the decryption of computer crime evidence was a violation of his Fifth Amendment right against self-incrimination).

are not subject to the same constitutional challenges. Unfortunately, current laws do not adequately prevent or punish doxing and swatting.

Many harassment cases are currently brought under state statutory or common law.[36] The dearth of federal law addressing situations of online harassment[37] has left it up to states to monitor cyberspace activity.[38] Of course, each state's limited ability to regulate activity in its jurisdiction makes state law an ineffective framework for regulating the Internet.[39] Beyond the states' lack of control over far-reaching online activity, there is no uniformity in how the states treat online harassment.[40] The perpetrators and victims of online harassment cannot easily discern their rights and protections because it is often unclear which state's cyber-harassment laws govern the situation and what, exactly, is the substance of those laws.[41]

Currently, policymakers differ on whether cyber-harassment laws are crafted to be speaker-centric or target-centric.[42] Speaker-centric laws focus on the alleged harasser's intent and activity whereas target-centric laws focus on the alleged victim's harm and reasonable expectation of harm.[43] Balancing the two approaches is possible, but burden-shifting creates additional constitutional due process and procedural problems.[44]

Examples of the differing burdens are shown by comparing state laws within the U.S. Courts of Appeals for the Fourth and D.C. Circuits. North Carolina and Maryland's cyberstalking statutes both require specific intent on the part of the perpetrator.[45] Virginia does not have specific cyberstalking or cyber-harassment laws, but its general stalking statute also requires speaker-centric specific intent.[46] The District of Columbia similarly does not have cyber-harassment laws, but its general stalking statute is implicated by showing either speaker-centric purposeful knowledge or target-centric reasonable fear of stalking.[47]

---

36. *See* Dianne Avery & Catherine Fisk, *Overview of the Law of Workplace Harrassment*, at 1, http://apps.americanbar.org/abastore/products/books/abstracts/5190452%20intro_abs.pdf [https://perma.cc/85JW-WXCS].

37. *See infra* Analysis, Section D.

38. *See generally* Fukuchi, *supra* note 26 (surveying existing state laws governing cyber-harassment); Nancy Leong & Joanne Morando, *Communication in Cyberspace*, 94 N.C. L. REV. 105 (2015) (surveying existing state laws governing cyber communication).

39. *See* Christine LiCalzi, *Computer Crimes*, 54 AM. CRIM. L. REV. 1025, 1067 (2017).

40. *See* Blum, *supra* note 25 (Articles surveying existing state laws governing cyber-harassment).

41. *See, e.g.*, D.C. CODE ANN. § 22-3133 (West 2009); MD. CODE ANN., CRIM. LAW § 3-805 (2016); VA. CODE ANN. § 18.2-60 (West 2016).

42. *See* Nancy Leong & Joanne Morando, *Communication in Cyberspace*, 94 N.C. L. REV. 105, 112–13 (2015) (discussing the "two different approaches to defining 'communication'" as speaker-centric versus target- centric).

43. *See id.*

44. *See* Fukuchi, *supra* note 26 at 310–15 (citing additional tests to determine violation of the Fourteenth Amendment when imposing non-mandatory presumptions in burden shifting).

45. *See* N.C. GEN. STAT. § 14-196.3 (2015); MD. CODE ANN., CRIM. LAW § 3-805 (2016).

46. *See* VA. CODE ANN. § 18.2-60 (West 2016).

47. *See* D.C. CODE ANN. § 22-3133 (West 2009).

As a result of these different laws, perpetrators and victims of cyber stalking and harassment in the Washington D.C. metropolitan area[48] may have a hard time determining their legal rights. One targeted attack of cyber activity is likely to take place in multiple states. This is assuming that state stalking and harassment statutes even govern the specific cyber activity at issue. Unfortunately, these state laws are almost always too broad to be limited to regulation of conduct. Existing state statutes instead often target harassing speech and expression, which are subject to the constitutional challenges and the issues mentioned above.[49]

Given the limitations of state law and the difficulty of regulating online communication, Congress should propose new federal laws to govern actions that perpetuate and result from online harassment — namely, laws dealing with doxing and swatting. These activities are the consequences of continuous online threats that result in concrete and identifiable harms.[50] Concurrently, doxing and swatting fall within the ambit of existing laws; therefore, lobbying for small and discrete changes in those laws is another option for organizations seeking to improve the current online environment.

C. Doxing and Swatting Fall Within the Purview of Existing Federal Laws, But the Federal Government Does Not Specifically Regulate Doxing and Swatting

Doxing is subject to existing federal laws related to data storage, data use, and information privacy.[51] On the other hand, swatting is subject to current federal laws relating to fraud and obstruction of justice.[52] While existing laws may cover doxing and swatting, specific statutory elements must be met in order for these cases to be brought.[53] The specific elements often either create loopholes for the perpetrator or are impossible to meet absent other factors being present in doxing and swatting schemes.[54]

Not only does the Department of Justice (DOJ) fail to actively prosecute doxing and swatting as a result of inadequate laws, law enforcement also suffers from a shortage of resources to deal with these crimes.[55] The police and Federal Bureau of Investigations (FBI) do not typically have the necessary means to identify, arrest, and charge perpetrators of doxing and

48. The area encompassing the District of Columbia, Maryland, and Virginia is also colloquially referred to as "the DMV."

49. *See, e.g.*, VA. CODE ANN. § 18.2-60 (West 2016); D.C. CODE ANN. § 22-3133 (West 2009).

50. *See supra* Introduction.

51. *See, e.g.*, The Communications Decency Act, 47 U.S.C. § 230 (2012); The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); The Stored Communications Act, 18 U.S.C. § 2701 (2012).

52. *See* 18 U.S.C. § 1501 et seq (2012).

53. *See* The Communications Decency Act, 47 U.S.C. § 230 (2012); The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); The Stored Communications Act, 18 U.S.C. § 2701 (2012).

54. *See id*.

55. *See* DLA PIPER, *supra* note 31, at 40-43.

swatting.[56] Therefore, the solution requires a two-fold process to stop the harmful activities that result from online harassment. First, Congress should amend existing laws or create new laws to punish doxing and swatting. Second, Congress needs to provide the necessary resources to implement those laws by increasing law enforcement personnel and their training.

D. Existing Federal Laws are Inadequate and Outdated

There are three existing laws that could potentially address doxing. These laws are: the Communications Decency Act (CDA),[57] the Computer Fraud and Abuse Act (CFAA),[58] and the Stored Communications Act (SCA).[59] The CDA promotes a safe and respectful online environment principally for underage users.[60] The CFAA provides an open Internet primarily for private organizations.[61] Lastly, the SCA outlaws tampering with data stored and controlled by Internet Service Providers (ISPs).[62] Unfortunately, ISPs have little control over user activity beyond what the ISPs themselves do with customer data.[63] Under the Trump Administration, ISPs are able to sell and distribute user data.[64] In the current environment, the SCA does not provide adequate protections for personal information, as the statute has not been significantly amended since its enactment in 1986.[65] Separately, the CFAA allows websites to dictate acceptable use of its sites through web terms of service.[66] Of course, terms of service are governed by private contract law, which does not historically consider public safety issues.[67]

ISPs and private websites owners have little incentive to regulate online safety concerns like doxing because although there are safety concerns with doxing, the issues do not factor much into a for-profit enterprise's cost-benefit analysis. Moreover, the CDA removes liability for ISPs and host websites through Section 230(c), which states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any

56. *See, e.g.*, Fagone, *supra* note 8.
57. *See* 47 U.S.C. § 230 (2017).
58. *See* 18 U.S.C. § 1030 (2017).
59. *See id.* § 2701.
60. *See* 47 U.S.C. § 230 (2017).
61. *See* 18 U.S.C. § 1030 (2017).
62. ISPs are the communication facilities referenced in 18 U.S.C. § 2701 (2017).
63. *Contra* Thomas Fox-Brewster, *Now Those Privacy Rules Are Gone, This Is How ISPs Will Actually Sell Your Personal Data*, FORBES (Mar. 30, 2017), https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc-privacy-rules-how-isps-will-actually-sell-your-data/ [https://perma.cc/4HS7-TU2N].
64. *See* Tom Brant & Angela Moscaritolo, *Trump Officially Hands Control of Your Data to ISPs*, PC MAGAZINE (Apr. 4, 2017), https://www.pcmag.com/news/352595/gop-senators-hand-control-of-your-data-to-isps [https://perma.cc/C62W-SZ2R].
65. *See* 18 U.S.C. § 2701 (2017).
66. *See id.* § 1030.
67. *See* Alison S. Brehm & Cathy D. Lee, *From the Chair: Click Here to Accept the Terms of Service*, https://www.americanbar.org/publications/communications_lawyer/2015/january/click_here.html [https://perma.cc/4DLG-MLZN].

information provided by another information content provider."[68] Therefore, currently, no federal regulation exists to prevent online harassment generally or doxing specifically.

There are even fewer laws that could punish people who engage in swatting.[69] Instead, swatting cases are often brought under allegations of larger conspiracies, with only one of several claims alleging swatting.[70] The federal laws relating to obstruction of justice do not include a component dealing with false police reports,[71] which did not create significant problems for law enforcement until swatting became an issue related to online harassment.[72]

As a result of increased incidences of doxing and swatting,[73] members of Congress have begun to propose laws to address these malicious activities. Representative Katherine Clark (D-Mass.) remains one of the leading proponents of anti-doxing, with her sponsorship of the Interstate Doxxing Prevention Act,[74] which was introduced in December 2016.[75]

Herself a victim of swatting, Representative Clark has made banning cyberstalking one of her legislative priorities.[76] In April 2015, she — along with eleven other sponsors — endorsed the Anti-Swatting Act of 2015.[77] Later that year, Representative Clark introduced the Interstate Swatting Hoax Act, which was co-sponsored by eight other Representatives.[78] Separately, Representative Sean Patrick Maloney (D-NY) introduced the Stop Swatting in Our Schools Act of 2016, which specifically asked Congress to establish a task force within the FBI to deal with swatting.[79] The Senate also introduced its own anti-swatting legislation known as the SWAT Act.[80]

Unfortunately, none of these bills has yet passed into law as of the writing of this Comment. Although one route would be to follow Congress' initiatives to pass new statutes regulating doxing and swatting, another option

68. *See* 47 U.S.C. § 230 (2017).

69. *But cf.* 18 U.S.C. § 1501 et seq (2012).

70. *See, e.g.*, *Man Faces Five Years in Federal Prison in "Swatting" Case*, U.S. DEP'T OF JUST. (July 29, 2014), https://www.justice.gov/usao-ndtx/pr/man-faces-five-years-federal-prison-swatting-case [https://perma.cc/6JX5-5W7E]; James T. Jacks, *Last Defendant Sentenced in Swatting Conspiracy*, U.S. DEP'T OF JUST. (Nov. 16, 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/nalleySent.pdf [https://perma.cc/T4QD-JZFK].

71. *See* 18 U.S.C. § 1501 et seq. (2017).

72. *See supra* Introduction and Background.

73. *See id.*

74. "Doxxing" is also commonly spelled "doxing," as written throughout this Memo.

75. *See* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

76. *See* Joshua Miller, *Police Swarm Katherine Clark's Home After Apparent Hoax*, BOSTON GLOBE (Feb. 1, 2016), https://www.bostonglobe.com/metro/2016/02/01/cops-swarm-rep-katherine-clark-melrose-home-after-apparent-hoax/yqEpcpWmKtN6bOOAj8FZXJ/story.html [https://perma.cc/H9BH-PLNR].

77. *See* H.R. 2031, 114th Cong. (2015).

78. *See* H.R. 4057, 114th Cong. (2015).

79. *See* H.R. 4804, 114th Cong. (2016).

80. *See* S. 1018, 114th Cong. (2015).

would be to amend and improve existing laws that cover Internet activity and police reporting.

IV. RECOMMENDATIONS

While both doxing and swatting fall within the purview of existing laws, neither are actually addressed by those laws. To improve and amend existing laws, doxing could be regulated by specifically proscribing and imposing liability the sharing of personal and sensitive information.[81] Swatting, on the other hand, could be added as an element within the federal obstruction of justice statute, 18 U.S.C. § 1501 et seq. For example, Congress could simply add language prohibiting the use of swatting to effectuate 18 U.S.C. § 1511.[82] Such an amendment would eliminate the requirement of showing conspiracy under the current statute.[83] Of course, Section 1511 could also be expanded to include obstruction of justice for federal law enforcement, such as the FBI, who often ends up dealing with swatting cases due to the Bureau's enhanced capabilities.[84]

Although a number of creative solutions may exist as to how to address doxing, additional suggestions for improving existing data privacy laws are to amend the SCA, CFAA, and/or CDA as follows:

- Define and clarify unlawful "access" under the SCA to explicitly prohibit tampering and/or distribution of user data held by ISPs. While this would allow the government to regulate the malicious manipulation of personal information, the proposed amendment would not push the onus onto ISPs to regulate public safety. This would remain the responsibility of the federal government.[85]

- Require websites under the CFAA to include in their terms of service a provision for users not to engage in unauthorized access or use of data. Currently, the CFAA only prohibits individuals who "knowingly accessed a computer without authorization."[86] In the current cloud computing environment, access to others' data itself

81. This can be done by amending Section 230(c) as discussed *infra*.

82. This statute is titled "Obstruction of State or Local Law Enforcement." The proposed amendment could be phrased to mirror existing laws to prohibit certain "use of electronic mail," generally, or it could proscribe certain "use or handling of data," specifically.

83. *See* 18 U.S.C. § 1511 (2015).

84. *See* Fagone, *supra* note 8.

85. Currently, the statute reads: "(a) Offense. — Except as provided in subsection (c) of this section whoever — (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."

86. *See* 18 U.S.C. § 1030 (2017).

should be regulated, since information is commonly held in the cloud and locally out of the reach of desktops and laptops.[87]

- Amend the CDA's contentious Section 230(c) to allow for potential liability of information services and edge providers.[88] While this is a larger amendment than the above suggestions to revise the SCA and/or the CFAA, eliminating Section 230(c) of the CDA would drastically further the safe and decent use of the Internet. By imposing liability on ISPs, social media websites separate from ISPs such as Facebook would then be pushed to take steps to prevent "obscene … excessively violent, harassing, or otherwise objectionable" material from being published on their sites.[89]

While any or all of the above suggestions could be lobbied for, some alternatives will be easier to implement than others. For example, preventing swatting could simply involve a minor revision to the existing obstruction of justice statute — a revision which would be to the benefit of both swatting victims and law enforcement.[90]

On the other hand, preventing and punishing doxing may involve substantial revisions to existing data privacy laws, but such amendments could update those laws to match modern technology and its use. Not only would the amendments improve privacy on the Internet, but they might also address cybersecurity. Cybersecurity is a budding issue on Capitol Hill, and as such, Congress would likely be amenable to introducing and passing cybersecurity laws that at the same time regulate doxing. The above recommendations would increase protection for doxing and swatting victims without violating perpetrators' constitutional rights.

V. CONCLUSION

Since regulating speech remains subject to constitutional challenges, the solution to preventing online harassment is to target the related, resulting conduct itself, with a focus on data privacy. Stakeholders should lobby Congress to address doxing and by passing new laws and/or to amend existing statutes, as suggested above.

---

87. Cloud computing refers to the "storing and accessing data and programs over the Internet instead of your computer's hard drive." *See* Eric Griffith, *What Is Cloud Computing?*, PC MAGAZINE (May 3, 2016), https://www.pcmag.com/article2/0,2817,2372163,00.asp [https://perma.cc/7UQ4-VTFL].

88. An example of an edge provider is YouTube. An edge provider is defined as "[a]ny individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet." *See* David Post, *Does the FCC Really Not Get It About the Internet?*, THE WASH. POST (Oct. 31, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/31/does-the-fcc-really-not-get-it-about-the-internet/?noredirect=on&utm_term=.fcc1cde725fa [https://perma.cc/82JU-QCWE].

89. Note that under Section 230(c), websites do not fall under the jurisdiction of the CDA. *See* 47 U.S.C. § 230(c)(2)(A) (2017).

90. *See* 18 U.S.C. § 1501 et seq (2012).

Ultimately, the key issue at stake in regulating online harassment and its results may not be the First Amendment right to speech, but rather quite the opposite. Online users might be keen to allow more of their communication and activity to be public, including to government officials, if it were to keep them safe.[91] As described above, it is possible to leverage existing regulatory infrastructure to prevent and punish doxing and swatting in the current technologically advanced environment. The solution, however, would require collaboration between public and private industries. The government and private organizations, working together, can administer terms of service and use restrictions that would curtail incidences of doxing and swatting.

91. This includes the police force, which would be tasked with enforcing any new or amended laws.

The Mobile-Sierra Doctrine: An Unlikely Friend for Opponents of Zero-Rating

McKenzie Schnell *

TABLE OF CONTENTS

* J.D., May 2018, The George Washington University Law School. Articles Editor, *Federal Communications Law Journal*, Vols. 69–70.

I. INTRODUCTION

Like the politics of the presidents who appointed them, the Federal Communications Commission (FCC)'s zero-rating policies under former Chairman Tom Wheeler and current Chairman Ajit Pai are in marked contrast. Under Chairman Wheeler, zero-rating was regulated on a case-by-case basis, but Chairman Pai has yet to regulate the practice at all.[1] Zero-rating is an increasingly common pricing strategy where Internet service providers (ISPs) provide consumers with access to content, applications, and services without that access accruing towards their broadband or mobile data caps.[2] While popular with consumers, zero-rating is controversial because of its potentially discriminatory implications for edge providers and consumers: edge providers that cannot pay for zero-rating are less competitive, making their product less frequently used, which subsequently impedes users' choice.[3] Edge providers are considered to be "[a]ny individual or entity that provides any content, application, or service over the Internet."[4] Edge providers, like Google and Facebook, use the consumer's ISP to deliver content.[5] The FCC has never banned zero-rating outright because not all zero-rating practices are considered discriminatory and some, depending on their structures, can further competition and consumer choice.[6]

In 2016, under the directive of former Chairman Wheeler, the FCC's Wireless Telecommunications Bureau (WTB) issued a report concluding that AT&T's Sponsored Data and Verizon's FreeBee Data 360 zero-rating practices were potentially discriminatory because they appeared to favor downstream affiliates over unaffiliated edge providers.[7] Despite these findings, Commissioner Pai quickly ceased all investigations into AT&T and

1. *See* Sam Gustin, *Trump's New FCC Chief Just Opened the Floodgates for Zero-Rating*, MOTHERBOARD (Feb. 3, 2017), https://motherboard.vice.com/en_us/article/trumps-new-fcc-chief-just-opened-the-floodgates-for-zero-rating [https://perma.cc/WD5L-DSZM].

2. *See, e.g.*, Peter Nowak, *Why 'zero rating' is the new battleground in net neutrality debate*, CBC NEWS (Apr. 7, 2015 5:00 AM), http://www.cbc.ca/news/business/why-zero-rating-is-the-new-battleground-in-net-neutrality-debate-1.3015070 [https://perma.cc/UW7X-BXR6].

3. Barbara van Schewick, *Network Neutrality and Zero-Rating*, THE CTR. FOR INTERNET & SOC'Y 1–2, (Feb. 19, 2015), http://cyberlaw.stanford.edu/files/publication/files/vanSchewick2015NetworkNeutralityandZerorating.pdf [https://perma.cc/36BT-AJHY].

4. 47 C.F.R. § 8.2(b) (2015).

5. *See* Brian Feldman, *'Sorry ISPs Are Trying to Do What?' What to Know About Congress's New Internet-Privacy Rollback*, N.Y. MAG.: SELECT ALL (Mar. 28, 2017, 5:55PM), http://nymag.com/selectall/2017/03/why-congress-is-dismantling-the-fccs-internet-privacy-rules.html [https://perma.cc/Y9AS-DNNJ].

6. *See* WIRELESS TELECOMM. BUREAU, FED. COMM. COMM'N, POLICY REVIEW OF MOBILE BROADBAND OPERATORS' SPONSORED DATA OFFERINGS FOR ZERO-RATED CONTENT AND SERVICES 1 (2016) [hereinafter *Policy Review*].

7. *See id.* at 16–17.

Verizon's zero-rating practices upon taking office.[8] In a statement seemingly justifying his position, Pai stated, "[t]hese free-data plans have proven to be popular among consumers, particularly low-income Americans, and have enhanced competition in the wireless marketplace."[9] The FCC's current position on zero-rating should be troublesome to the American public because as it stands, the discriminatory practices associated with zero-rating will persist and likely expand.[10] This paper argues that a bold, but possible, solution for curtailing zero-rating during this administration is a lawsuit arguing that, pursuant to the *Mobile-Sierra* Doctrine, zero-rated contracts like those between AT&T, Verizon, and their affiliated providers are harmful to the public interest. A lawsuit of this nature will force the FCC to *at least* regulate *discriminatory* zero-rating practices.

This paper examines how to address discriminatory zero-rating practices under the Commission's new Republican leadership in five stages. First, it provides a background framing the topic of zero-rating and contextualizes the zero-rating debate within broader net neutrality discussions. Second, it delineates the actors involved in zero-rating arrangements, the various zero-rating structures, the arguments for and against zero-rating, and the broader politics surrounding the debate. Third, it introduces the 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services associated with former Chairman Wheeler.

Fourth, it introduces and describes the *Mobile-Sierra* Doctrine – a doctrine that arose from two Supreme Court decisions and stands for the proposition that bilateral contract rates cannot be unilaterally changed.[11] Under the *Mobile-Sierra* Doctrine, courts, in extraordinary circumstances or when such rates are contrary to the public interest, can order the requisite commission to change rates that they find are not "just and reasonable."[12]

Lastly, it analyzes the current zero-rating landscape and concludes by proposing that a lawsuit applying the *Mobile-Sierra* Doctrine is the best mechanism for curbing discriminatory zero-rating practices during Chairman Pai's tenure.

---

8. *See* Jessica Melugin, *FCC Chairman Pai Ends Obama-era Investigations of 'Zero-rating' Data Plan*, CEI, (Feb. 7, 2017), https://cei.org/blog/fcc-chairman-pai-ends-obama-era-investigation-zero-rating-data-plans [https://perma.cc/Y8ZD-HAZJ].

9. Richard Lawler, *The FCC Stops Investigating Carrier's 'Zero-Rating' Plans*, ENGADGET (Feb. 3, 2017), https://www.engadget.com/2017/02/03/the-fcc-stops-investigating-carriers-zero-rating-plans/ [https://perma.cc/E9VW-MB8M].

10. *See* Melissa Repko, *Trump's FCC Drops Investigation Into Zero-Rating*, DALLAS NEWS (Feb. 3, 2017), http://www.dallasnews.com/business/technology/2017/02/03/trumps-fcc-drops-investigation-zero-rating-saying-denying-americans-free-data [https://perma.cc/6H2Q-Y7G2].

11. Michael A. Rosenhouse, Annotation, *Construction and Application of the Mobile-Sierra Doctrine, Under Which Federal Energy Regulatory Commission Must Presume Gas or Electricity Rate Set in Freely Negotiated Wholesale Contract Meets Statutory "Just and Reasonable" Standard*, 62 A.L.R. Fed. 2d 427, *2 (2012).

12. *Id.*

II. BACKGROUND ON NET NEUTRALITY AND ZERO-RATING

A. FCC Regulatory Powers as It Pertains to Zero-Rating

The Communications Act of 1934 created the FCC and authorized it to regulate wire and radio communications, both interstate and foreign.[13] The Communications Act of 1934 was amended by the 1996 Telecommunications Act which Congress intended to spur competition within the telecommunications market by removing unnecessary barriers to entry.[14] The most notable change, for the purpose of this paper, in the 1996 Act was the reclassification of broadband cable services, otherwise known as ISPs, from a telecommunication service to an information service.[15] These two classifications are distinguishable in that telecommunication services offer "telecommunications for a fee directly to the public … regardless of the facilities used"[16] while information services provide "a capability for [processing]… information via telecommunications."[17] This change is significant because telecommunications services are subject to stricter regulatory controls pursuant to Title II of the 1934 Communications Act compared to information services under Title I of the 1934 Act.[18]

In the early 2000s, the FCC's decision to regulate ISPs as information services began to take center-stage starting with *National Cable and Telecommunications Ass'n v. Brand X Internet Services*.[19] Brand X argued that regulating ISPs under Title I would lead to a slippery slope where any communications provider could circumvent common carrier regulations by bundling information services with telecommunications.[20] Ultimately, the Supreme Court ruled against Brand X, using *Chevron* deference,[21] with the majority finding that the statutory definitions between the two classifications were ambiguous and therefore, the FCC's statutory construction was reasonable and permissible.[22]

---

13. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified in scattered sections of 47 U.S.C.).

14. Telecommunications Act § 101, 47 U.S.C. §§ 251-261 (2012).

15. *See* Sara Kamal, *If It Isn't Broken, You're Not Looking Hard Enough: Net Neutrality and Its Impact on Minority Communities*, 68 FED. COMM. L.J. 329, 332 (2016).

16. Nat'l Cable & Telecommunications Ass'n v. Brand X Internet Servs., 545 U.S. 967, 977 (2005).

17. *Id.* at 987.

18. *See* Kamal, *supra* note 23 at 332.

19. *See* Brand X Internet Servs., 545 U.S. at 967.

20. *See id.* at 997.

21. *Chevron* deference "requires a federal court to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is the best statutory interpretation." *Id.* at 980.

22. JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE, 196 (2007).

B. *Net Neutrality: An Internet Structure That Treats All Information Equally*

The subject of net neutrality is the crux of the zero-rating controversy because the rules that govern net neutrality will subsequently impact the regulation of zero-rating.[23] Net neutrality is

> An Internet structure that does not favor one application over another… whereby each node connected to the Internet passes data bound for some other destination on a 'first-come, first-served' basis, without prioritizing, degrading, or blocking a transmission based on the kind of information contained . . . .[24]

In other words, under net neutrality, all information transferred over the Internet should be equally prioritized and accessible to consumers. This information structure was in place when the Internet came into existence.[25] As the Internet began to expand, the companies providing Internet services began to consolidate and realize their power to prioritize and degrade certain content.[26] Following the Brand X decision in 2005, diverging political opinions began to further emerge about this traffic-management system that has been in place since the Internet's conception.[27]

Proponents of net neutrality contend that without this Internet safeguard, ISPs will act as gatekeepers and favor the transmission of certain content at the expense of other content.[28] For example, because Comcast and NBC are affiliated, Comcast would be incentivized to promote NBC's content over ABC's to its customers, which would lead to a slower load time for ABC.[29] Conversely, opponents assert that the principles of the free-market are capable of neutralizing discriminatory implications arising from an Internet structure without net neutrality.[30] Opponents also contend that FCC regulation only hinders innovation as well as business opportunities for content providers.[31]

The FCC's position on net-neutrality was illustrated by a 2005 policy statement adopting four principles ensuring that "broadband networks are

---

23. *See id.* at 350.
24. JONATHAN M. EISENBERG ET AL., CAL. ANTI. & UNFAIR COMP. L. § 10.13 (2016).
25. *See id.*
26. *See id.*
27. NUECHTERLEIN & WEISER, *supra* note 30 at 196.
28. *See* EISENBERG, *supra* note 37.
29. Alyson Shontell, *EXPLAINED: 'Net Neutrality' For Dummies, How It Affects You, And Why It Might Cost You More*, BUS. INSIDER (Jan. 15, 2014, 4:29 PM), http://www.businessinsider.com/net-neutralityfor-dummies-and-how-it-effects-you-2014-1 [https://perma.cc/M8X8-NM3X].
30. *See* Nisha Ragha, *The Fall of Net Neutrality: The End of an Era and A Call for Reform*, 13 CARDOZO PUB. L. POL'Y & ETHICS J. 559, 566 (2015).
31. *See* EISENBERG, *supra* note 37.

widely deployed, open, affordable, and accessible to all consumers."[32] Despite this policy statement, the FCC did not adopt any formal rules regarding net neutrality.[33] However, when evidence from 2007 showed that Comcast was interfering with its customers' peer-to-peer file sharing traffic, the FCC issued an order in 2008 which deemed Comcast's behavior, and the like, unlawful unless "it further[s] a critically important interest and [is] narrowly or carefully tailored to serve that interest."[34] In 2010, the D.C. Circuit vacated the 2008 order finding that Title I did not contain the authority to proscribe the conditions set forth upon Comcast.[35]

The FCC responded with the first Open Internet Order which set forth transparency, anti-blocking, and anti-discrimination requirements for broadband providers.[36] Under the 2010 Order, "transparency" required broadband providers to disclose things like their network management practices, performance characteristics, and terms and conditions of their broadband services.[37] And "anti-blocking" regulations ensured that providers would not obstruct lawful content, applications or services that compete with their services.[38] Moreover, "anti-discrimination" regulations under the 2010 Order provided that broadband providers would not preference some network traffic at the expense of others.[39]

In response to "[e]merging Internet trends since 2010" which gave the FCC "more, not less, cause for concern about [net neutrality threats]," the Commission adopted the 2015 Open Internet Order to "[ground their] open Internet rules in multiple source of legal authority." In 2015, the FCC adopted a new Open Internet Order, which delineated bright-line rules for regulating threats to the open Internet.[40] The order explicitly bans blocking, throttling, and paid prioritization –the three primary practices the FCC identified as jeopardizing an open Internet.[41] The 2015 Order was also significant in its decision to reclassify broadband service as a telecommunications service and subject broadband providers to certain common carrier regulations under Title II of the Communications Act.[42] Moreover, the Order provided that service

32. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Policy Statement, FCC 05-151, para. 4 (2005), https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf [hereinafter 2005 Policy Statement].

33. NUECHTERLEIN & WEISER, *supra* note 30 at 199.

34. *Id.* at 199.

35. *Id.* at 200.

36. *Id.*

37. FCC, Report and Order on Preserving the Open Internet (Dec. 23, 2010), https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.

38. *Id.*

39. *Id.*

40. 2015 Open Internet Order, 30 FCC Rcd. at 60 (Mar. 12, 2015) https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

41. *Id.*

42. *Id.*

providers cannot unreasonably interfere with consumers' ability to access the Internet or with edge providers' ability to provide services to consumers.[43]

C. Zero-Rating: A Catch-22 for Consumers

It was only a matter of time before zero-rating took center stage in the net neutrality debate, because while the FCC had prohibited fixed ISPs from charging application providers for zero-rating, it did not articulate how it specifically planned to regulate zero-rating.[44] To reiterate, zero-rating is a pricing strategy where ISPs provide consumers with access to content, applications, and services without that access accruing towards their broadband or mobile data caps.[45] To understand zero-rating and the nuances that accompany it, this section will proceed by looking at its actors, the primary site-selection models and sponsorship models.

1. Zero-Rating Actors

The main actors in the zero-rating debate are ISPs and edge providers.[46] As their name suggests, ISPs provide companies and individuals with access to the Internet.[47] Some well-known ISPs are AT&T, WorldNet, and IBM Global Network.[48] There are effectively two types of ISPs under the 2010 Order: fixed-line providers and mobile providers.[49] A fixed-line provider is a "broadband Internet access service that serves end user primarily at fixed endpoints using stationary equipment, such as the modem that connects an end user's home router, computer, or other Internet access device to the network."[50] mobile provider is "a broadband Internet access service that serves end users primarily using mobile stations."[51] Alternatively, an edge provider is any entity that provides access to Internet content, applications, or services.[52] AT&T's Sponsored Data and Verizon's FreeBee Data 360 are examples of powerful edge providers that will be elaborated upon later.[53] Interestingly, "individuals who generate and share content such as personal blogs or Facebook pages are both end users and edge providers, and a single

43. *See* Kelley Drye, *A First Look at the FCC'S Open Internet Order*, KELLEY DRYE CLIENT ADVISORY (Mar. 26, 2015), http://www.kelleydrye.com/publications/client_advisories/0965 [https://perma.cc/JP3T-VRP7].

44. *See* van Schewick, *supra* note 5.

45. *See* Nowak, *supra* note 2.

46. *See, e.g.*, van Schewick, *supra* note 5 at 3-4.

47. *See* Margaret Rouse, *ISP (Internet Service Provider)*, TECHTARGET (last updated Feb. 2006), http://searchwindevelopment.techtarget.com/definition/ISP [https://perma.cc/LH5A-S8HH].

48. *Id.*

49. 2010 Open Internet Order, *supra* note 51.

50. *See id.* at § 8.11(b).

51. *See id.* at § 8.11(c).

52. *See* Rouse, *supra* note 70.

53. *See* Giuseppe Macri, *Internet, Edge Providers Unite Against FCC Privacy Regulation* (Feb. 12, 2016), http://www.insidesources.com/fcc-internet-privacy-rules-face-opposition/ [https://perma.cc/5MLD-S5K8].

firm could both provide broadband Internet access service and be an edge provider, as with a broadband provider that offers online video content."[54]

2. Zero-Rating Site-Selection Models

Zero-rating exists in basically three models:[55] single-website plans, website bundles, and sponsored data as seen in Figure 1.[56] Single-website plans provide consumers with unlimited access to one website with no impact on their data.[57] The websites are often hand picked according to a provider's own agenda.[58] The second model, website bundles, provides consumers with access to multiple preselected websites[59] for any content provider who is willing to pay.[60] Alternatively, sponsored data plans allow content providers to provide their services to consumers via zero-rating by "sponsoring" the data consumers use so that there is no effect on data usage.[61]

Figure 1: Site-Selections Models in order of increasing user choice.[62]

3. Zero-Rating Sponsorship Models

The sponsorship models and subsequent costs of zero-rating exist in three states, as seen below in Figure 2. Under the self-sponsorship model, edge providers can contract to take on data costs[63] and subsequently, users can only visit the sponsored site(s).[64] WhatsApp, a popular messaging app, uses this model.[65] Under the hybrid-sponsorship model, edge providers pay for their own data while simultaneously subsidizing data that consumers can use towards additional websites of their own choosing.[66] The most altruistic model of the three is the general sponsorship model, where a "benefactor pays for Internet use without promoting its own services."[67]

---

54. 2010 Open Internet Order, *supra* note 51 at ¶ 20.
55. *See* van Schewick, *supra* note 5.
56. *See* BJ Ard, *Beyond Neutrality: How Zero Rating Can (Sometimes) Advance User Choice, Innovation, and Democratic Participation,* 75 MD. L. REV. 985, 990-96 (2016).
57. *See id.* at 990.
58. *Id.*
59. *See id.* at 993.
60. *See id.* at 990.
61. *Policy Review*, *supra* note 8.
62. Ard, *supra* note 79 at 993.
63. *See* Rebecca Curwin, *Unlimited Data, but a Limited Net: How Zero-Rated Partnerships Between Mobile Service Providers and Music Streaming Apps Violate Net Neutrality*, 17 COLUM. SCI. & TECH. L. REV. 204, 221 (2015).
64. *See* Ard, *supra* note 79 at 998.
65. *See* Aturo J. Carillo, *Having Your Cake and Eating It Too? Zero-Rating, Net Neutrality, and International Law*, 19 STAN. TECH. L. REV. 364, 373 (2016).
66. *See* Ard, *supra* note 79 at 998.
67. *Id.*

Figure 2: Sponsorship Models in order of increasing user choice.[68]

4. Arguments Surrounding the Zero-Rating Debate

Opponents of zero-rating advocate that it is discriminatory to start-up innovation, free speech, and consumers and undermines the spirit of the Internet. Exchanging fees for zero-rating is harmful to start-ups and small businesses because, unlike established companies, they do not have the extra capital to pay the fees to participate in the zero-rating service.[69] These smaller companies are disproportionally affected by zero-rating plans because larger companies will be able to pay for faster loading speeds or to avoid their content being calculated against users' bandwidth caps which will make them more appealing to consumers.[70] Start-up services will be less competitive and less likely to be used, which infringes upon their ability to exercise their right to free speech.[71] While there is little to no data about how users adjust their behavior in response to mobile data pricing practices, one South African study found that when Twitter was zero-rated, the average user went from exchanging 10 MB to 40 MB per day.[72] Furthermore, opponents contend that despite proponents' arguments that zero-rating lowers the costs for mobile Internet services, there is no evidence or guarantee of this.[73] In reality, "[a]pplication providers will have to recoup the costs of zero-rating somehow – e.g., through higher prices or more advertising on the site. Thus, users will [likely] pay the price."[74] For example, a study found that consumers in Europe were experiencing negative ramifications from ISPs that zero-rated their own applications in the form of increased prices and slower loading speeds.[75]

Underlying these practical implications is the theoretical argument that zero-rating disrupts the fundamental freedom that the Internet was built upon.[76] The Internet has been viewed as an environment where anyone can participate, but without net neutrality, it will be regulated by gatekeepers of sorts.[77] Opponents contend that these gatekeepers will favor ISPs with whom they have contracts or who have the largest audiences,[78] thus negating the spirit of the wide-open web that services like Facebook or Twitter were able to capitalize upon.

---

68. *Id.*
69. *See* van Schewick, *supra* note 5.
70. *Id.*
71. *Id.*
72. *See* Nick Feamster, *How Does Zero-Rating Affect Mobile Data Usage*?, FREEDOM TO TINKER (Feb. 10, 2016), https://freedom-to-tinker.com/2016/02/10/how-does-zero-rating-affect-mobile-data-usage/ [https://perma.cc/5EH4-GUV7].
73. *See* van Schewick, *supra* note 5.
74. *Id.*
75. *See id.*
76. *See* Jeremy Malcom et al., *Zero Rating: What It Is and Why You Should Care*, EFF (Feb. 18, 2016), https://www.eff.org/deeplinks/2016/02/zero-rating-what-it-is-why-you-should-care [https://perma.cc/5J5P-K9GA].
77. *See id.*
78. *See id.*

Proponents of zero-rating in developing markets counter that the practice expands the number of people who would otherwise be unable to access the Internet, while simultaneously decreasing costs and increasing consumer choice.[79] By providing differentiated Internet services and varying degrees of access, Internet Service Providers can decrease prices, which increases the number of customers who can afford the service.[80] Because the costs of mobile data services are higher than some people's per capita incomes, many people go without Internet access.[81] However, mobile Internet providers in developing countries have started to offer services like Facebook or local job-search websites as a non-profit public interest service, which means that consumers are no longer faced with preclusive data charges.[82] While proponents concede that these non-profit public Internet services provide limited Internet access, they assert that, "limited access is better than no access because it allows people to communicate and improve their lives using tools that would otherwise remain out of reach."[83] Consequently, the tug of war between zero-rating and net neutrality has been framed as a human rights issue.[84] Proponents for zero-rating contend that disenfranchised people have a right to improve their socio-economic position by accessing the Internet and expressing their fundamental human rights, even if it comes at the expense of curtailing access to the open Internet.[85]

In the U.S., the argument for zero-rating is not centered on its human rights merits but rather on how it advances free market principles.[86] Proponents contend that zero-rating encourages competition because it is a mechanism for smaller service providers to differentiate themselves.[87] By providing customized content, like Sprint with FuboTv, smaller providers are able to attract customers who would otherwise go to larger competitors.[88] Furthermore, proponents advocate that concerns about zero-rating promoting anti-competitive practices are overstated.[89] Many zero-rated programs are "carrier initiated and do not involve payments to carriers by the providers of zero-rated content," which means that start-ups or small businesses will not be that greatly disadvantaged.[90] Moreover, proponents contend that there is

79. FCC, Notice of Proposed Rule to Protect and Promote the Open Internet, (May 15, 2014), https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1_Rcd.pdf.

80. *See* Ellen P. Goodman, *Zero-Rating Broadband Data: Equality and Free Speech at the Network's Other Edge*, 15 COLO. TECH. L.J. 63, 80 (2016).

81. *See* Jeffrey A. Eisenach, *The Economics of Zero Rating*, NERA (Mar. 2015), http://www.nera.com/content/dam/nera/publications/2015/EconomicsofZeroRating.pdf [https://perma.cc/JDK5-9XGF].

82. *See* Ard, *supra* note 79 at 993.

83. *Id.* at 986.

84. *See* Carillo, *supra* note 88 at 417.

85. *See id.* at 419.

86. *See* Eisenach, *supra* note 104.

87. *See id.*

88. *See id.*

89. *See id.*

90. *Id.*

no evidence that zero-rated programs lead to discrimination and subsequent exclusivity.[91]

D. Comparing Zero-Rating Under Republican and Democratic Leadership

1. Obama Administration: Pro Regulation and Anti Discriminatory Practices

Under the Obama Administration, the FCC approached zero-rating on a case-by-case basis via the General Conduct Rule.[92] The FCC's 2015 Open Internet Order said that it would not ban zero-rating outright, because zero-rated plans can sometimes be advantageous to consumers.[93] The General Conduct Rule prohibits broadband providers from participating in conduct that:

> Unreasonably interfere[s] with or unreasonably disadvantages[s] (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users.[94]

a. 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services

The Wireless Telecommunications Bureau (WTB) conducted the 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services for the FCC.[95] This report was careful to explain that the WTB did not take issue with zero-rating as a general practice *per se*.[96] The report chose to focus on four zero-rating programs that illustrate the repeated issues that arise from zero-rating; these programs were T-Mobile Binge On, AT&T Data Perks, AT&T Sponsored Data, and Verizon FreeBee Data 360.[97] The WTB analyzed these four plans using the General Conduct Rule.[98]

---

91. *See id.*
92. *See* Notice of Proposed Rule to Protect and Promote the Open Internet, FCC Rcd. at 10 (Mar. 12, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1_Rcd.pdf.
93. *See id.* at 66.
94. 2015 Open Internet Order*, supra* note 59.
95. *See Policy Review*, *supra* note 8 at 1.
96. *See id.*
97. *See id.* at 8–9.
98. *See id.* at 3.

b. (a) T-Mobile Binge On

T-Mobile's Binge On is a zero-rated service that streams video services that meet certain technical standards.[99] Essentially, content providers can provide T-Mobile customers with video programming that is comparable to standard definition television, as opposed to high definition.[100] The WTB report found that T-Mobile's Binge On was not discriminatory towards edge providers and customers.[101] Central to this finding was the fact that T-Mobile did not force edge providers or customers to participate in Binge On.[102] T-Mobile does have technical requirements for edge providers that want to stream data but many edge providers have been able to meet these stipulations.[103] Moreover, T-Mobile does not stream its own video programming and is therefore not incentivized to favor its own "downstream" affiliates over unaffiliated edge providers.[104] Also, T-Mobile charges all content providers an identical price.[105]

c. AT&T Data Perks

AT&T Data Perks provides customers with extra data for participating in various activities like watching advertisements, buying products, using promotional games or apps, and completing surveys.[106] Advertisers who want customers to view and interact with their products mostly utilize AT&T Data Perks.[107] The report found that Data Perks does not violate the General Conduct Rule.[108] Once consumers watched a video or downloaded an application, they had relative freedom to use the additional data however they wished.[109] Like T-Mobile's Binge On, AT&T does not have downstream affiliates who use the Data Perks app, which means that unaffiliated providers are not discriminated against in favor of affiliated providers.[110] Furthermore, Data Perks only zero-rates small amounts of data.[111]

d. AT&T Sponsored Data

AT&T Sponsored Data allows third-party edge providers to supply streamed video programming to customers without them having to use their monthly data allotment.[112] The report voiced serious concerns that AT&T

99. *See id.* at 11.
100. *See id.*
101. *See id.*
102. *See id.*
103. *See id.*
104. *Id.*
105. *See id.*
106. *See id.* at 12.
107. *See id.*
108. *See id.*
109. *See id.*
110. *See id.*
111. *See id.*
112. *See id.* at 12.

Sponsored Data induces anti-competitive effects and stated that some of AT&T's practices may violate the General Conduct Rule.[113] Specifically, the report noted that AT&T has not provided evidence to counter the presumption that it may be providing Sponsored Data to unaffiliated third parties on less favorable terms than its downstream affiliate, DIRECTV.[114] Such a practice would violate the General Conduct Rule because "such arrangements likely obstruct competition for video programming services delivered over mobile Internet platforms and harm consumers by inhibiting unaffiliated edge providers' ability to provide such service to AT&T's wireless subscribers."[115]

e. Verizon FreeBee Data 360

Verizon FreeBee Data 360 allows content providers to pay on a per-gigabyte-used basis for sponsored data to supply Verizon customers with zero-rated content.[116] The WTB found that similar to AT&T Sponsored Data, Verizon's FreeBee Data 360 might also violate the General Conduct Rule by favoring downstream affiliates.[117] The report stated that it was not aware of any safeguard that would prevent Verizon from offering different terms to both affiliated and unaffiliated edge providers.[118]

2. Trump Administration: Seemingly Anti Regulation of Zero-Rating

The election of President Trump in 2017 spurred the reversal of several pro-consumer initiatives like the investigations into AT&T's and Verizon's discriminatory zero-rating practices[119] that were championed by former Chairman Wheeler.[120] President Trump designated Ajit Pai as the new Chairman of the FCC and Chairman Pai's stance on zero-rating is in marked contrast to the Obama Administration's as evidenced by his recent statement: "the Federal Communications Commission will not focus on denying Americans free data. Instead, we will concentrate on expanding broadband deployment and encouraging innovate service offerings."[121] While the FCC has yet to issue a formal policy regarding zero-rating, Chairman Pai's statement in conjunction with the Trump Administration's appointment of Jeffrey Eisenach – an economist in favor of deregulation and zero-rating

113. *See id.*
114. *See id.* at 13.
115. *Id.*
116. *Id.* at 9.
117. *See id.* at 16.
118. *See id.*
119. *See* Gustin, *supra* note 1.
120. *See* Repko, *supra* note 17.
121. *Id.*

practices – to advise on telecom issues makes it likely that zero-rating will not be banned but rather encouraged.[122]

III. THE *MOBILE-SIERRA* DOCTRINE

The rather obscure *Mobile-Sierra* Doctrine authorizes regulatory commissions to adjust private contract rates so that they are "just and reasonable."[123] Under the Doctrine, there is an initial presumption that a rate set in a freely negotiated contract passes the statutory "just and reasonable" standard.[124] However, this presumption is overcome by purchasers or sellers showing extraordinary circumstances or public interest necessity.[125]

A. Background on the Mobile-Sierra Doctrine

The *Mobile-Sierra* Doctrine arises from two Supreme Court cases, *United Gas Pipe Line Co. v. Mobile Gas Service Corp*. and *Federal Power Commission v. Sierra Pacific Power* that addressed whether the Federal Energy Regulatory Commission could modify bilateral contract rates.[126] Under both the Natural Gas Act and Federal Power Act, rates have to be filed with the Commission and any changes to those rates have to go through the Commission: the same bureaucratic process holds true for bilateral contracts.[127] Under both acts, the rates of the utilities need to be "just and reasonable" – what is "just and reasonable" is under the discretion of the Commission.[128]

While the Supreme Court decided both *Mobile* and *Sierra* on the same day, the analytical framework from *Mobile* was used to guide the decision for *Sierra*.[129] In *Mobile*, United Gas Pipe Line Company (United) sought to change the agreed upon rate specified in a long-term contract by filing a new schedule with the Federal Power Commission without the consent of Mobile Gas Service Corporation (Mobile), with whom it had contracted.[130] Mobile contended that United could not unilaterally change a contract rate.[131] The Court held that parties could not unilaterally change contract rates by filing new tariffs because the filing requirement articulated in the Natural Gas Act was a precondition to changing a rate, not an authorization to change rates.[132] The Court applied that rationale to *Sierra* and proceeded to delineate how the

122. *See* Jeff Dunn, It looks like we're going to have a less open internet under Donald Trump, BUS. INSIDER (Nov. 11, 2016), http://www.businessinsider.com/donald-trump-fcc-net-neutrality-zero-rating-policy-future-2016-11 [https://perma.cc/4LY4-CXMF].

123. 62 A.L.R. Fed. 2d 427 (2012).

124. *Id.*

125. *See id.*

126. *See id.*

127. *See id.*

128. *Id.*

129. *See* 62 A.L.R. Fed. 2d at 427.

130. *See* United Gas Pipe Line Co., v. Mobile Gas Serv. Corp., 350 U.S. 332, 336 (1956).

131. *See id.*

132. *Id.* at 332.

Commission could determine whether a contract rate was "just and reasonable" and therefore lawful:

> The sole concern of the Commission would seem to be whether the rate is so low as to adversely affect the public interest – as where it might impair the financial ability of the public to continue its service, cast upon other consumers an excessive burden, or be unduly discriminatory.[133]

Since the *Mobile-Sierra* decisions, courts have further delineated the scope and applicability of the Doctrine. In *In re Permian Basin Area Rate Cases*, the Court stated that agreements should only be changed in circumstances of unequivocal public necessity.[134] Moreover, in *Morgan Stanley Capital Group Inc. v. Public Utility District Number 1*, the Court stated that commissions must presume a rate set in a freely negotiated contract is "just and reasonable," and that presumption is only overcome if the commission finds that the contract is seriously harmful to the public interest or in extraordinary circumstances.[135] When analyzing whether a contract was harmful to the public interest, the Supreme Court clarified that one should not look at whether the public was immediately harmed by the contract, but instead at whether the contract would pose an excessive burden on consumers "down the line."[136] For example: "the disparity between the contract rate and the rates consumers would have paid (but for the contracts) further down the line, when the open market was no longer dysfunctional . . . could amount to an 'excessive burden.'"[137]

Lower courts have disagreed as to whether this heightened standard can be overcome.[138] For example, some courts have held allegations of price discrimination resulting from a contract as insufficient to overcome the "just and reasonable" test, but "at least one court has found the anticompetitive effect of a contract price sufficient to rebut the *Mobile-Sierra* presumption."[139]

In *Texaco Inc. and Texaco Gas Marketing Inc. v. Federal Energy Regulatory Commission*, the FERC exercised its authority and changed a contract rate between a pipeline and a shipper to accommodate the public interest requirement of the *Mobile-Sierra* Doctrine.[140] The FERC looked "down the line" and determined that the contractual pricing mechanism used in the first contract would distort gas marketing pricing and would prove anti-competitive to the company's main competitor.[141] The court ultimately

133. Fed. Power Comm'n v. Sierra Pac. Power Co., 350 U.S. 348, 355 (1956).

134. *See* In re Permian Basin Area Rate Cases, 390 U.S. 747, 822 (1968).

135. *See* Morgan Stanley Capital Group Inc. v. Public Utility Dist. No. 1, 554 U.S. 527, 545–46, 550 (2008).

136. *See id.* at 552.

137. *See id.* at 553.

138. *See* 62 A.L.R. Fed. 2d at 427.

139. *Id.*

140. *See* Texaco Inc. and Texaco Gas Marketing Inc. v. Federal Energy Regulatory Com'n, 148 F.3d 1091 (D.C. Cir. 1998).

141. *See id.*

deferred to the Commission's decision, finding that it satisfied its burden of articulating a supportable and reasonable explanation of how the public interest required a modification of a private contract rate.[142] Furthermore, although the court found that the *Mobile-Sierra* Doctrine was not overcome by an amendment of a telecommunications interconnection agreement, the Doctrine has been considered in contracts pertaining to telecommunications, as seen in *Quick Communications, Inc. v. Michigan Bell Telephone Company*.[143]

B. Parties That Have Standing Under the Mobile-Sierra Doctrine

Although courts and interested parties originally assumed that only sellers could challenge rates using the *Mobile-Sierra* Doctrine, the Supreme Court has gone on to clarify that sellers, purchasers, and even non-contracting parties can challenge rates.[144] *In Morgan Stanley Capital Group Inc. v. Public Utility District Number 1*, the Court noted that even though it was sellers in *Mobile* and *Sierra* that challenged the contract rates, purchasers can also challenge contracts.[145] The Court went on to clarify that purchasers have the same burden as sellers in overcoming the presumption that a contract rate is "just and reasonable."[146] The Court cited *Potomac Electric Power Co. v. F.E.R.C.* and *Boston Edison Co. v. F.E.R.C.* in its decision.[147]

1. Standing for Purchasers under the *Mobile-Sierra* Doctrine

In the former case, Potomac Electric Power Co. (PEPCO) requested under the Federal Power Act (FPA) to unilaterally modify its contract rate with Allegheny Power System (APS).[148] PEPCO and FPA entered an agreement stipulating that "PEPCO would purchase contract entitlements to a share of the Ohio Edison System's installed generating capacity and associated energy" and then "APS would purchase from the Ohio Edison System the power intended for PEPCO."[149] APS would then "resell the power purchased from the Ohio Edison System to PEPCO."[150] PEPCO filed a complaint against APS to FERC requesting that FERC order APS to reduce its rate because it was arbitrarily higher than APS' rates for comparable

142. *See id.* at 1097.
143. *See* Quick Communications, Inc. v. Michigan Bell Telephone Co., 515 F.3d 581 (6th Cir. 2008).
144. 62 A.L.R. Fed. 2d at 427.
145. *See* 554 U.S. 527, 534 (2008).
146. *Id.* at 534-35
147. 62 A.L.R. Fed. 2d at 427.
148. *See* Potomac Elec. Power Co. v. F.E.R.C., 210 F.3d 403, 404 (D.C. Cir. 2000).
149. *Id.* at 404.
150. *Id.*

services.[151] PEPCO argued that "the public interest was adversely affected by the contractual rate" because the excessive rates were set entirely by APS and accordingly, PEPCO had little bargaining power at the time because of APS' market power.[152] Ultimately, the court did not question the purchaser's standing but found against PEPCO because it did not produce evidence supporting its claims that the rates were unduly discriminatory or excessively burdensome.[153]

In *Boston Edison Co. v. F.E.R.C.*, municipal customers challenged the rate formula of electricity supply contracts.[154] Boston Edison Co. (BECO) had entered into an energy contract with municipal agencies for the sale of electricity produced at a nuclear power plant in Massachusetts.[155] Customers contended that BECO's inclusion of nuclear plant addition interest in its rate formula subjected them to impermissibly high charges.[156] Unlike in PEPCO, the court found for the purchasers but held that the Commission could not order BECO to refund the overcharges because of the relevant statute of limitations.[157]

2. Standing for Non-Contracting Parties under the *Mobile-Sierra* Doctrine

The Supreme Court states in *NRG Power Marketing, L.L.C. v. Maine Public Utilities Commission* that non-contracting parties can also challenge contract rates under the *Mobile-Sierra* Doctrine because such claims are not dependent on the identity of the complainants who seek them, as seen above.[158] This case involved concerned parties who opposed a comprehensive settlement agreement that involved New England's energy grid.[159] There were issues with the reliability of the grid, so the FERC approved an agreement that established a rate-setting mechanism for energy sales and stated that the *Mobile-Sierra* public interest standard would govern rate challenges.[160] Proponents of the settlement contended that the opponents did not have standing under the *Mobile-Sierra* Doctrine because they were a non-contracting party.[161] The Court of Appeals also found this argument compelling.[162] But, the Supreme Court found differently and reasoned that if commissions must presume that contract rates are "just and reasonable" without being a party to the contract, then it would be counterintuitive for

151. *See id.* at 405.
152. *Id.* at 406.
153. *See id. at 409.*
154. *See* Boston Edison Co. v. F.E.R.C, 856 F.2d 361, 361 (1st Cir. 1988).
155. *See id.* at 362.
156. *See id.* at 363.
157. *See id.* at 374.
158. *See* NRG Power Marketing, LLC v. Maine Public Utilities Com'n., 558 U.S. 165, 176 (2010).
159. *See id.* at 167-68.
160. *See id.* at 168.
161. *See id.*
162. *See id.*

non-contracting parties to not be afforded the same presumption.[163] The Court went on to state that "the *Mobile-Sierra* Doctrine does not overlook third-party interests; it is framed with a view to their protection."[164]

IV. A LAWSUIT IS THE BEST MECHANISM FOR CURBING DISCRIMINATORY ZERO-RATING PRACTICES IN THE CURRENT POLITICAL LANDSCAPE

The FCC's recent dismissal of the WTB's Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services and broader changes in zero-rating regulations demonstrate that any regulation of discriminatory practices will likely not be done on the Commission's own accord. This means that the discriminatory practices alluded to in the 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services will persist and likely expand.[165] Therefore, the best mechanism for regulating discriminatory zero-rating practices and preserving net neutrality under the new Republican leadership is a lawsuit brought by customers, edge providers or non-contracting third parties against AT&T and Verizon via the *Mobile-Sierra* Doctrine. In all of these lawsuits, the challenges would need to overcome the presumption that the contract is "just and reasonable" and prove that the contract is seriously harmful to the public interest or show extraordinary circumstances.[166] Specifically, these potential plaintiffs would need to prove that their respective contracts "impair the financial ability of the public utility to continue its service, cast upon other consumers an excessive burden, or be unduly discriminatory."[167] This argument need not be supported by immediate evidence because the Court has stated that courts should not look at whether the public was immediately harmed by the contract, but instead at whether the contract would pose an excessive burden on consumers "down the line."[168]

A. Lawsuit Brought by Customers Under the Mobile-Sierra Doctrine

Customers of AT&T and Verizon could bring a lawsuit like the customers of electricity in *Boston Edison Co. v. F.E.R.C.*[169] Except in this scenario, customers would not be challenging the formula used to determine their rates[170] but rather the rates themselves. Because AT&T and Verizon are likely favoring their downstream affiliates, DIRECTV and go90 by providing

163. *See id. at 174-75.*
164. *See id.* at 175.
165. *See* Repko, *supra* note 17.
166. *See Morgan Stanley Capital Group Inc.*, 554 U.S. at 550.
167. *Fed. Power Comm'n*, 350 U.S. at 355.
168. *Morgan Stanley Capital Group Inc.*, 554 U.S. at 552-53.
169. *See Boston Edison Co.*, 856 F.2d at 362.
170. *See id.*

them with better terms and conditions compared with unaffiliated content providers,[171] they are subsequently disrupting competition in the market, which impacts the prices offered to consumers. The customers in *BECO* argued similarly that BECO's inclusion of nuclear plant addition interest in its rate forum subjected them to impermissibly high charges, and the court found in the customers' favor.[172] Moreover, unlike the customers in BECO, the customers affected here might even be able to receive refunds for the overcharges, providing that they bring the suit within the statute of limitations.[173]

B. Lawsuit Bought by Unaffiliated Edge Providers Under the Mobile-Sierra Doctrine

Unaffiliated edge providers who are discriminated against should bring a lawsuit against AT&T and Verizon like the purchasers in *Potomac Electric Power Co. v. F.E.R.C*. In *PEPCO*, PEPCO filed a complaint against APS to FERC requesting that FERC order APS to reduce its rate because it was arbitrarily higher than APS' rates for comparable services, which was unduly discriminatory.[174] PEPCO argued that the public interest was adversely affected by the contractual rate because the excessive rates were set entirely by APS and accordingly, PEPCO had little bargaining power at the time because of APS' market power.[175] Here, unaffiliated edge providers should make the same claim if they can show that affiliated providers are getting a better deal. However, in *PEPCO*, the court found in favor of FERC because PEPCO did not produce evidence supporting its claims that the rates were unduly discriminatory or excessively burdensome.[176] Here, unaffiliated edge providers *do* have some evidence that these rates are ultimately unduly discriminatory and burdensome. Digital Fuel Monitor extensively researched the impact of zero-rating in markets outside the United States and found that ISPs were able to raise prices after zero-rating had allowed them to monopolize the market.[177] Conversely, in the Netherlands, where zero-rating was banned, one ISP has already doubled its Internet volume caps.[178] These arguments would likely have merit as the Court explicitly stated that discriminatory effects do not have to be immediate under the *Mobile-Sierra* Doctrine but rather we can look down the line at whether the contract would pose an excessive burden on consumers.[179]

---

171. *Policy Review*, *supra* note 8.
172. *See Boston Edison Co.*, 856 F.2d at 363.
173. *See id.* at 372.
174. *See Potomac Elec. Power Co.*, 210 F.3d at 406.
175. *Id.* at 409.
176. *See id*.
177. *See* Antonios Drossos, *The real threat to the open Internet is zero-rated content*, DIGITAL FUEL MONITOR (last visited Apr. 9, 2017), http://dfmonitor.eu/downloads/Webfoundation_guestblog_The_real_threat_open_internet_zerorating.pdf. [https://perma.cc/J324-HKEF].
178. *Id.*
179. *See Morgan Stanley Capital Group Inc.*, 554 U.S. at 527.

C. Lawsuit Brought by Non-Contracting Parties Under the Mobile-Sierra Doctrine

Another solution is for a non-contracting party like Public Knowledge or the ACLU to bring a lawsuit under the *Mobile-Sierra* Doctrine. Again, in *NRG Power Marketing, L.L.C. v. Maine Public Utilities Commission*, the Court held that non-contracting parties can also challenge contract rates under the *Mobile-Sierra* Doctrine because such claims are not dependent on the identity of the complainants who seek them.[180] Here, Public Knowledge would be an ideal party because they are a non-profit organization that advocates for an open Internet.[181] Moreover, the ACLU could be a possible party because they stand for the principle that net neutrality is the only way to preserve the open Internet.[182]

V. CONCLUSION: THE *MOBILE-SIERRA* DOCTRINE: AN UNLIKELY FRIEND FOR OPPONENTS OF ZERO-RATING

Under the FCC's new Republican leadership, the best solution for curbing discriminatory zero-rating practices is a lawsuit arguing that, pursuant to the *Mobile-Sierra* Doctrine, zero-rated contracts like those between AT&T, Verizon and their affiliated providers are harmful to the public interest. Zero-rating has become increasingly debated and controversial since the 2015 Open Internet Order.[183] Opponents contend that it violates the principles of net neutrality and is ultimately harmful to customers.[184] Proponents counter saying zero-rating promotes innovation and is a manifestation of free market principles.[185] Since the 2015 Order, the only formal recognition of the zero-rating conundrum by the FCC was the 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services by the WTB.[186] Unsurprisingly, the 2016 Policy Review found that some zero-rating models are probably unduly discriminatory.[187] However, Commissioner Ajit Pai has stated that he will not be regulating zero-rating, and his dismissal of the WTB's 2016 Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services reflects that sentiment.[188] While certainly an unlikely friend to proponents of zero-rating, the *Sierra-Mobile* Doctrine could serve as a mechanism for a lawsuit that would force the FCC to regulate discriminatory zero-rating practices. Not all zero-rating structures are discriminatory, but some

180. *See NRG Power Mktg., LLC*, 558 U.S. at 176.

181. *See About Us*, PUB. KNOWLEDGE, https://www.publicknowledge.org/about-us/ (last visited Apr. 11, 2017) [https://perma.cc/ZR4X-67Z5]

182. *See Net Neutrality*, ACLU, https://www.aclu.org/issues/free-speech/internet-speech/net-neutrality (last visited April 10, 2017) [https://perma.cc/ESZ2-QZWE].

183. *See* van Schewick, *supra* note 5.

184. *See* Carillo, *supra* note 88 at 377.

185. *See* Ard, *supra* note 79 at 988.

186. *See Policy Review*, *supra* note 8.

187. *See id.*

188. *See* Repko, *supra* note 17.

structures are.[189] Therefore, in order to protect a free and open Internet and the customers who use it, a lawsuit via the *Sierra-M*obile Doctrine is our only hope.

189. *Policy Review*, *supra* note 8.

They Are Watching You: Drones, Data & the Unregulated Commercial Market

Samantha Dorsey *

TABLE OF CONTENTS

* J.D., May 2018, The George Washington University Law School. Member, *Federal Communications Law Journal*, Vols. 69–70.

I. INTRODUCTION

It is a sunny July afternoon and you are laying outside on your pool raft in your fenced-in backyard. You take off your sunglasses to take in the cloudless blue sky—but to your surprise, a small unmanned aircraft system (hereinafter "UAS"), commonly referred to as a drone, is hovering over your backyard. Try yelling at it, try telling the UAS to get off of your property and to stop recording you—see what happens. *Nothing*. The drone is unarmed and is most likely not breaking any law by hovering over your private residence and using its savvy surveillance and data collecting functions.

What information and data were just collected, how much was collected and who collected it? What will happen to the data just collected; will you ever be notified of its use? These are the issues that have arisen in recent years, as the commercial and personal use of UASs have increased, without associated privacy guidelines maintaining the same growth. There is presently no hard-and-fast regulation or law requiring consent before collecting data via UASs, nor any requirement for a UAS operator to notify individuals of their identity or that they will be surveilling their private residences. Thus, a regulatory solution must be implemented to create general guidelines and enforce best practices to limit overreaching UAS data collection.

The present privacy protection framework surrounding the emerging commercial drone market fails to both hold commercial drone operators accountable for data collection and provide individuals with the ability to know what type of information is being collected and by whom. While the expectations of one's privacy has changed a great deal as technology continues to grow, this Note will discuss the necessity of a nationally unified regulatory framework that will designate and place restrictions upon data collection, explain how that data may be used, and establish an accountability log that will provide individuals with the opportunity to access their data that is being collected by a commercial UAS entity. To implement this regulatory framework, Congress will need to pass legislation that addresses all data collection privacy concerns and also grants agencies like the Federal Trade Commission ("FTC") the authority to interpret and establish their specific rules.

Before delving into the major issues and lack of regulations regarding UASs in the commercial market, this Note will provide detailed background information on UASs, basic privacy theories, and the privacy risks that may be implicated by UAS use. The following sections will provide comprehensive insight on the present uses and capabilities of UASs, including privacy issues and attempts to solve such concerns. After addressing the threats UASs pose, a regulatory solution will be proposed.

II. FROM THEN UNTIL NOW: A LOOK AT DRONES

A. What is a UAS and What Are Its Capabilities?

An unmanned aircraft system ("UAS"), commonly referred to as a drone, "is an aircraft without a human pilot onboard."[1] Rather, "the UAS is controlled from an operator on the ground."[2] "Small" UASs will be the primary focus of this Note, unless otherwise specified. Under Federal Aviation Administration ("FAA") regulations, a small UAS is an aircraft weighing less than 55 pounds.[3]

There are many intended uses of UASs, resulting from the varying interests of UAS operators and UAS customers. The primary use for many UAS operators is to collect imaging for real estate endeavors, various inspections, agriculture and filmmaking.[4] Additionally, both nationally and internationally, there has been an increase in utilizing UASs for delivery services from both the operator and customer standpoint.[5]

In an attempt to keep up with demands for faster and more efficient delivery services, many individuals and companies view drone delivery as the next best thing. For example, Amazon, one of the largest delivery services in the United States, currently has a trial-run-stage drone delivery service which it claims will be capable of delivering packages to customers in thirty minutes or less.[6] While Amazon plans on launching its drone delivery service in the United States in the near future, it has already tested this service in the United Kingdom.[7] Amazon's drone delivery trial run in the United Kingdom first delivered an Amazon Fire TV and a bag of popcorn to an Amazon subscriber in December 2016. The entire delivery took a total of thirteen minutes from the customer clicking "order" to the items appearing at the customer's doorstep.[8]

While Amazon may be striving to meet its customers' demands for the fastest delivery possible, there are other motives for drone delivery services.

---

1. Unmanned Aircraft Systems, FAA, www.faa.gov/uas/ [https://perma.cc/47XT-9B9E] (last modified Mar. 21, 2017).
2. *Id.*
3. *See id.*
4. *See* Commercial UAS Exemptions By the Numbers, AUVISI, http://www.auvsi.org/advocacy/exemptions70 [https://perma.cc/L2A9-CC7R] (last visited Apr. 11, 2017).
5. *See* Farhad Manjoo, Think Amazon's Drone Delivery Idea is a Gimmick? Think Again, N.Y. TIMES (Aug. 10, 2016), http://www.nytimes.com/2016/08/11/technology/think-amazons-drone-delivery-idea-is-a-gimmick-think-again.html?_r=0 [https://perma.cc/DSB6-YRCG].
6. Matt McFarland, Amazon Makes its First Drone Delivery in the U.K., CNN (Dec. 14, 2016), http://money.cnn.com/2016/12/14/technology/amazon-drone-delivery/ [https://perma.cc/3Z7N-R9JC]. While the trial run delivery was successful in the United Kingdom, the drone's delivery route flies outside a human's line of sight, which is not yet legal in the United States.
7. *See id.*
8. *Id.*

Internationally, Harvard graduate Keller Rinaudo, has launched *Zipline*, a time-sensitive medical delivery service.[9] *Zipline* drone delivery is more than delivering a television to an impatient customer, it is a new medical advancement that may be used to save lives.

1. Who Can Operate a UAS?

Who is the operator on the ground? As per Part 107 of the FAA's Small Unmanned Aircraft Rule ("Part 107") the operator of a small UAS must be (1) at least 16 years old, (2) have a remote pilot certificate with a small UAS rating, or (3) be directly supervised by someone with such a certificate.[10] In order to qualify for a remote pilot certificate, an individual must either pass an initial aeronautical knowledge test at an FAA-approved knowledge testing center or have an existing non-student Part 61 pilot certificate.[11]

The operators of UASs are required to follow the FAA's newly enacted August 2016, Part 107 Rule, which set forth the new pilot certification and training rules, as well as safety rules including time, height, and speed restrictions for small UASs.[12] These safety regulations may be waived if the FAA authorizes a Section 333 exemption. This is where the problem of data collection begins.[13]

Under the Section 333 exemption, the seemingly most important flying restrictions dictated by Part 107 that provided some privacy protection against nonconsensual data collection (e.g. prohibitions against flying beyond line of sight, over people, at night, and above 400 feet in the air) are not enforced.[14] If a pilot's Section 333 waiver is granted, s/he may operate at night, beyond line of sight, above 400 feet, as well as in other specific types of operation.[15] The exemption is granted when the activity proposed requires such an exemption, like surveying a residential area.[16] This waiver opens up the door to the hypothetical scenario presented in the introduction—the UAS pilot is now authorized to fly or hover above your property, even if you are not a part of the UAS operation.[17] The FAA has set forth very specific safety rules and restrictions to prevent physical collisions or potential security threats (it is

9. *See* April Glaser, Zipline's Keller Rinaudo Explains Why Drone Delivery Took Flight in Rwanda Before the U.S., RECODE (Nov. 11, 2016), http://www.recode.net/2016/11/11/13598806/founder-zipline-drone-delivery-flight-rwanda-blood-keller-rinaudo [https://perma.cc/P5M3-WENU].
10. *See* Unmanned Aircraft Systems, *supra* note 1.
11. *See id.*
12. *See id.*
13. *See id.*
14. *See id.*
15. *See id.*
16. *See id.*
17. *See id.*

illegal to fly, for instance, in Washington D.C. or near airports) but has failed to consider or adopt privacy regulations in its new Part 107 regulation.[18]

2. UAS Surveillance Capabilities

While all UASs have varying levels of surveillance capabilities, many of them are highly advanced. This section will illustrate the level of technology that some UASs possess and how other companies have used similar technology for other means of surveillance and data collection that have led to similar privacy issues.

Many UASs are technologically capable of data collection, and some to a much higher degree than others. Most UASs are "equipped with sophisticated imaging technology that provides the ability to obtain detailed photographs of terrain, people, homes, and even small objects."[19] The giga-pixel cameras used to outfit UASs can "provide real-time video streams at a rate of 10 frames a second" and "track up to 65 different targets across a distance of 65 square miles." They "may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers."[20] The technologies utilized by UASs are growing rapidly, and soon may even include facial recognition.[21] The use and emergence of these technologies will only continue to provide UAS operators with greater tools and capabilities in collecting data.

Similar sensors and surveillance tools used in UASs have already been employed by the likes of Google in its *Google Street View* mapping project, which takes 360 degree views of streets all over the world by way of highly equipped vehicles.[22] Google has since faced privacy-based complaints, as people are concerned with their faces not being properly blurred when the street shots are available on Google's mapping site.[23] However, Google has technically not violated any privacy laws in the United States because under current tort "invasion of privacy" laws, there is no expectation of privacy when a person is in a public space and in fact, the risk of surveillance is assumed.[24]

---

18. *See* Naomi Lachance, D.C.'s No-Drone Zone Gets Help From Superman And E.T., NPR (Mar. 28, 2016), http://www.npr.org/sections/alltechconsidered/2016/03/28/472138137/d-c-s-no-drone-zone-gets-help-from-superman-and-e-t) [https://perma.cc/GZ4Q-AWJL].

19. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, EPIC, https://epic.org/privacy/drones/ [https://perma.cc/SG5S-S2RZ] (last visited Feb. 23, 2018).

20. *Id.*

21. *Id.*

22. Lindsey A. Strachan, Re-Mapping Privacy Law: How the Google Maps Scandal Requires Tort Law Reform, 17 RICH. J.L. & TECH. 1, 1 (2011).

23. *See id.* at 4.

24. *See id.* at 17.

3. Ways in Which UAS Surveillance Data Has Raised Privacy Concerns

You were wearing a yellow shirt and blue jeans outside of the Walmart in your town *someday* since the *Google Street View* initiative took off. Want to know how the world knows that? It is on the Internet. While this simple tidbit of information may not immediately scream "privacy threat!" it certainly may in other circumstances.

Google has maintained that its *Street View* technology is no more revealing than what is already public—and only takes pictures of things so highly public that there is no privacy right to begin with.[25] For example, if someone was photographed by *Street View* technology walking into a pornographic video store, this would not be an invasion of privacy—even though it would likely cause great embarrassment if posted on the Internet for anyone to access.[26] However, Google did begin to blur all faces of individuals captured in street views since mid-2008 after many of these types of concerns and complaints were raised.[27]

When discussing privacy law, it is important to distinguish between public space privacy expectations and private space privacy expectations. While Google may be permitted to take and post public street views, it may face issues when dealing with privately-owned streets. For example, cities like North Oaks, Minnesota requested to have their privately-owned streets' "street views" taken down.[28] These requests were honored by Google because unlike the majority of *Street View* photos of streets and homes, these North Oaks pictures were not initially taken on a publicly owned sidewalk or other publicly-owned parcel of property.[29]

In addition to private property privacy concerns, Google's *Street View* project has had some national security implications. In 2008, *Google Street View* was delayed in the Baltimore and Washington, D.C. area because the Department of Homeland Security was concerned that some of the images may have been taken in security-sensitive locations.[30] Additionally, in that same year, the Department of Defense requested Google not publish *Street View* content of U.S. military bases and remove all existing content of bases.[31] Google complied.[32]

As discussed in this Note's introduction section, on the surface, UASs' initiatives may seem to be free of any menace, but there are still underlying privacy concerns.[33] First, while the primary intention of UAS pilots and/or the companies they represent may be in furtherance of the aforementioned

25. *See id.*
26. *See id.*
27. *See id.* at 7-8.
28. *See id.*
29. *See id.* at 12.
30. *See id.*
31. *See id.*
32. *See id.*
33. Unmanned Aircraft Systems, *supra* note 1 at 2, Sec 1.

uses, the aircraft is still actively surveying the land beneath it and collecting data. Second, the primary intention of the UAS pilot may *only* be to collect data.

B. Privacy and Data Collection

Claims of invasion of privacy often turn on whether the purported victim actually had a reasonable expectation of privacy under the circumstances.[34] This reasonable expectation of privacy has changed as technology has emerged over the past few decades. Surveillance may also be evaluated differently if it occurs in a fleeting instance rather than over a sustained period of time and if there is an understanding of what may become of the collected information.

Privacy and property rights in the modern age are ever-evolving with technological advances and constant data collection. The most pertinent privacy interest implicated by the use of UASs is the "collection of information about people," called "surveillance."[35] "Surveillance takes place in nearly all [UAS] flights, as one of their major purposes is to collect information."[36] Such surveillance may entail a "broad and indiscriminate recording of people on the ground using a camera sensor on the aircraft."[37] It is pertinent to discuss and evaluate all aspects of privacy law and theory to have a strong foundation when approaching the privacy implications of UASs.

1. Reasonable Expectation of Privacy

What is the standard for determining what should be deemed private? Should a homeowner's backyard and home be viewed as private? Since the holding in *United States v. Causby*, the Supreme Court has long held that, "if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere."[38] While the Court in *Causby* was focused on trespass and takings issues, the same rationale may be applied in terms of UAS surveillance over one's land.[39] Moreover, since *Causby*, the Supreme Court has also held that the test for privacy should be based upon what a reasonable person would expect to be private.[40] Should the hypothetical sunbathing landowner expect to have full enjoyment and privacy over his land? The answer to that question is based on what a reasonable person would expect to be private when taking into account both the *Causby* and *Katz* holdings.

---

34. Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

35. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43965, DOMESTIC DRONES AND PRIVACY: A PRIMER 6 (2015), https://fas.org/sgp/crs/misc/R43965.pdf [https://perma.cc/AK9B-VP7T].

36. *See id.*

37. *See id.*

38. *See* United States v. Causby, 328 U.S. 256, 264 (1946).

39. *See id.* at 267.

40. *See* Katz, 389 U.S. at 347.

While it may be true that an individual going outside in public view would expect to be visible from an aerial aircraft, that is not to say that an individual expects to be recorded or surveyed, especially while on one's own land. While the Fourth Amendment is applicable only to government action, the privacy protection and intrusion standard established in *Katz v. United* States—requiring a person to exhibit an actual expectation of privacy and, that the expectation was reasonable—may reasonably presume that unsolicited surveillance and data collection of an individual on his personal property may constitute an unreasonable intrusion of privacy.[41]

2. Different Types of Surveillance: Pattern of Life

Society's expectations of privacy still exist even with the emergence of technology and data collection. There are two major classifications of surveillance that are helpful to keep in mind when trying to adapt a UAS and its surveillance tactics to that of traditional surveillance. Assuming *arguendo* that a UAS was only surveying over one's land for a fleeting moment, would this reasonably pass the "privacy intrusion" standard? On its face, the answer may appear to be yes, but in reality it likely would not. This question leads us to distinguish between two types of video surveillance and monitoring, "episodic surveillance" and "persistent surveillance," which ultimately yield the same results and may be either intentional or unintentional data collection.[42]

Episodic surveillance is comparable to a snapshot—a UAS flying over one's land and taking, for instance, one short video or picture of the land and then exiting the air space above the property.[43] Alternatively, while persistent surveillance varies in quantitative measures of time and amount of collection, it may be defined as a continuous hovering over an area for a given amount of time as a means of data collection.[44] The issue here is that there is no bright line between episodic and persistent surveillance.

Episodic surveillance, or "incremental observations" may not be seen individually as intrusions of privacy, but when viewed as a whole, the sum total of such data collection may very well be seen as a reasonable violation of privacy.[45] The sum total of the data collection is referred to as a "pattern of life," so while any single still-frame of either of the aforementioned types of surveillance may be in itself a defensible incursion on privacy, the whole video is something more than the sum of its parts.[46]

Although it is not the primary goal of UAS flight, passive data collection occurs through cell phone or computer history tracking in an

41. *See id.*
42. K.K, A Looming Threat, THE ECONOMIST (Mar. 19, 2015), https://www.economist.com/democracy-in-america/2015/03/19/a-looming-threat [https://perma.cc/Q4YS-ZJ6V].
43. *See id.*
44. *See id.*
45. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).
46. *See id.*

episodic and persistent nature.[47] This type of collection persists by way of continuous UAS sensors.[48] Even if the collection is unintentional, it produces a mass of data—without a meaningful opportunity for consent by the individual being surveyed.[49] The difference between passive data collection on a cell phone and on a UAS is that the cell phone user is generally aware that his or her data is being collected and has elected to continue using the cell phone regardless of that invasion.

Therefore, the result of pattern of life data collection, either by passive or impassive intent, allows the UAS pilot, or the pilot's employer, to learn of the intricacies of an individuals' life; including that person's daily habits, relationships, wealth, purchasing preferences, etc. Is this type of surveillance and data collection a reasonable expectation of being in "public?"

3. Data Collection and Post-Collection Uses

Even if one were to say that the initial nonconsensual collection of another individual's data would fail to constitute intrusion of that person's individual privacy interests, "the subsequent manipulation and storage of that data may warrant an alternative privacy analysis."[50] Specifically, the privacy theory of aggregation supposes that while the collection of bits of data, such as episodic data collection, may not violate an individual's privacy interests if left in piece meal form, extensive collection of information from one or multiple sources may rise to the level of a legal privacy intrusion when all information is woven together.[51]

While the privacy theory of aggregation relies upon the compilation of multiple sources, the unique all-encompassing pattern-of-life data collection that emanates from UAS surveillance, in addition to other data collection records (e.g. telephone, banking and/or utility records) only increases the unique privacy infringement beyond the mere collection of those individual data sets.[52]

Furthermore, while some individuals may not be aware of third-party data collection and sharing practices, there is generally a terms and conditions agreement at the beginning of any contract or that appears prior to application use that requires the potential customer or user to consent to their data being collected and the ways in which their data may be used. This element is completely absent in UAS data collection at this time.[53] Thus, an individual may consent to data collection multiple times in a given day—they have given their consent, and they have agreed to having certain data collected—whereas data collection by way of a UAS changes the aggregation theory by

47. *See* Craig Mundie, Privacy Pragmatism: Focus on Data Use, Not Data Collection, 93 FOREIGN AFF. 28, 31 (2014).
48. *See id.*
49. *See id.*
50. THOMPSON II, *supra* note 35, at 8-9.
51. *See* Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 507 (2006).
52. *See id.*
53. *See* id, at 494.

incorporating nonconsensual surveillance to the data compilation unbeknownst to the individual.[54]

In addition to the collection of unauthorized data, data collected by passive means, by, for instance, aerial surveillance for a land development company, has the potential to be sold to third parties.[55] Even though the data was initially collected for one specific use, it may later be used for a different use, to a different party, with different implications for the unknowing individual.[56] What are the results of this data misuse? It could result in a number of scenarios; identity theft or impersonation, personal embarrassment, or even companies making unwarranted or unwelcomed inferences about the individual's preferences or behaviors.[57]

4. Privacy Theories: Control, Autonomy, Anonymity

The use of UASs may not result in an initial categorization of an invasion of privacy in the minds of many, but as this section will discuss, UAS use implicates many of the leading privacy theories. The major tort principles to be prohibited in the realm of privacy law include: (1) intrusion upon the plaintiff's seclusion, solitude, or into his private affairs, (2) public disclosure of embarrassing private facts about the plaintiff, (3) publicity which places the plaintiff in a false light in the public eye, and lastly, (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[58] It is important to note that these privacy laws have not changed in over forty years.[59] These privacy torts were established—yet not updated—with the following privacy theories.

A leading privacy theory is based upon the premise that every individual has the right to control information about oneself, and should retain the ability to decipher to whom and what amount of his or her information should be communicated.[60] This paradigm breaks down when an individual is no longer given the opportunity to consent to the relinquishment of one's data—this will be discussed further in the next subsection concerning aggregation of collected data.[61] The question comes down to how much control should an individual have over how much he or she allows society to see?

Similar to the control theory, the theory of personal autonomy affords an individual the ability to make their own life decisions "free from interference or control by both government and private actors," which nonconsensual UAS drone collection may certainly hinder.[62] The constant

54. *See id.* at 507.
55. Mundie, *supra* note 47 at 526-27.
56. *See id.*
57. *See id.*
58. *See* Strachan, *supra* note 22 at 14.
59. *See id.*
60. *See* ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).
61. *See id.* at Infra section 2C.
62. THOMPSON II, *supra* note 35 at 7 (citing Whalen v. Roe, 429 U.S. 589, 599 (1977)).

threat of having a UAS hovering over one's home could result in self-regulated behavior as a result of the pervasive monitoring that may occur at any given time, which is a far cry from the autonomy that an individual seeks.[63] Self-regulated behavior may be as basic as someone feeling uncomfortable sunbathing in their private backyard. Kenneth Meredith, a Kentucky resident, for example, shot down a drone that was hovering over his backyard while his young daughter was sunbathing and stated, "when you're in your own property, within a six-foot privacy fence, you have the expectation of privacy."[64]

Another privacy theory drawing from the unanswered question of what is "public" is that of anonymity and one's "state of privacy that occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[65] This state of privacy is viewed as being secure when one is within his private residence and land—if this is how anonymity is perceived, then would overhead surveillance of one's own backyard violate this privacy theory?

C. Attempts at Regulating Activity

1. Regulatory Privacy Guidelines

The Electronic Privacy Information Center ("EPIC") petitioned the FAA to establish and enforce privacy rules to protect citizens from such privacy intrusions, but the FAA claimed that privacy issues "[were] beyond the scope of [their] rulemaking."[66] Rather than participate in a public notice and comment rulemaking addressing the issues EPIC wanted to discuss, the FAA teamed up with the Department of Transportation and participated in the National Telecommunications and Information Administration (hereinafter "NTIA") "multi-stakeholder process."[67] This process was "aimed at developing privacy best practices for the commercial and private use of [drones]."[68]

Ultimately however, the FAA did not create any privacy rulemaking or regulatory guidelines, as the NTIA multi-stakeholder process did not produce any legal restrictions on the use of domestic drones for aerial surveillance, nor

63. *See* THOMPSON II, *supra* note 35 at 9.

64. *See* Chris Matyszczyk, Man Shoots Down Drone Hovering Over House, CNET (July 30, 2015), https://www.cnet.com/news/man-shoots-down-drone-hovering-over-house/ [https://perma.cc/5DLX-GHJM].

65. *See* THOMPSON II, *supra* note 35 at 8 (citing WESTIN, *supra* note 60) (internal quotations omitted).

66. *See* EPIC v. FAA—What About Privacy?, DRONEBUSINESS.CENTER (Aug. 24, 2016), https://dronebusiness.center/epic-v-faa-privacy-12046/ [https://perma.cc/Q7MC-QXZM].

67. *See* id; Voluntary Best Practices for UAS Privacy, Transparency, and Accountability, NTIA, https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf [https://perma.cc/4D6L-54DK] (last visited Aug. 30, 2018).

68. *See* EPIC v. FAA—What About Privacy?, *supra* note 66.

establish any legal rights for individuals who are subject to drone surveillance in the United States.[69] Rather, the multi-stakeholder process created nonbinding "best practices" by providing UAS users with recommended privacy guidelines, information for all commercial drone pilots concerning privacy during their pilot certification process, and new guidance to local and state governments on drone privacy issues.[70]

2. State Laws and Concerns

The state of California is known for its beaches, palm trees and Rodeo Drive—all of which attract famous actors, singers, and models. Due to the lack of UAS privacy regulation by the FAA or other federal entities, California Governor Jerry Brown signed a law in 2015 to protect celebrities from paparazzi UASs.[71] The state legislation, in pertinent part, reads that a UAS operator is liable for physical invasion of privacy if that operator "knowingly enters onto the land or into the airspace above the land of another person without permission…in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff."[72]

Wisconsin legislators were concerned with illicit pictures being taken by a UAS and implemented legislation that makes it illegal to photograph a nude image with a drone.[73] The statute reads "whoever uses a drone… with the intent to photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy is guilty of …[a] misdemeanor."[74]

While California and Wisconsin have taken the initiative to establish state-based regulations on the use of UASs, they still have many issues to address concerning data and privacy that may arise from the use of such equipment. Moreover, while these state-based initiatives are steps in the right direction, drones have the capability to fly over more than one state at a time, thus requiring a more nationally-based regulation scheme rather than state-by state-imposed regulations.

---

69. *See id.*; *see also* Voluntary Best Practices for UAS Privacy Transparency and Accountability, *supra* note 67.

70. *See* EPIC v. FAA—What About Privacy?, *supra* note 66; Voluntary Best Practices for UAS Privacy Transparency and Accountability, *supra* note 67.

71. *See* A.B. 856, 2015-2016 Leg., Chapter 521, (Ca. 2015).https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB856 [https://perma.cc/EFR4-4PSG].

72. *See id.*

73. *See* Wisc. State Leg. Act 213 (2014), https://docs.legis.wisconsin.gov/statutes/statutes/942/09/5/b/2/a [https://perma.cc/SV25-E8BP] (creating Crimes Against Reputation, Privacy and Civil Liberties, Chapter 942.10, Use of a Drone).

74. *See id.*

III. ADDRESSING & ANALYZING THE PROBLEM

A. Potential UAS Privacy Infringement Concerns

Privacy expectations are changing as technology continues to grow and emerge at a rapid pace in modern times. Society as a whole may have a new sense of reasonable privacy expectations as popular technologies, like cell phones, computers and their accompanying application systems constantly track users' data. This is not to say that expectations cease to exist in some manner. For instance, individuals may be aware that by using a credit card, their purchase history may be tracked and collected and potentially sold to stores partnering with their credit card company.[75] Online shoppers, or more realistically all Internet users, may know that their search history and interests are being stored and shared through cookies.[76] Users agree to much of this data collection, and users might consider it tolerable because they are willing to give up some of their privacy for the ability to find information in seconds, share their stories and pictures with relatives and friends across the world, and have Amazon TVs and popcorn delivered to their doors at a moment's notice.

In general, it may be that the current rationale held by consumers is that personal data-collection is acceptable as long as the benefits reaped by such technology use is greater than the privacy infringing data collection. While this rationale may not be explicitly agreed upon by society as a whole, it is implicitly what a technology-user agrees to upon using any service that comes with a user agreement. As aforementioned, users often agree to have their data collected and therefore agree to give slight way to their privacy protection.

Users agree to have their data collected because they want to use the technology, or because of necessity. However, it is technically possible to live off of the data collecting grid. If individual users do not want any data collected, they have the option of not using Facebook, Instagram or Snapchat. Users do not have to go online shopping; they may do so in person at a department store using cash—not traceable credit or debit cards. While it would be rather difficult, it is not completely unfeasible for individual users to escape data collection, if they truly wanted to do so.

It seems that the "more good than harm" rationale by consensual data collection users is based on the notion that such users would rather have easy and instantaneous access to family members and news and the ability to order something online that will be delivered in two days without leaving their home. The data collected from consenting users may not be viewed as a negative—and may actually be seen as a beneficial tool for the average

75. Kate Kaye, Mastercard, AMEX Quietly Food Data to Advertisers: Privacy Concerns Prevent Some Targeting Options, ADAGE (Apr. 16, 2013), http://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800/ [https://perma.cc/GXK9-GXS3].

76. Chris Hoffman, The May Ways Websites Track You Online, HOW-TO GEEK (Sept. 28, 2016), https://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/ [https://perma.cc/2MB6-CBZC].

technological user. For instance, cookies tracking consensual users online use may lead them to learn of stores that they may not have heard of but sell the goods and provide the same services that they use on a daily basis.[77] For these types of users, the trade-off of having their data collected yields more positive results than being unable to utilize all of the modern advances that are right at their fingertips.

While this "trade-off" agreement between technology operators and technology consumers may work for present technology, it comes up short for potential commercial UAS uses. Even assuming *arguendo* that commercial UAS operators may potentially incorporate data collection agreements with the individuals using their delivery services, this agreement would still fail to address the other non-consenting individuals who may be affected by UAS data collection. While UAS use in the public commercial market is fairly new, the use has not yet reached the level of implied consent where society will just accept the trade-off—because they want these UAS services, they will deal with any and all privacy concerns. Maybe one day, but not now.

Presently, a user-data collection agreement made between, for instance, Facebook and the individual Facebook user who has agreed to have their data collected by Facebook, would be greatly at odds with a UAS operator and a UAS consumer. The disconnect between the parties lies in the UAS operator's ability to collect data from individuals who do not agree to such data collection.[78] The regulations currently in place do not address the lack of consent between UAS operators and individuals who may have data collected, either directly or for aggregate use. It does seem odd that individuals must consent to data collection when simply, and willingly, buying a pair of shoes online, but are not given the choice for opting out of UAS data collection above their homes when they are not even subscribed to such a service.[79]

Moreover, there are numerous potential beneficial uses of commercial UASs, including consumer uses in connection with instantaneous delivery services and medical delivery services, and for businesses in regard to data collection and delivery expansion opportunities.[80] The data collection of non-UASs is primarily based on consensual Internet or credit-based collection; however, privacy from data collection in your own home or backyard is an entirely different type of intrusion of privacy that has not generally been affected by non-consensual technology user agreements—until now.

---

77. *See id.*

78. *See* Solove, *supra* note 51.

79. *See id.*

80. Stephen Shankland, Zipline's Second-Gen Drones Speed its Medical Delivery Business, CNET (Apr. 2, 2018), https://www.cnet.com/news/zipline-new-delivery-drones-fly-medical-supplies-faster-farther/ [https://perma.cc/LV6B-7EQ4]; Anthony Foxx, Growing the Economy through Innovation: New Rules for the Commercial and Scientific Use of Drones, THE WHITE HOUSE: PRESIDENT BARACK OBAMA (June 21, 2016), https://obamawhitehouse.archives.gov/blog/2016/06/21/growing-economy-through-innovation-new-rules-commercial-and-scientific-use-drones [https://perma.cc/3UX8-3GJY].

B. *Current Regulations Are Missing the Mark*

Current regulations are missing the mark in addressing how much, to what extent, and whose data may be collected by way of a UAS. UASs bring up an entirely new aspect of data collection and privacy expectations. UAS operators are no longer just trying to "infringe" on users' online privacy rights but are now capable of collecting data from users'—*and non-users'*—homes and backyards.[81] While the United States' regulations have generally kept up with the times in terms of privacy and privacy expectations on smart phones and computers, the autonomy of ones' privacy within their homes may not have maintained the same adaptation.[82]

Presently, regulations in connection with UASs are primarily concerned with safety regulations and flying ordinances, not with the data collection of UAS operators.[83] As UAS technology grows, the concern must be focused on data collection and individual privacy, as well as safety. While these requirements may be sufficient to ensure that UAS operators are qualified to fly, they fall short of establishing any accountability or transparency in their operations. Presently, under FAA regulations, UAS operators are not required to publicly disclose the data collected during their flights, or what will become of the collected data, nor are they required to obtain consent for such collection from the individuals undergoing surveillance.[84]

IV. A REGULATORY COMPROMISE

While there may be no perfect solution this early in the UAS game, a regulatory framework which will provide best practices and data protection is a respectable starting point. The regulatory framework that I will propose will allow individuals to use UAS delivery services and will protect non-participants. As the use of UASs in the commercial market increases, the framework will likely be amended and nuances will be fleshed out. For now, the most important goal is to give individuals the right to protect their data through clear avenues.

As the drone industry expands, different parties, namely UAS operators and UAS consumers/users, will inevitably seek to have their various interests protected. Therefore, a regulatory framework created and implemented by Congress appears to offer the best solution to balancing data collection and protection of individuals voluntarily using UAS services as well as non-users.

The regulation proposal must address the most pressing issues in UAS data collection and privacy protection to some degree while granting agencies like the FTC and FAA the authority to create detailed means of addressing all concerns. Congress must first address the limitations of UAS consensual user

81. Smartphone Privacy, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 19, 2017), https://www.privacyrights.org/consumer-guides/smartphone-privacy [https://perma.cc/4DCK-HJG4].

82. *See id.*

83. *See* Unmanned Aircraft Systems, *supra* note 1.

84. *See id.*

agreements and create reasonable barriers that allow some data collection but prevent UAS operators from having an unlimited and unwarranted amount of leeway when collecting user data. Additionally, the regulation must address how such collected data is to be controlled in terms of third-party data sharing. Furthermore, the regulation must create boundaries for how much, how long, and what may be collected by UASs passing over non-users' homes for the protection of non-UAS users, who have not agreed to any user agreements and do no personally use any UAS services.

A. Best Practices for Collecting Data from a UAS Delivery Service Customer

This section will consider only delivery service users and will create general limitations for the type of data that may be collected. Data should be collected in an episodic manner and only for purposes of functional use—in other words, data should only be collected for purposes of advertising, generating land maps, or land surveys.

Just as in many other user agreements, the proposed UAS regulation must hold UAS operators accountable for notifying all users of the type of data that can potentially be collected and sold to third parties. While this information may deter some prospective users from using UAS services, it must be made readily available to potential users in the same fashion that the majority of other application systems, retail websites, social media websites or credit card providers inform potential users of the types of data they may collect.[85] Moreover, the UAS operators must be required to distinguish between data being collected in terms of surveillance data, and that of purchasing data—depending on the UAS service being utilized.

For instance, if Amazon's "drone" delivery service ever comes to full fruition in the United States, Amazon would have the ability to collect surveillance data of the Amazon drone delivery subscriber in two ways. First, Amazon would be able to collect data on a subscriber's land size, type of car he or she drives, or how many people live in his or her home, amongst other available data. Second, Amazon would also be able to collect the subscriber's purchasing data and may be able to use that data in its own personal advertisements. Additionally, Amazon has the ability to sell such collected data to affiliated third parties who could potentially use such data in its own aggregate data collection for future solicitation and advertising to that Amazon subscriber.[86]

---

85. Leuan Jolly, Data Protection in the United States: Overview, THOMAS REUTERS PRACTICAL LAW, http://us.practicallaw.com/6-502-0467#a686014 [https://perma.cc/YW9F-5VS4]. The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt out of these practices, providing an opt-out mechanism.

86. Kiri Masters, A Simple Guide To Amazon's Complicated Advertising Business, FORBES (June 8, 2018), https://www.forbes.com/sites/kirimasters/2018/06/08/a-simple-guide-to-amazons-complicated-advertising-business/#283aaa623910 [https://perma.cc/M858-JCA6].

Next, in terms of data collection, there must be a balance between the modern "emerging technology and incessant data collection," reasonable expectations of privacy, and simply going too far.[87] If a consumer uses UAS delivery services, they should expect to forego some privacy protections—just like other user agreements that trade service for data. While normal course of business data collection practices should be followed in terms of collecting a subscriber's purchasing history and tendencies, the new regulation should create guidelines for UAS data collection that may take place if the UAS is delivering goods to a home or business.

This type of data collection should be limited to data that can be used for advertising and for corporate use to expand programs and technology based on individuals' likes and dislikes. It should not be used as a tool to exploit or cause reputational harm or embarrassment. While it may seem difficult to view any data collection as not having some type of advertising purpose, there is certainly a limit, even if it may be very broad. Essentially, almost all data can be used for advertising purposes in one way or another, so the regulation here would give agencies the discretion to decide what those limits are and in what way the data may be construed and stored. For instance, it may be acceptable for a UAS to capture a sunbather in her backyard for the purpose of discovering what type of swim brand she is donning, but it may not be permissible to share the actual photo of her in her swimsuit. Here, the regulation should follow the lead from states like California and Wisconsin, who have already imposed data collection limitations to bar pictures of individuals that can be used in any harmful way or used as a tracking device.[88]

The relevant issue is deciding how such permissible data collection should occur via episodic surveillance or persistent surveillance.[89] As previously discussed, regardless of how much data is being collected from seemingly every type of electronic device and application system that an individual interacts with, society's expectation to maintain at least some autonomy in private residences must warrant some regulation of UAS surveillance of private residences.[90]

The reason is that while individuals may have adapted to vast data collection on the Internet and via phone applications with or without their explicit consent, such collection does not literally take place in their own homes, although these technologies are within the user's own home.[91] Thus, it would seem pertinent that the regulation should permit only episodic surveillance of a user's home and only when delivering the goods or

87. *See* United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J. concurring); *See also* Solove, *supra* note 51 at 494.

88. It is important to note the distinction between the California and Wisconsin laws which limit which types of photos may be taken of individuals and the purpose they intend to seek is in stark contrast with Street View whose intention is purely functional. *See* Assembly Bill 856, *supra* note 71; *See* Crimes Against Reputation, Privacy and Civil Liberties, *supra* note 73.

89. *See* Jones, 565 U.S. at 430-31; *see also* Solove, *supra* note 51 at 494.

90. Solove, *supra* note 51 at 90.

91. *See id.*

performing the functions that the user employed the UAS operator to partake in.

As previously addressed, when pieced together, episodic surveillance inevitably and essentially creates the same quantity of data collection as persistent surveillance would.[92] However, the regulation's restriction of allowing only episodic surveillance would more closely resemble the more familiar type of surveillance that could occur by traditional delivery services. Of course, the traditional sense of delivery would yield a less voluminous collection of data than would a UAS's "bird's eye view" advantage but would equate to a more episodic surveillance.

For example, picture a UPS delivery person given the task of both delivering a customer's packages *and* collecting data. The UPS delivery person would not persistently sit outside of the customer's home and take note of all that is visible. Rather, the UPS delivery person would go to the customer's door, deliver the customer's package, take note of the property and any other overt data, and move on to the next delivery. Thus, episodic surveillance closely resembles traditional delivery service and surveillance. While this type of suggested surveillance may incite underlying aggregation theory issues, when put in the UPS delivery person context, the aggregate data collection would still resemble the same kind of data collected on a daily basis by a delivery man.

Moreover, UASs are just yet another type of technology that individuals will inevitably be forced to become accustomed with because it seems evident that they are here to stay—just like the global use of cell phones and computers. Using this logic, the regulation should focus on limiting UAS operators to episodic surveillance because on its face, this surveillance is less intrusive than persistent surveillance. Remember that sunbathing homeowner who was trying to have a nice, relaxing day in a private backyard? While any means of intrusion in one's backyard may be initially be viewed as an intrusion—whether or not it was consented to in a user agreement—it may seem *less* intrusive if the UAS simply flew over the home and did not hover for an extended period of time. Therefore, as a way of allowing individuals to maintain some sense of autonomy and control over what they share with the corporate world, the data collection manner that is *viewed* as (and may actually be) less intrusive is the manner in which the regulation should proceed.

B. Best Practices for Collecting Data from a Non-UAS-Delivery-Services-Participant

While consenting UAS delivery service customers can expect to have more data collected from them to enhance their personalized advertisements, non-participants require protection for their privacy and data collection. The issue is how much is too much data collection? It would be unreasonable and likely impossible to require a UAS operator to be expected to turn on and off its surveillance data collection technology when flying above different homes.

92. *See id.*

While this may very well be a possibility with advanced technology, this Note takes the position that it would be unreasonable to require that these delivery services turn their data collection surveillance off and on when flying above different homes.

The regulatory framework should be two-fold, which will both limit and restrict how collected data is utilized and provide non-participants with opt-out options. As noted earlier, most UAS surveillance obtained from a street view could technically be carried out by other non-UAS means. A UAS could collect data in a more efficient manner, but a person could just as easily sit outside someone's home and obtain the same type of street view data. Thus, it seems impracticable to restrict *all* data collection, so the real protection should lie in the utilization of such collected data.

While data obtained by a publicly accessible view may be collected, it should be restricted in a manner that does not directly link the collected information with the individual surveyed. The data should be anonymized and aggregated to prevent any link between an individual and his or her respective collected data. This may work against employers of UASs because they will not be able to specifically tailor their advertisements to any one individual. However, the issue here is consumer protection, not corporate gain. Again, it is important to note that this anonymous data collection is centrally focused on the notion that it applies only to publicly accessible data.

The next element to the regulatory framework would be creating a "Do-Not-Collect" system where individuals may request that their data not be collected at all, or if it is, to be used in a specific way—whether it be for surveying purposes, advertisement purposes, etc., This system will be tailored to data that is collected beyond the scope of a publicly accessible view. This way, parties are aware that their data is being collected and can make their own autonomous choices. Additionally, this gives the option to consent to data collection if individuals enjoy having a more tailored advertisement experience or just do not care at all.

C. *What About UASs That Are Employed Only for Surveillance—Not Delivery Services?*

As with Google's *Street View* project, UASs are often used for surveillance and mapping.[93] Because privacy laws remained relatively stagnant in the latter part of the twentieth century, there is not much basis for individuals' privacy infringement claims when surveillance photos are taken from public airways into private lots—as long as the images are already readily viewable from a public space.[94]

Moreover, when looking at the "intrusion upon seclusion tort," which has been a principle of tort privacy law since the 1960s, a plaintiff must prove "an intentional intrusion upon the seclusion of their private concerns which was substantial and *highly offensive to a reasonable person*, and aver

93. *See* Domestic Unmanned Aerial Vehicles, *supra* note 19.
94. *See* Strachan, *supra* note 22 at 8, 11.

sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of ordinary sensibilities."[95] The issue with proving such an intrusion is that it is difficult for a plaintiff to contend that a mere photo of his or her home rises to the level of "highly offensive" conduct to a "reasonable person."[96] Thus, unless the present privacy tort laws are reformed, it would seem logical to follow a similar approach to that of Google's *Street View, by establishing a "take down" request system,* when regulating surveillance of both public and private property.[97]

The regulation should hold that any individual who finds a UAS surveillance-collected image to be intrusive should be given the opportunity to submit an initial formal "take down request" through the company itself. Non-compliant companies would be notified and eventually penalized by the Federal Trade Commission upon refusal to blur or delete the photo through a UAS data collection compliance department. Refusal to comply with individual take down requests would be reviewed and ruled on within the FTC's independent review board, and that would be the final decree unless the complainant chose to appeal to a federal court.

As with the Google *Street View* approach, until privacy tort law is reformed, surveillance that is not highly offensive and is taken from public property is still valid data collection. But society should still be given the opportunity to voice concerns and possibly have images removed from the Internet. Moreover, images that are not explicative or endangering and do not warrant a take down but still contain a person should always be disseminated with the face blurred. This model adapts to modern privacy expectations but still has an interested party, the compliance department, advocating for the prevention of over-indulgent UAS data collection that may violate privacy rights.

V. CONCLUSION

While modern technological emergence relies heavily on data collection, United States privacy laws have failed to keep up with the evolving and growing technical landscape. It has become more and more difficult to draw clear lines as to what constitutes privacy violation in the modern era. The regulations that this Note proposes to keep the newly developing field of commercial UASs in check are the first steps in maintaining accountability of UAS operators and their affiliates. Developing the UAS data collection regulations will provide individuals with the opportunity to engage in the new and exciting technology that UASs encompass while still offering that sun-bathing individual some privacy protection in a world that consistently shrinks the meaning of "reasonable privacy expectations."

95. *Id.* at 14 (quoting Boring v. Google, 362 Fed. App'x 273, 279) (emphasis added).
96. *See id.*
97. *See* id at 13.

9-1-1, What's Your Risk? Minimizing the Risk of Police Violence Through Computer-Assisted Dispatch

Bethany Krystek *

TABLE OF CONTENTS

* J.D., May 2018, The George Washington University Law School. Member, *Federal Communications Law Journal*, Vols. 69–70.

I. INTRODUCTION

Psychiatrist and human rights activist Ralph Crawshaw once said that "the exercise of power by a police official is one significant manifestation of an interaction between the world of the powerful and the powerless."[1] Despite Crawshaw's skepticism, one scholar suggested that "[t]he obligation of the police leadership to protect Human Rights will be fulfilled when it is realized that power for the police is not an end in itself but is a means to serve the people."[2] Yet in the last decade, those in densely populated inner cities are plagued by the following paradox: How can those specifically designated to keep us safe end up being those who many fear the most?

The nature of a police force itself promotes the idea of protection and security. In the United States, when you call 9-1-1 you feel confident the police department will know how to locate you and send help.[3] Typically, the dispatcher will ask the caller a series of questions to determine the nature and priority of the emergency using the computer-based telephone system.[4] This information is then entered into a Computer-Aided Dispatch (CAD) system.[5] The dispatcher then relays the request to a police officer, who is typically located through the use of a GPS-based vehicle locating system, which tracks the location of officers throughout the city.[6] The dispatcher then makes a subjective assessment to determine which officers to send to the location of the emergency based on the officer's distance from the emergency location and estimated time of arrival.[7] When the officer arrives, the rational constituent anticipates that the officer will address the situation by only using as much force as necessary to protect his own safety and the well-being of the surrounding community.[8] However, over the last decade in many U.S. cities, this assumption that police officers will respond by using an appropriate level of force has become rather dubious, causing increased police-related fatalities and a demise in the public trust of law enforcement.[9]

This Note will discuss some implications of current police dispatch technology and suggest an algorithm-based solution that will minimize the violent triggers brought out by Post-Traumatic Stress Disorder while

---

1. S. B. M. Prasanna, *Role of Police in Protection of Human Rights: A Review*, 2 INDIAN SOC. SCI. J. 52, 52 (2013), https://www.questia.com/library/journal/1P3-3358585851/role-of-police-in-protection-of-human-rights-a-review [https://perma.cc/R8NU-ES8U].
2. *Id.*
3. *See* Carol Fleischer, *The History of Police Communications*, CITY OF IRVINE, https://legacy.cityofirvine.org/ipd/divisions/communications/history_of_police_communications.asp [https://perma.cc/FYR3-VP67] (last visited Mar. 12, 2017).
4. *See id.*
5. *See id.*
6. *See id.*
7. *See id.*
8. *See* Jeffrey M. Jones, *In U.S., Confidence in Police Lowest in 22 Years*, GALLUP (June 19, 2015), http://www.gallup.com/poll/183704/confidence-police-lowest-years.aspx?g_source=police&g_medium=search&g_campaign=tiles [https://perma.cc/2V75-BA24].
9. *See id*.

decreasing the chance for the use of excessive force. Section I will introduce the issue of police use of excessive force and its implications. Section II will provide background on the development of police dispatch technology, including the first police communication systems, the road to 9-1-1, and the current regime: computer aided dispatch systems. Section II will also detail the rise in police use of excessive force, and the psychology behind excessive force. Section III will describe problems with the current state of CAD, including the lack of digital prevention mechanisms, the fact that post-traumatic incident policy guidelines vary widely by city, and the failure to leverage full technological capabilities. Section IV will suggest a risk-based approach to CAD, including how to revamp CAD using a coding system to leverage current technologies and how the risk-based CAD system could be applied through a national mandate. Section IV will also assess the cities where risk-based CAD would have the greatest impact, the anticipated costs of compliance with a risk-based CAD system, and the source of funding for risk-based CAD.

II. BACKGROUND

A. The Development of Police Dispatch Technology

1. The First Police Communication Systems

Although CAD and other forms of police technology provide for a quick and efficient response by emergency personnel, these are relatively new technologies aiding police communication.[10] The first documented police communications date back to Old England, where "constables[11] carried a hand bell or rattle, referred to as a ratchet."[12] The constables would sound the rattle when necessary to alert others in the surrounding area of their need for assistance.[13] These rattles were used by "police forces, fire brigades, and military units across the British Empire up through [World War I]."[14]

---

10. *See* Kenneth E. Morgan, *Computer Aided Dispatch Technology: A Study of the Evolution and Expectations of CAD and a Comparative Survey of CAD in the U.S. Fire Service and the Clark County Fire Department*, UNLV U. LIBR., https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1575&context=thesesdissertations [https://perma.cc/D87Y-AX9N] (last visited Aug. 27, 2018).

11. A constable is a British word for police officer, particularly one of the lowest rank. *Constable*. OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/constable [https://perma.cc/23RM-XFJ3] (last visited Mar. 29, 2017).

12. Gail Koger, *In the Beginning*, 9-1-1 MAG., http://www.9-1-1magazine.com/In-The-Beginning/ [https://perma.cc/D8DJ-QVXQ] (last visited Mar. 12, 2017).

13. *See id.*

14. Edward J. Steenberg, *Police Rattles & Whistles*, SAINT PAUL POLICE HIST. SOC'Y, http://www.spphs.com/history/whistles/index.php [https://perma.cc/HNS8-MLQ3] (last visited Mar. 12, 2017).

Another form of police communication was developed in the late 1800s.[15] Police communicated with one another on the streets by placing a red signal light near major intersections where officers were needed.[16] By 1870, the Chicago Police Department updated its signal lights with "call booths," accessible only by an officer or "reputable citizen" who was issued a key.[17] Inside each call booth was a "telegraph that was set up with a device that looked like a clock with a bell on top."[18] For police officers to communicate with police headquarters regarding their status, "an officer would move the pointer on the telegraph to one of eleven specific choices[19]…and pull a handle."[20] Just a decade later, the Chicago Police Department updated the call booths by adding telephones that linked the officer directly to the police department.[21]

Detroit was the first city to utilize an "on the air" voice communication for police dispatch.[22] In 1928, the Detroit Police Department began utilizing a one-way radio to facilitate arrests.[23] However, the application of the one-way radio was limited in the sense that only the police department could talk to the officer, and the officer could not directly respond; police officers had to communicate back to headquarters through telephone or call booths.[24] A marked advancement in police technology came five years later with the advent of the two-way radio, which was first used in Bayonne, New Jersey.[25] The two-way radio connected the Bayonne Police Department to nine of their patrol vehicles.[26]

With popular manufacturers such as General Electric, RCA, and Motorola mass-producing police radios, by 1940 the first statewide radio system was implemented by the Connecticut State Police.[27] Still, when an officer left his vehicle, he was unable to communicate directly with headquarters, creating a major need for a hand-held mode of communication.[28] Hand-held radios were first developed in 1960 using technologies utilized during World War II.[29] While hand-held radios were an advancement, they also had drawbacks.[30] The first hand-held radios were the

15. *See* Fleischer, *supra* note 3.
16. *See* Koger, *supra* note 12.
17. *See* Fleischer, *supra* note 3.
18. *Id.*
19. The choices "were arson, thieves, forgers, riot, drunkard, murder, accident, violation of city ordinances, fighting, testline, and fire." *Id.*
20. *Id.*
21. *See id.*
22. *See id.*
23. *See id.*
24. *See id.*
25. *See* Koger, *supra* note 12.
26. *See id.*
27. *See* Fleischer, *supra* note 3.
28. *See id.*
29. *See id.*
30. *See id.*

"size of a brick and weighed about five pounds."[31] Naturally, an officer could not carry such a heavy and cumbersome object or wear it in his or her belt without it hindering his or her actions.[32]

Still, even with these vast improvements in radio technology, a new deficit was identified.[33] Because many people did not know the seven-digit phone number for their local police department, telephone operators became "unofficial public safety dispatchers."[34] This placed telephone companies in the precarious position of determining the best point of contact for a particular emergency, often in the absence of the caller's exact location.[35] It became clear that an "easily remembered means" was necessary to "connect callers to the appropriate agency and identify their location."[36]

2. The Creation of 9-1-1

The National Association of Fire Chiefs was the organization to first call for a nationwide emergency telephone number.[37] In 1957, the Association recommended use of a single number for reporting fires.[38] A decade later, the President's Commission on Law Enforcement and Administration of Justice recommended that a single number be established nationwide for reporting emergency situations.[39] Additionally, "[t]he use of different telephone numbers for each type of emergency was determined to be contrary to the purpose of a single, universal number."[40] As a result, the President's Commission sought help from the Federal Communications Commission (FCC) to develop a single-number solution.[41]

In November 1967, the FCC met with the American Telephone and Telegraph Company (AT&T) in hopes of creating what would become a universal emergency number that could be utilized throughout the country.[42] At the time, AT&T operated a vast majority of telephone traffic in the United States.[43] In 1968, "AT&T announced that it would establish the digits 9-1-

31. *Id.*
32. *See id.*
33. *See* Fleischer, *supra* note 3.
34. *Id.*
35. *See id.*
36. *Id.*
37. *See 9-1-1 Origin & History*, NAT'L EMERGENCY NUMBER ASS'N, https://www.nena.org/?page=911overviewfacts [https://perma.cc/VH2U-7DVP] (last visited Mar. 12, 2017).
38. *See id.*
39. *See id.*
40. *Id.*
41. *See id.*
42. *See id.*
43. *See* Carolyn Abate, *History of 911: America's Emergency Service, Before and After Kitty Genovese*, PBS (Jan. 19, 2017), http://www.pbs.org/independentlens/blog/history-of-911-americas-emergency-service-before-and-after-kitty-genovese/ [https://perma.cc/T9HQ-QVJS].

1… as the emergency code throughout the United States."[44] The code 9-1-1 was chosen for two reasons:

> First, and most important, it met public requirements because it is brief, easily remembered, and can be dialed quickly. Second, because it is a unique number, never having been authorized as an office code, area code, or service code, it best met the long-range numbering plans and switching configurations of the telephone industry.[45]

Congress supported AT&T's plan and ultimately passed legislation requiring the telephone providers to absorb the cost of central office modifications and local law enforcement agencies to pay network trunking[46] costs according to tariffed rates.[47] The Executive Branch confirmed the establishment of 9-1-1 in March 1973 by issuing a "national policy statement which recognized the benefits of 9-1-1, encouraged the nationwide adoption of 9-1-1, and provided for the establishment of a Federal Information Center to assist units of government in planning and implementation" from the White House's Office of Telecommunications.[48]

9-1-1 was serving about 17% of the population of the United States by the end of 1976.[49] By 1979, 9-1-1 had extended to "approximately 26% of the population of the United States… and nine states had enacted 9-1-1 legislation," while "9-1-1 implementation was growing at the rate of 70 new systems per year."[50] By the end of the 20th century "nearly 93% of the population of the United States was covered by some type of 9-1-1 service."[51] In response to the widespread use of a single emergency number, advances in police dispatch technology soon followed.[52]

3. The Current Regime: Computer Aided Dispatch Systems

Computer Aided Dispatch (CAD) systems were developed by vendors in the 1960s to accommodate the newly created 9-1-1 systems.[53] CAD

---

44. *See 9-1-1 Origin & History*, *supra* note 37.
45. *Id.*
46. A "trunk" connects a private telephone network to the public telephone network. Trunks contain channels that facilitate incoming and outgoing telephone calls. *See, e.g.*, *Pricing*, SIP.US, http://www.sip.us/pricing/ [https://perma.cc/PJP2-2YG2] (last visited Mar. 29, 2017).
47. *See 9-1-1 Origin & History*, *supra* note 37.
48. *Id.*
49. *See id.*
50. *Id.*
51. Coverage is approximately 96% today. *Id.*
52. *See* TOM MCEWEN ET AL., COMPUTER AIDED DISPATCH IN SUPPORT OF COMMUNITY POLICING, NAT'L INST. OF JUST. (2002), https://www.ncjrs.gov/pdffiles1/nij/grants/204025.pdf [https://perma.cc/4UVS-Z3FR].
53. *See id.*

systems support two key objectives of the professional policing model: "(1) satisfying citizens with rapid responses to all calls for service and (2) effecting arrests to reduce crime."[54] The implementation of CAD technology both decreased the response time to send officers to calls for assistance and allowed for more efficient emergency resource allocation.[55]

There are two features of CAD systems that are particularly important for the purposes of this Note. First, CAD systems "provide a rich source of data because of the detailed information they contain on what patrol officers do," such as resource management, call taking, location verification, dispatching, unit status management, and call disposition.[56] Second, "less than 20 percent of the citizen calls in a CAD system are for serious crime incidents. The rest are for incidents that affect the callers' quality of life to such an extent that they believe police intervention is necessary," such as a noise complaint or reporting an abandoned vehicle.[57] Despite nationwide advances in police dispatch technology, the police have still struggled to maintain public trust.[58]

B. The Rise in Police Use of Excessive Force

Despite advances in police dispatch technology, public distrust of the police is at an all-time low. [59] The public's skepticism likely stems from numerous officer shootings involving unarmed civilians, which attracted significant media attention.[60] While the National Institute of Justice states that there is no single, agreed upon definition of "force," it notes that the "International Association of Chiefs of Police has described use of force as the 'amount of effort required by police to compel compliance by an unwilling subject.'"[61] The Legal Information Institute has further defined the term "excessive force" as "force in excess of what a police officer reasonably believes is necessary." [62] The National Institute of Justice uses five categorizations within a "Use of Force Continuum" to describe various levels of police contact.[63] The least violent method of resolution is called "Officer Presence," which categorizes incidents where no force is used.[64] The second

54. *Id.*
55. *See id.*
56. *Id.*
57. *Id.*
58. *See* Jones, *supra* note 8.
59. *See id.*
60. *See id.*
61. *Police Use of Force*, NAT'L INST. OF JUST., https://www.nij.gov/topics/law-enforcement/officer-safety/use-of-force/pages/welcome.aspx [https://perma.cc/3VM6-WZ2V] (last modified Nov. 29, 2016).
62. *Excessive Force*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/excessive_force [https://perma.cc/95U9-5NC5] (last visited Mar. 12, 2017).
63. *The Use-of-Force Continuum*, NAT'L INST. OF JUST. (Aug. 3, 2009), https://www.nij.gov/topics/law-enforcement/officer-safety/use-of-force/Pages/continuum.aspx [https://perma.cc/MG2J-ECAA].
64. *See id.*

category is "Verbalization," in which the force is not physical and the police issue calm, non-threatening demands.[65] The third category is "Empty-Hand Control," in which police officers "use bodily force to gain control of a situation."[66] The fourth category is "Less-Lethal Methods," in which less-lethal technologies are used to gain control of a situation.[67] Lastly, "Lethal Force" is defined as the use of deadly weapons used to gain control of a situation.[68] The Institute points out that this type of force "should only be used if a suspect poses a serious threat to the officer or another individual."[69] The appropriate use of force is context-specific; there is no single level that is in and of itself "excessive."[70]

Recent police shootings in Ferguson, Missouri,[71] Staten Island, New York,[72] and Charleston, South Carolina,[73] to list a small portion of many, have increased citizens' level of concern over police use of excessive force.[74] Fatal shootings across the country have ignited a public uproar and grave concern about police violence.[75] A Gallup poll in 2015 indicated that only 52% of American adults had "a great deal" or "quite a lot" of confidence in the police; this marked the lowest percent of confidence in police in 22 years.[76] 18% of Americans said they had "very little" or "no" confidence in

---

65. *See id.*

66. There are two types of "Empty-Hand Control": soft techniques and hard techniques. When using soft techniques, police officers use "grabs, holds, and joint locks to restrain an individual," as opposed to hard techniques, in which police officers use "punches and kicks to restrain an individual." *Id*.

67. There are three types of "Less-Lethal Methods": blunt impact, chemical, and Conducted Energy Devices (CEDs). Blunt impact allows an officer to "immobilize a combative person" by using a "baton or projectile." Chemical force restrains an individual by using "chemical sprays or projectiles embedded with chemicals," such as pepper spray. CEDs "immobilize" an individual by discharging a "high-voltage, low-amperage jolt of electricity at a distance." *See id*.

68. *See id*.

69. *Id.*

70. The Supreme Court has rejected a generalized excessive force standard for civil rights deprivation cases brought under 42 U.S.C. § 1983. *See* Graham v. Connor, 490 U.S. 386, 393–94 (1989).

71. *See* Larry Buchanan et al., *What Happened in Ferguson?*, N.Y. TIMES (Aug. 10, 2015), https://www.nytimes.com/interactive/2014/08/13/us/ferguson-missouri-town-under-siege-after-police-shooting.html [https://perma.cc/6UXN-TJNS].

72. *See* Deborah E. Bloom & Jareen Imam, *New York Man Dies After Chokehold by Police*, CNN (Dec. 8, 2014, 5:31PM), http://www.cnn.com/2014/07/20/justice/ny-chokehold-death/ [https://perma.cc/W8EU-M3KX].

73. *See* Alan Blinder, *Mistrial for South Carolina Officer Who Shot Walter Scott*, N.Y. TIMES (Dec. 5, 2016), https://www.nytimes.com/2016/12/05/us/walter-scott-michael-slager-north-charleston.html [https://perma.cc/42K4-HLRL].

74. *See* Martin Kaste, *After Stephon Clark Shooting, Questions Remain About Police Use Of Force*, NPR (Apr. 4, 2018, 6:02 PM), https://www.npr.org/2018/04/04/599525838/after-stephon-clark-shooting-questions-remain-about-police-use-of-force [https://perma.cc/9U8T-SZFZ].

75. *See, e.g.*, Salazar-Limon v. Houston, 826 F.3d 272 (5th Cir.), *cert. denied*, 137 S.Ct. 1277, n.2 (2017) (Sotomayor, J., dissenting) ("Some commentators have observed the increasing frequency of incidents in which unarmed men allegedly reach for empty waistbands when facing armed officers.").

76. *See* Jones, *supra* note 8.

the police, also the highest percentage in over 22 years.[77] 2016 showed a slight uptick to 56% of American adults having "a great deal" or "quite a lot" of confidence in the police; however, 14% of Americans still said they had "very little" or "no" confidence in the police.[78] Over the course of the 22-year study, Americans have only reported such minimal confidence since 2012.[79]

Although the Violent Crime Control and Law Enforcement Act of 1994 required the government to keep "data about the use of excessive force by law enforcement officers,"[80] such a database never came to fruition.[81] Even though the Bureau of Justice Statistics and the National Institute of Justice began jointly publishing an annual report in 1996 on "Police Use of Force," the Institute itself has admitted that "the mechanisms for systematically acquiring data are not yet in place."[82] Still 20 years later, there is no single streamlined source for excessive force data. The data that is currently reported on "excessive force" comes from a host of various surveys, none of which directly relate to whether the amount of police force used is justified under the circumstances.[83] While at first glance the FBI's Uniform Crime Reporting Program (UCR) appears to show more promise by posting the annual statistics regarding the number of "justifiable homicides" by law enforcement, [84] other organizations have noted problems with these

77. *See id.*

78. *See* Frank Newport, *U.S. Confidence in Police Recovers From Last Year's Low*, GALLUP (June 14, 2016), http://www.gallup.com/poll/192701/confidence-police-recovers-last-year-low.aspx?g_source=police&g_medium=search&g_campaign=tiles [https://perma.cc/D9N7-BQRG].

79. From 1993 to 2011, the combined minimal and no confidence ratings ranged from 8-13%. Only since 2012 have these same percentages consistently ranged between 13-18%. *See* Jones, *supra* note 8.

80. The Act requires that the Attorney General publish an annual summary of data acquired on police use of force. *See* 34 U.S.C. § 12602 (2017).

81. There is no national database of officer-involved shootings or incidents in which police use excessive force. *See Police Use of Force*, *supra* note 63.

82. TOM MCEWEN ET AL., *supra* note 54.

83. The following surveys collect data on various aspects of law enforcement use of force, although none are specifically devoted to unjustified use of police force: Police-Public Contact Survey (PPCS), Arrest-Related Deaths (ARD) program, Law Enforcement Management and Administrative Statistics (LEMAS), Survey of Inmates in Local Jails (SILJ), Census of Law Enforcement Training Academies (CLETA), FBI's Supplementary Homicide Reports (SHR), and FBI's Law Enforcement Officers Killed and Assaulted (LEOKA). *See Use of Force*, BUREAU OF JUST. STAT., https://www.bjs.gov/index.cfm?ty=tp&tid=84 [https://perma.cc/G3FM-A863] (last revised Mar. 10, 2017).

84. *See Expanded Homicide*, FBI: UCR, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/offenses-known-to-law-enforcement/expanded-homicide [https://perma.cc/DH43-58H4] (last visited Mar. 12, 2017).

statistics.[85] For example, UCR reports do not include any information on victims or offenders, which are provided on a separate form called the Supplementary Homicide Report (SHR).[86] David Klinger, an associate professor of criminology and criminal justice at the University of Missouri and a specialist in policing and the use of deadly force, has noted that "[n]obody that knows anything about the SHR puts credence in the numbers that they call 'justifiable homicides.'"[87] So, while we know the use excessive force may be rising, there is a gap in concrete data to show just how many of these deaths were "justifiable," as opposed to "unjustifiable."[88]

In the absence of transparent and easily accessible government data, the media has taken a significant interest in pursuing this epidemic.[89] The Washington Post now has a live database for fatal police shootings, which is searchable by state, gender, race, age, mental illness, and weapon.[90] Other criteria include whether the police officer was wearing a body camera, whether the suspect tried to flee the scene, and whether the officer responsible has been identified.[91] While these efforts meant to increase law enforcement accountability should be applauded, there is no category for "use of excessive force."[92]

The government's most recent inquiries are just beginning to uncover the deep-rooted issue of police violence. For example, the 2014 fatal Chicago police shooting of 17-year-old Laquan McDonald spurred the Department of

85. *See* Reuben Fischer-Baum, *Nobody Knows How Many Americans the Police Kill Each Year*, FIVETHIRTYEIGHT (Aug. 19, 2014, 11:36 AM), https://fivethirtyeight.com/features/how-many-americans-the-police-kill-each-year/ [https://perma.cc/N6WT-4CB3] (citing John Wihbey & Leighton Walter Kille, *Excessive or reasonable force by police? Research on law enforcement and racial conflict*, JOURNALIST'S RESOURCE, https://journalistsresource.org/studies/government/criminal-justice/police-reasonable-force-brutality-race-research-review-statistics [https://perma.cc/6NK8-HSWE] (last updated July 28, 2016)).

86. *See id.*

87. *Id.*

88. *See id.*

89. *See* Matt Apuzzo & Sarah Cohen, *Data on Use of Force by Police Across U.S. Proves Almost Useless*, N.Y. TIMES (Aug. 11, 2015), https://www.nytimes.com/2015/08/12/us/data-on-use-of-force-by-police-across-us-proves-almost-useless.html [https://perma.cc/JG72-RHGV].

90. *See Fatal Force*, WASH. POST, https://www.washingtonpost.com/graphics/national/police-shootings-2016/ [https://perma.cc/6Y7R-U7QL] (last visited Mar. 12, 2017); *see alsoHow The Washington Post Is Examining Police Shootings in the United States*, WASH. POST (July 7, 2016), https://www.washingtonpost.com/national/how-the-washington-post-is-examining-police-shootings-in-the-united-states/2016/07/07/d9c52238-43ad-11e6-8856-f26de2537a9d_story.html [https://perma.cc/53B8-VQZT].

91. *See id.*

92. *Id.*

Justice to examine the Chicago Police Department's practices.[93] The report, released January 2017, concluded that the Chicago police engaged in numerous instances of unjustified force, including "shooting at vehicles without justification, using Tasers on people who posed no threat, and using force to retaliate against and punish people."[94] The recent spotlight and unsettling discoveries on widespread police use of excessive force suggests a need to study, determine, and remedy the root cause of the issue.

C. The Psychology Behind Excessive Force

The use of excessive force has deep roots in psychology. It has long been recognized that "[e]xcessive force needs to be considered a result not only of individual personality traits but also of organizational influences."[95] While individual factors such as aggressive or abusive personalities and triggers from former job experience may make officers more prone to the use of excessive force,[96] organizational factors are perhaps more influential and more often overlooked.

Post-Traumatic Stress Disorder (PTSD) and its less severe forms are a part of everyday life for many law enforcement officers.[97] According to the Anxiety and Depression Association of America, PTSD is "a serious potentially debilitating condition that can occur in people who have experienced or witnessed a natural disaster, serious accident, terrorist incident, sudden death of a loved one, war, violent personal assault such as rape, or other life-threatening events."[98] While PTSD is generally treatable, people suffering from PTSD "continue to be severely depressed and anxious for months or even years following the event."[99]

For police officers, PTSD can be triggered in two ways: through a single traumatic event or from ongoing stress.[100] A single traumatic event

---

93. *See* Jason Hanna & Madison Park, *Chicago Police Use Excessive Force, DOJ Finds*, CNN (Jan. 13, 2017, 4:56 PM), http://www.cnn.com/2017/01/13/us/chicago-police-federal-investigation/ [https://perma.cc/6FN5-PUC6] (citing INVESTIGATION OF THE CHICAGO POLICE DEP'T, U.S. DEP'T OF JUST. C.R. DIVISION AND U.S. ATT'YS OFF. NORTHERN DISTRICT OF ILL. (Jan. 13, 2017), http://i2.cdn.turner.com/cnn/2017/images/01/13/cpd.findings.pdf [https://perma.cc/Z7R8-ZCRD]).

94. *See id.*

95. *See* ELLEN M. SCRIVNER, CONTROLLING POLICE USE OF EXCESSIVE FORCE: THE ROLE OF THE POLICE PSYCHOLOGIST, NAT'L INST. OF JUST. (1994), https://www.ncjrs.gov/pdffiles1/Digitization/150063NCJRS.pdf [https://perma.cc/8Z25-LXUQ].

96. *See id.*

97. *See* Constance Scharff, *Police Brutality and PTSD: Is There a Connection?*, HUFFINGTON POST: BLOG (Sept. 8, 2015, 9:51 AM), http://www.huffingtonpost.com/constance-scharff-phd/police-brutality-and-ptsd_b_8094396.html [https://perma.cc/YJ28-TUBD].

98. *Understand the Facts: Posttraumatic Stress Disorder (PTSD)*, ANXIETY AND DEPRESSION ASS'N OF AM., https://www.adaa.org/understanding-anxiety/posttraumatic-stress-disorder-ptsd [https://perma.cc/EZ39-44EN] (last visited Apr. 11, 2017).

99. *Id.*

100. *See* Scharff, *supra* note 99.

could be responding to a life-threatening domestic violence incident or participating in the fatal shooting of a suspect.[101] Ongoing stress includes "being witness to difficult situations that one is powerless to change," such as "responding day after day to cases of domestic violence, child abuse, desperate people stealing to put food on the table, or to help individuals who are suicidal or so high they are a threat to themselves or others."[102] Both single traumatic events and ongoing stress can significantly impact an officer's ability to do his or her job effectively, including using the appropriate amount of force.[103]

There are many similarities between the experiences of military veterans and police officers who develop PTSD.[104] Both veterans and police officers "have a culture of denying the psychological wounds their jobs can create and are sometimes inhibited by that culture and personal beliefs when it comes to seeking treatment."[105] While some focus primarily on the "[f]ailure to treat PTSD, which is estimated to affect nearly one in three officers at some point in their careers," another nexus point should center on preventing the dispatch of law enforcement officers to back-to-back violent incidents, potentially avoiding the PTSD trigger altogether.[106] It is well known that those untreated officers "are more likely than their counterparts without PTSD to overreact and make poor decisions in difficult situations."[107] Thus, a potential solution could be putting officers who are especially at risk in less risky situations.

III. PROBLEMS WITH THE CURRENT STATE OF CAD

CAD data can be particularly beneficial in identifying problems and in measuring the impact of problem solving efforts. However, CAD applications have been criticized as inadequate.[108] There are several weaknesses in CAD that stem from call classification processes.[109] For

101. *See id.*
102. *Id.*
103. *See* John Violanti, *PTSD among Police Officers: Impact on Critical Decision Making*, COMMUNITY OF POLICING DISPATCH (May 2018), https://cops.usdoj.gov/html/dispatch/05-2018/PTSD.html [https://perma.cc/XAX2-DELH].
104. *See id.*
105. *Id.* (citing Tom McGhee, *Police officers struggle with PTSD, but treatment can bring stigma*, THE DENV. POST (June 18, 2014 3:12PM), http://www.denverpost.com/2014/06/18/police-officers-struggle-with-ptsd-but-treatment-can-bring-stigma/ [https://perma.cc/WNU4-SJCE] (last updated Apr. 27, 2016 5:48AM); Hal Brown, *The Effects of Post Traumatic Stress Disorder (PTSD) on the Officer and the Family*, AM. ACAD. OF EXPERTS IN TRAUMATIC STRESS, http://www.aaets.org/article132.htm [https://perma.cc/7PZX-8QU4] (last visited Apr. 11, 2017); *What's Stopping You? Overcome Barriers to Care*, U.S. DEP'T OF VETERANS AFF., http://www.ptsd.va.gov/public/treatment/therapy-med/Stigma_Barriers_to_Care.asp [https://perma.cc/RB79-N89C] (last updated Aug. 14, 2015)).
106. Scharff, *supra* note 99.
107. *Id.*
108. MCEWEN ET AL., *supra* note 54, at 1.
109. *Id.* at 1-2.

example, "the type of call" inputted into CAD is typically based on information conveyed by the caller, who may not be able to correctly identify two related, but distinctly different crimes, such as the difference between "a burglary and a robbery or between vandalism and graffiti."[110] In addition, many call centers may fail to adequately identify each type of call, creating an over-utilized but misrepresentative "other type of call" category.[111] Other problems relate to determining the incident address, which can be problematic when "the telephone number and address from [9-1-1] systems may not be the location of the incident."[112] A final problem is the need for a new vocabulary to describe CAD information. In some cities, every record gets counted as a call for service, including "multiple calls on the same incident, assist units at the same incident, and administrative and self-initiated activities," which make it difficult to ascertain the availability of different officers on-call.[113]

In addition to the problems that have been previously posited, as discussed below, the CAD system is far from perfect. The current CAD dispatch system, accompanied by manually implemented, city-specific police department policies, creates additional flaws that can inadvertently lead to the use of excessive police force.[114] These weaknesses include a (1) a lack of digital prevention mechanisms in the CAD system, (2) a wide variance in city-specific post-traumatic incident policy guidelines, and (3) a failure to leverage CAD's full technological capabilities.[115]

A. Lack of Digital Prevention Mechanisms

Police officers use CAD to "facilitate incident response and communication in the field."[116] "Calls for service" (CFS) initiate the CAD process, in which citizens or other agencies requesting services provide "notification of events or activities of concern."[117] A CFS may originate in a variety of ways, including "alarm systems, E911 systems, direct calls…, walk-ins, CAD-to-CAD interfaces or Web-based systems."[118] Call taking entails "receiving the call, obtaining sufficient and accurate information from the caller, determining whether this is a duplicate of a call in progress, and recording or updating the CFS in the CAD system."[119] The call taker may also "verify, analyze, classify, and prioritize the call prior to routing the CFS

110. *See id.* at 2.
111. *See id.* at 2.
112. *Id.* at 2.
113. *Id.* at 2.
114. *See*, *e.g.*, STANDARD FUNCTIONAL SPECIFICATIONS FOR LAW ENFORCEMENT COMPUTER AIDED DISPATCH (CAD) SYSTEMS, U.S. DEP'T OF JUST. 1, http://www.theiacp.org/portals/0/pdfs/LawEnforcementCADSystems.pdf [https://perma.cc/QA7A-DZRN] (last visited Apr. 11, 2017).
115. *See id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*

to the dispatcher."[120] A police officer in the field may also generate a CFS by contacting the "dispatcher or the call taker, or [s/]he may actually create the call electronically using the optional MDT [mobile data terminal] interface."[121]

First, the call taker will assign the emergency a "nature code, which may include general classification and subtypes of the call."[122] Then, the CAD system will prioritize the call based on type "to determine the appropriate dispatch and response needs."[123] Following prioritization, the system "automatically evaluates the CFS location to determine…whether a call is a duplicate."[124] Then, the call taker either confirms or eliminates this possibility by evaluating the information already in the system with that obtained from the caller.[125] At this point the call taker requests the caller's basic information, including the "type of call (nature of the complaint), the priority, and the location"[126] of the emergency.[127] Once the basic information is entered into the CAD system, the fifth step is to route the call to the appropriate dispatcher.[128] The last step for the call taker is to cross-check the caller's location against address listings already in the CAD system, which can be a street address, intersection, or common place.[129]

At this point in the CAD process, the dispatcher takes over. "The dispatcher is presented with the recommended resources…based upon preset criteria for the type and priority of CFS."[130] Other information the dispatcher uses to determine the necessary resources include the "history of the location, suspect, and the possibility that hazardous materials may be involved."[131] Officers available for dispatch are designated as unassigned.[132] The CAD determines officer "proximity based on a closeness calculation, which can be distance or driving time."[133] The officer is then selected and dispatched accordingly.[134] Once the officer has left the scene, the CFS is closed.[135]

---

120. *Id.*
121. *Id.*
122. *Id.* at 4.
123. *Id.*
124. *See id.*
125. "Calls for service may be received by many sources for the same CFS, such as a traffic accident witnessed by two or more motorists or a fire alarm reported from an electronic monitoring system or a witness reporting smoke coming from a business. The call may be determined to be unique, but if it is not it will be linked to another existing call." *Id.*
126. "In many instances, the call taker has access to the call origination location" but if not, the emergency "location must be elicited from the caller." It is important to note that "the caller's location may not be the location of the call for service." *Id.*
127. *Id.*
128. *See id.*
129. *See id.*
130. *Id*. at 6.
131. *Id.* (Some CAD systems have the capability to allow the dispatcher to override the recommended resources "based on the additional information or requests by officers on the scene.").
132. *See id.* at 7.
133. *Id.*
134. *See id.*
135. *See id.* at 15.

While the current CAD system accounts for concerns for those *at* the scene, it fails to account for concerns for those *arriving* to the scene.[136] The only criteria within the current CAD system used to determine which officers are dispatched are (1) location and (2) availability.[137] No process of the system correlates the violence of the incidents with the police officers being dispatched; they are treated as wholly separate. This is a mistake given that the two concepts are deeply intertwined. For example, an officer who just finished responding to a suicide, "Officer #1," would show as "unassigned" in the dispatch system right alongside someone who just finished conducting house surveillance for eight hours, "Officer #2." The current CAD system does not differentiate between the two and thus will treat them interchangeably. If a call came in to respond to an armed robbery, Officer #1 and Officer #2 have a statistically equal chance of being deployed to the scene.

From a risk-management standpoint, this makes little sense. While Officer #1 and Officer #2 have an equal chance of being deployed, the "risk" associated with their deployment is far from equal. It is much riskier to send Officer #1 to the scene, who might overreact to the robbery and use lethal weapons as a response to the violent trigger of guns and potential hostages. Officer #2 would be a far less risky choice, as he has not experienced any incidents on duty that day that would give him a predisposition to violence. As a practical matter, it is counterintuitive to fail to take the risks of each police officer and his or her current experiences into account in CAD.

B. Post-Traumatic Incident Policy Guidelines Vary Widely by City

Although there is no formal mechanism in place to prevent police officers from responding to back-to-back violent incidents, it is nonetheless important to recognize that some police departments may attempt to manually address these concerns through their standard operating procedures. Although there is no nationwide stance on this issue, the International Association of Chiefs of Police (IACP) recommends that officers not be required to return to work immediately following a post-shooting or other critical incident intervention session.[138] Still, individual cities vary widely on their prevention mechanisms following police officer involvement in traumatic incidents. For example, the Cincinnati Police Department requires contact with police psychologists and administrative leave following an incident resulting in death or serious injury.[139] The Boise Police Department, on the other hand, notes that their recommendation of a minimum of three

136. *See id.* at 7.

137. *See id.*

138. *See* OFFICER-INVOLVED SHOOTING GUIDELINES, INT'L ASS'N OF CHIEFS OF POLICE 9 (2013), http://www.theiacp.org/portals/0/documents/pdfs/psych-officerinvolvedshooting.pdf [https://perma.cc/8WQC-3CM7].

139. *See Post Critical Incident Trauma*, CITY OF CIN., 1-2, http://cincinnati-oh.gov/police/assets/File/Procedures/19106.pdf [https://perma.cc/57XA-FDH6] (last updated Mar. 14, 2013).

days' administrative leave and initial consultation with a psychologist or psychiatrist within 72 hours of the traumatic incident are mere guidelines, not requirements.[140]

There are several problems with this policy-based approach. First, each city may determine what a "critical" or "qualifying" incident is differently, which presupposes that the traumatic effect in responding to the same types of incidents is dependent on the officer's geographical location. Second, some cities require that officers take administrative leave, while others only recommend it and may only issue it upon officer request, making the time to process a situation and address any mental health concerns dependent on the locale the officer serves.[141] Lastly, some cities may choose to see the guideline as a mere recommendation and ignore it, possibly due to a failure to recognize the risks or short staffing. Thus, the current individual city policy-based approach to risk-management is ineffective when implemented on a national scale.

C. Failure to Leverage Full Technological Capabilities

From the description of the CAD process, it is clear that the system is capable of handling multiple inputs. The CAD system is already used to intake the caller's location, nature of the emergency, and contact information.[142] This system is fully capable of adding additional inputs to account for the level of violence anticipated at the incident, based on the nature of the incident described.[143] A main part of the CAD revolution was to be able to communicate electronically with those dispatched or unassigned in various locations. Thus, the CAD system would also be capable of taking in additional information from officers when they close out each CFS.

IV. A RISK-BASED APPROACH TO CAD

While some appear to have posited a risk-based approach to CAD[144], no city has yet to implement this type of approach on a large scale with the goal of minimizing police violence. There are several benefits to utilizing a risk-based approach. Federal law enforcement agencies have noted that risk-

---

140. *See Policy Manual*, BOISE POLICE DEP'T, 22, https://police.cityofboise.org/media/8830/BPD%20Policy%20Manual%20-%20Sept%202015%2020150901_Redacted.pdf [https://perma.cc/W2L4-FQXD] (last updated Sept. 1, 2015).

141. *See Post Critical Incident Trauma*, *supra* note 141; *see also Policy Manual*, *supra* note 142.

142. *See* STANDARD FUNCTIONAL SPECIFICATIONS FOR LAW ENFORCEMENT COMPUTER AIDED DISPATCH (CAD) SYSTEMS, *supra* note 116.

143. The author confirmed this assumption with a prominent CAD Developer. Telephone Interview with Eric Sargent, Crimestar Corporation (Mar. 2, 2017).

144. A recent patent of a CAD system posits the idea that the importance of calls be ranked through a risk-assessment of the situation pertaining to the caller. *See* Protocol builder for a call handling system, U.S. Patent No. 7,646,858, at [2] (filed Apr. 11, 2007), http://www.freepatentsonline.com/7646858.pdf [https://perma.cc/WBZ2-G4FL].

based management can "enhance national interests, conserve resources, and assist in avoiding or mitigating the effects of emerging or unknown risks."[145] This created the general idea of "risk-based resource allocation," which is used in a variety of Government sectors with limited resources.[146]

A. How to Re-vamp CAD: Use of Coding to Leverage Current Technologies

The revised CAD system would require two new input components. One new component would be inputted during the 9-1-1 call by the dispatcher and another by the police officer following the incident. These components would be comprised of a risk-rating system, on a 1-5 scale. For dispatchers, the 1-5 scale would represent the severity and potential violence of the offense. For example, if the dispatcher receives a call that someone is locked out of his or her car, this would be a very low-risk incident, with a minimal chance of violence. Such an incident would receive a "1" from the dispatcher on the risk-rating scale. However, if the dispatcher receives a call from a bystander who heard shots fired across the street, this would be a very high-risk incident, with a much more likely chance of violent activity. This type of incident would receive a "5" from the dispatcher on the risk-rating scale. These numbers represent the projected level of violence necessary to gain control of a situation.

Following the incident, the police officer would input the actual level of violence used. For example, if the police officer was called to the scene of a fender bender, this would be likely a heated but nonviolent incident. This would receive a "1" or at most a "2" from the police officer on the risk-rating scale. Yet if the police officer was called to a home to break up a domestic violence dispute, this would be a more physical and intense experience, deserving of at least a "5" on the scale.

Based on these two numbers, the CAD system would change the way that police officers are dispatched to reduce the use of excessive force. Rather than solely dispatching based on location, the CAD system would use a combined algorithm of the location *and* the officer's most recent risk-rating. A potential algorithm could look something like this:

---

145. RISK MANAGEMENT FUNDAMENTALS, U.S. DEP'T OF HOMELAND SECURITY 8 (Apr. 2011), https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf, [https://perma.cc/ZD99-YKWG].

146. *See generally* Diana Farrell et al., *Risk-based resource allocation*, MCKINSEY & CO. (Feb. 2013), https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Risk/Working%20papers/42_Risk-based_resource_allocation.ashx, [https://perma.cc/9CFS-2YZL].

Dispatch = (0.5)Distance * (0.5)Risk Rating[147]

This would result in officers who are close to the scene but who also have not just responded to violent incidents being dispatched. This would reduce the chance of a police officer operating on autopilot and overexerting him or herself. While at first glance it might appear dangerous to dispatch officers who may be farther from the scene, this concern could be alleviated by first implementing a risk-rated system in some of the country's largest cities. In large cities, are most incidents in a smaller geographic area and less likely to be spread out, and these also are more likely to have police forces populous enough to minimize the risk of any significant delay in deployment.

B. Application of Risk-Based CAD Through a National Mandate

The revised CAD system should be implemented by a national mandate issued by Congress. Such a bill would typically have to pass both houses of Congress and receive a signature from the President. There would be three main components of the mandate: (1) geographical requirements, (2) anticipated costs of compliance, and (3) funding.

1. Cities Where Risk-Based CAD Would Have the Greatest Impact

A major concern, given the cost, is how many metropolitan police forces should be required to implement this mandate. The answer was again developed using an algorithm, this time based on the rate of each city's violent crimes and its overall population. The cities were determined using the following algorithm:

Greatest Need = (0.5)Population*(0.5)Rate of Violent Crime[148]

This targets cities that both (1) have the resources to allow for a risk-rated CAD system and (2) are prone to violent crime and thus pose a greater

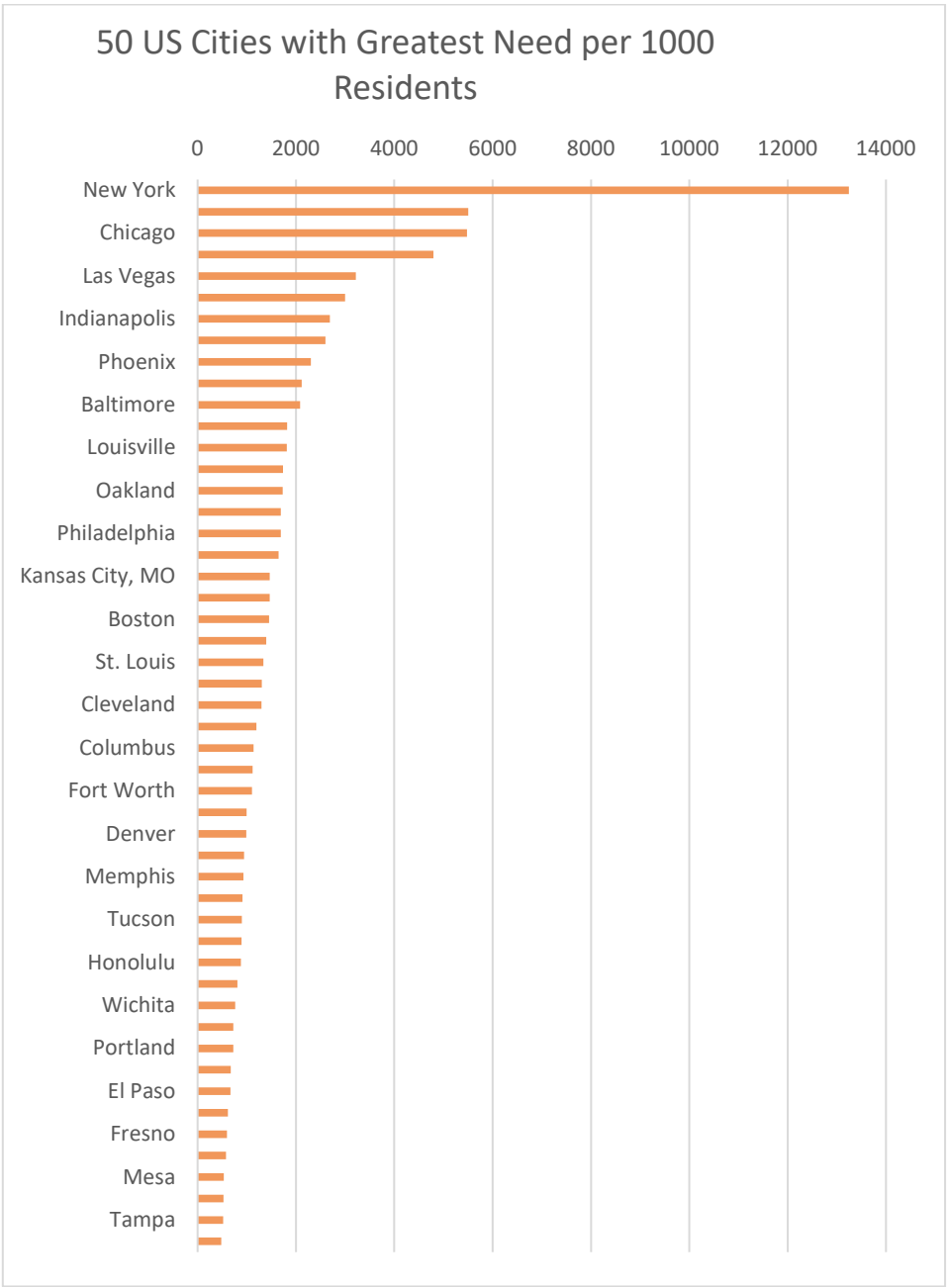
147. The algorithm would be incorporated into the dispatch system to automatically dispatch officers based on their proximity to the incident and their most recent "force" level. 0.5 was chosen as the initial factor to use for both components of the algorithm to equally consider the distance of the police officer from the scene and the potential level of violence required. Of course, the algorithm would need to be studied over time and tested for efficiency using various factors to achieve the best results. For example, it would be important to compare the current suggested factors with (0.4) Distance * (0.6) Risk Rating, and vice versa. The most effective factors would be determined both by how many times police officers were required to respond to back-to-back violent incidents using those numbers and which numbers produced the least number of excessive force interactions between civilians and the police.

148. The cities chosen to implement the algorithm would be based on their population and their most recent rate of violent crime. 0.5 was chosen as the initial factor to use for both components of the algorithm to equally consider the fact that the algorithm requires a larger police force for successful implementation and that areas ridden with violent crime will be best served by excessive force reduction efforts.

risk of requiring police officers to respond to back-to-back violent incidents.[149] The population data leveraged was from the 2014 population projections by the US Census Bureau and the rate of violent crime was leveraged from the 2014 FBI Uniform Crime Report.[150] Figure 1 below reflects the cities in most need of risk-based CAD, according to the algorithm.

149. Because E-911 funds are collected as a standard surcharge on every telephone, and telephone use (mobile or otherwise) is widespread nationwide, cities with greater populations will inherently coincide with cities that have greater public safety funding. *See generally Understanding Your Telephone Bill*, FCC, https://www.fcc.gov/consumers/guides/understanding-your-telephone-bill, https://perma.cc/86LR-C4KP (last updated Jan. 24, 2017).

150. *See 2015 Police Violence Report*, MAPPING POLICE VIOLENCE, https://mappingpoliceviolence.org/2015/, https://perma.cc/A8SU-SE63 (last visited Apr. 11, 2017) (citing *2014 National Population Projections*, U.S. CENSUS BUREAU, https://www.census.gov/population/projections/data/national/2014.html, https://perma.cc/P58M-ARKL (last visited Apr. 11, 2017); *Crime in the U.S. 2014*, FBI: UCR, https://ucr.fbi.gov/crime-in-the-u.s/2014/crime-in-the-u.s.-2014, https://perma.cc/3KXY-43ZV (last visited Apr. 11, 2017)).



As evidenced above, some of the nation's largest metropolitan cities such as New York, Houston, Chicago, and Los Angeles top the list. However, the data revealed that some smaller cities, such as Milwaukee, Oakland, and Colorado Springs also have a need.[151]

151. *See id.* (mapping killings by America's largest city police departments in 2014 and 2015 where Oakland, Milwaukee, and Colorado Springs are listed).

2. Anticipated Costs of Compliance with a Risk-Based CAD System

There are four major costs associated with implementation of a risk-based CAD system: (1) dispatch and police officer training, (2) police department policy and procedure update, (3) additional dispatcher CAD input time, and (4) CAD software update to incorporate the algorithm.[152]

a. Dispatcher and Police Officer Training

Both 9-1-1 dispatchers and police officers would need to be trained in how to use the new risk-rating system. As of the 2015 Bureau of Labor Statistics, police officers made about $29.46 per hour on average.[153] Police dispatchers made about $18.27 on average.[154] It is much more difficult to ascertain the "average" size of a police force, as such numbers vary widely based on a host of factors including the size of the city, rate of crime, etc. However, to be conservative, NYPD's force of 34,500 was used.[155] Estimates indicated that NYPD employed roughly 1,091 dispatchers in in 2009.[156] The actual presentation of the training should take no more than one hour[157] to relay the new procedure to current officers, instruct them on how to use the numbers on the risk-rated scale, and allow time for officers to ask questions. The training materials, namely a chart on how to rate specific types of incidents, would be incorporated into the policy and procedures as discussed below. Training on the new risk-rating system would be incorporated into new officer's training efforts at little to no cost, as it would become part of the normal dispatch and report-writing training. This would result in a very conservative estimate of $1,016,370[158] per department to train police officers

152. *See generally* MCEWEN ET AL., *supra* note 54. Each cost estimate is exemplary only. More study would be required to determine the precise costs required to create, obtain, and implement the proposed algorithm.

153. *See May 2015 National Occupational Employment and Wage Estimates*, BUREAU OF LAB. STAT., https://www.bls.gov/oes/current/oes_nat.htm#33-0000 [https://perma.cc/46LW-5AHE] (last modified Mar. 30, 2016).

154. *See Police, Fire, and Ambulance Dispatchers*, BUREAU OF LAB. STAT. (Dec. 17, 2015), https://www.bls.gov/ooh/office-and-administrative-support/police-fire-and-ambulance-dispatchers.htm [https://perma.cc/5WZT-ZSD6].

155. *See Frequently Asked Questions: Police Administration*, NYPD, http://www.nyc.gov/html/nypd/html/faq/faq_police.shtml#, [https://perma.cc/7QGY-EDSA] (last visited Apr. 11, 2017).

156. *See New '911' Operators Join NYPD Force of Emergency Dispatchers*, NYPD (Feb. 3, 2009), http://www.nyc.gov/html/nypd/html/pr/pr_2009_ph02.shtml [https://perma.cc/MT59-6NQK].

157. This is merely an assumption, the actually training time may be shorter or longer.

158. While at first glance this may seem significant, it is important to note that New York is over twice as large as the next biggest United States city, Los Angeles. Thus, for most cities, this number would likely be cut at least in half. *See 2015 Police Violence Report*, *supra* note 152.

and $19,165 per department to train 9-1-1 dispatchers.[159] As more is learned about the algorithm, a monthly update may be necessary for the first year of implementation to tweak the numbers preceding each variable to ensure maximum effectiveness.[160]

b. Police Department Policy and Procedure Update

To implement the new CAD system, the policies and procedures would need to be updated in each metropolitan city that initiates the change. This would require police staff to (1) describe the new processes for call intake and post-incident reporting, and (2) provide numerous examples of what differentiates each risk-rating level for both dispatchers and police officers. The updates should take no more than two hours[161] for a single police force. Per the 2015 Bureau of Labor Statistics, administrative staff made an estimated $17.55 per hour on average.[162] For the new CAD system, police department administrative staff would need to update the department's policies and procedures, at a cost of approximately $29.46 per hour on average as of 2015.[163] Thus, the policy and procedure update should result in only a minimal expense of about $94 per department. The cost to re-print the selected portion of the updated policies and procedures would also need to be factored in. As of 2017, a typical letter-size pack of paper cost about $7.99 for 500 sheets.[164] Assuming that the new policy and procedure takes no more than five pages to relay, a conservative estimate of the cost of the policy and procedure would be approximately $2,757.

c. Additional Dispatcher CAD Input Time

The additional time a dispatcher or police officer needs to input the risk-ratings into the

system and the associated costs are largely dependent on proper and thorough training. If the dispatchers and police officers have the five categorizes memorized, the input will be almost instantaneous upon hearing the complaint or departing the scene. However, if law enforcement officials spend considerable time looking up the ratings, the new CAD approach will begin to become costly. This can be avoided by providing numerous concrete examples and an interactive practice session during the initial training

159. This is a very conservative estimate given that the NYPD serves the largest city in the nation and thus has a respectively sizable police force.

160. *Supra* note 149.

161. This is merely an assumption, the actually training time may be shorter or longer.

162. *See Secretaries and Administrative Assistants*, BUREAU OF LAB. STAT. (Dec. 17, 2015), https://www.bls.gov/ooh/office-and-administrative-support/secretaries-and-administrative-assistants.htm [https://perma.cc/VGD5-BXNR].

163. *See May 2015 National Occupational Employment and Wage Estimates*, *supra* note 155.

164. *See Staples Multipurpose Paper, 8 1/2" x 11", 500/Ream (513099-WH)*, STAPLES, http://www.staples.com/Staples-Multipurpose-Paper-8-1-2-inch-x-11-inch-Ream/product_513099 [https://perma.cc/Z7GY-8LJR] (last visited Apr. 11, 2017).

exercise as well as specific examples in the policy manual. Providing officials with a concrete and visual sense of risk-rating will make any additional CAD input time negligible following a brief initial learning curve.

d. CAD Software Update to Incorporate Algorithm

In addition, there may be potential costs associated with updating the CAD technology itself. Some major developers of CAD technology, including Crimestar and TriTech, are already capable of one of the two inputs required for the algorithm to work.[165] These CAD systems currently have the capability to operate on an algorithm that prioritizes certain types of calls over others, and effectually ensures that officers respond to more dangerous emergencies more quickly than less imperative concerns.[166] For example, many dispatchers already use a 1-10 numbering system to prioritize the police response,[167] with one being the most imminent (i.e., fight in progress with a knife involved) and ten being the least imminent (i.e., barking dog).[168] Because CAD technology has the capacity for unlimited "inputs" of information relating to each call, it is unlikely that a software update would be required to indicate the level of force used after the incident as well.[169] However, to fully incorporate the risk-rated algorithm into the system, lines of code would likely need to be developed to update current CAD software.[170] The cost of the new software would likely be determined by how long it takes the programmers to develop it.[171] It is important to note, however, that because CAD technology already uses a similar response prioritization algorithm for the order of call responses, creating the code for this particular risk-rated algorithm would not prove cumbersome. After the programmers have updated the software, police departments would then need to purchase the CAD software updates individually.

3. Funding for Risk-Based CAD

a. E-911 Surcharge Increase on Phone Bills

The Federal Communications Commission (FCC) has previously authorized a surcharge on telephone bills[172] called a "911 Emergency Service

165. Telephone Interview with Eric Sargent, *supra* note 143.

166. *Id.*

167. Dispatchers must make an educated guess on the type of call based on the information provided by the caller. Due to the increased potential for initial inaccuracy, CAD technology has the capability to escalate or de-escalate calls by switching the prioritization level as more information about the incident is acquired. *Id.*

168. *Id.*

169. *Id.*

170. *Id.*

171. *Id.*

172. *See Understanding Your Telephone Bill*, *supra* note 151.

Fee."[173] Fee amounts vary by state and are usually charged as a fixed amount, but sometimes come from a percentage of the bill total.[174] The FCC has stated that the intent of the tax is to provide financial assistance to local governments' emergency services.[175] This surcharge was precisely intended to serve as financing for 9-1-1 developments and enhanced technologies to protect local communities.[176]

Although states with large cities and police forces may argue that the entire surcharge is already being utilized by other aspects of emergency services such as paying dispatchers, obtaining current city maps, and squad cars, this seems highly unlikely due to the increasing number of states, including New York, that divert the revenue from E-911 fees to non-public safety uses.[177] In New York, for example, as of January 2017, the 9-1-1 surcharge is between $0.35-$1.00 for landlines and $1.20-$1.50 for wireless telephones.[178] A recent study showed that 96% of people who live in New York City have cell phones,[179] and thus would be subjected to this tax. Therefore, a conservative estimate using $1.20 as the wireless surcharge of how much New York City obtains from the tax each year is approximately $9,781,723. Assuming these funds are being fully utilized, a negligible increase in the monthly surcharge per consumer, such as $0.20[180] could have a significant impact on the City's ability to fund the training necessary for the change. A $0.20 increase on the wireless telephone surcharge in New York City could bring in an estimated additional $1,630,287. This is over $500,000 of the estimated cost, signifying that the increase could potentially be even lower. While an increase in the 9-1-1 surcharge would surely have some impact on New York City residents, in a city whose median household income

173. *See Billing Glossary: Glossary of Terms*, VERIZON, https://www.verizon.com/support/consumer/account-and-billing/taxes-and-surcharges [https://perma.cc/X49D-SXQP] (last visited Apr. 11, 2017).

174. *See 9-1-1 Surcharge - User Fees by State*, NAT'L EMERGENCY NUMBER ASS'N (Jan. 2017), https://www.nena.org/?page=911RateByState [https://perma.cc/9QA8-28UE].

175. *See Understanding Your Telephone Bill*, *supra* note 151.

176. *See id.*

177. *See* Michael O'Rielly, *States Must Stop Raiding 9-1-1 Fees*, FCC BLOG (Mar. 1, 2017 4:52PM), https://www.fcc.gov/news-events/blog/2017/03/01/states-must-stop-raiding-9-1-1-fees [https://perma.cc/P2ZQ-ADY3].

178. *See 9-1-1 Surcharge - User Fees by State*, *supra* note 176.

179. *See* NEW YORK CITY MOBILE SERVICES STUDY: RESEARCH BRIEF, N.Y.C. DEP'T OF CONSUMER AFF. (Nov. 2015) http://www1.nyc.gov/assets/dca/MobileServicesStudy/Research-Brief.pdf [https://perma.cc/2NL4-7LPP].

180. For example, Verizon calculates the amount of monthly flat fee charges for a cell phone at the NYPD Police Headquarters (1 Police Plaza, New York, NY 10007) as $2.94 ($1.50 of that being the local 9-1-1 surcharge). Thus, a $0.20 increase in the 9-1-1 surcharge would represent approximately a 13% increase in the 9-1-1 surcharge itself and an overall flat fee increase of approximately seven percent. *See Taxes and Surcharges Estimator*, VERIZON WIRELESS, https://www.verizonwireless.com/support/taxes-and-surcharge-estimator/ [https://perma.cc/J7MK-SA9V] (last visited Apr. 11, 2017).

from 2011-2015 was $53,373,[181] this increase is unlikely to pose an undue burden when applied at the local level.

b. Achievement of Objectives Through NG9-1-1

The proposed national mandate for risk-based CAD is also supported by a national movement to re-vamp emergency services called Next Generation 9-1-1 ("NG9-1-1").[182] NG9-1-1 replaces the "existing narrowband, circuit switched 9-1-1 networks which carry only voice and very limited data" to support for additional information to be streamed to 9-1-1.[183] Some of the posited changes include the capability to receive 9-1-1 messages via text message and the ability to receive image and video transmissions as well.[184] Other changes to the network would include "access to . . . telematics data, building plans and medical information over a common data network."[185] NG9-1-1 highlights the need for a more flexible system with increased ability to share and transfer information between local and state entities as well as third parties involved in emergency services.[186] Certain vendors of CAD are already referring to their products as "aimed at, enabling, or being wholly NG9-1-1 compliant."[187]

As early as 2011, the FCC's Public Safety and Homeland Security Bureau noted that the transition from 9-1-1 to NG9-1-1 is a priority.[188] Since then, the FCC has stated that NG9-1-1 will provide "new location accuracy benchmarks for indoor as well as outdoor wireless calls" and encourage "development of 'dispatchable location[s]' as alternative[s] to coordinate-based location[s]," and that "carrier compliance with [NG9-1-1] standards will be measured based on live 911 call data starting in April 2017."[189] As of December 2015, the FCC had reported that 36 states, the District of Colombia, and Puerto Rico reported spending 9-1-1/E-911 funds on NG9-1-1

181. *See QuickFacts: New York City, New York*, U.S. CENSUS BUREAU (2015), http://www.census.gov/quickfacts/table/PST045215/3651000 [https://perma.cc/V7AA-Y54T].

182. *What is NG9-1-1?*, NAT'L EMERGENCY NUMBER ASS'N (Sept. 2008), https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf [https://perma.cc/YNB2-VL6Q].

183. *Id.*

184. *See id.* For example, such image and video streaming could provide additional support for those with disabilities, such as those hard of hearing and whom utilize American sign language as their primary form of communication.

185. *Id.*

186. *See id.*

187. *Id.*

188. *See generally* Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment, *Notice of Proposed Rulemaking*, FCC 11-134 (2011), https://apps.fcc.gov/edocs_public/attachmatch/FCC-11-134A1_Rcd.pdf [https://perma.cc/3ZC8-DACS].

189. David L. Furth, *FCC NG911 Update*, FCC PUB. SAFETY AND HOMELAND SECURITY BUREAU 3 (July 25, 2016), http://pubs.naruc.org/pub/35A09669-CACC-0D05-C039-19BB5F30EE11 [https://perma.cc/T4L9-ZQX8].

programs.[190] On a national level, approximately $165 million, roughly six percent of the total amount of 9-1-1/E-911 fees collected, are being spent on the transition to NG9-1-1.[191]

The objectives of NG9-1-1 are directly congruous with a risk-based CAD system. Both NG9-1-1 and a risk-based CAD system are directed towards improving the accuracy and reliability of 9-1-1 communications, as well as the ultimate safety of both citizens and police officers.[192] While NG9-1-1 focuses on ensuring that police officers arrive to the right locations, a risk-based CAD system ensures that the least risky police officers are being sent there.[193] Thus, a risk-based CAD system is directly aligned with the intent and purpose of NG9-1-1 and could be essential to its ultimate success. However, there is still another way to secure funding for the national mandate that does not involve increasing or diverting E-911 funds that are already used for public safety purposes.[194]

c. Full Utilization of 9-1-1 Funding

There is currently no federal mechanism to ensure that states use 9-1-1 funds for public safety purposes.[195] As a result, some states have not hesitated to take advantage of this loophole.[196] The New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act) requires the FCC to submit an annual report to Congress on the collection and distribution of 9-1-1 and E-911 fees and charges by the states, the District of Columbia, U.S. territories, and Tribal Nations.[197] The most report issued in December 2016 noted that eight states and one territory diverted their 9-1-1 fees.[198] "Iowa, New Hampshire, New Jersey, Washington, and West Virginia used a portion of their 9-1-1/E-911 funds to support non-9-1-1 related public safety programs", while "Illinois, New Hampshire, New York, Rhode Island, and Puerto Rico used a portion of their 9-1-1/E-911 funds for either non-public safety or unspecified uses."[199] Non-public safety programs receiving 9-1-1 fees included "General Funds" and "Work Promotion and Economic Activity Funds."[200] This amounts to a total of approximately $220 million in diverted

190. *See On State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, FCC, 3 (Dec. 30, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-17-61A2.pdf [https://perma.cc/DVW8-UKB4].

191. *See id.*

192. *See* Furth, *supra* note 191.

193. *See id.*

194. *See* O'Rielly, *supra* note 179.

195. *See id.*

196. *See id.*

197. New and Emerging Technologies 911 Improvement Act of 2008 § 6(f), 47 U.S.C. § 615a-1(f) (2016).

198. *See On State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*, *supra* note 192.

199. *Id.*

200. *Id.*

fees, which is approximately eight percent of total 9-1-1/E-911 fees collected.[201]

To force states to use their 9-1-1 funds solely for public safety purposes, there must be some consequences for diversion. Then-FCC Commissioner O'Rielly suggested in [year] three actions the FCC could take to remedy this problem: (1) bar diverting states from imposing 9-1-1 fees on interstate calls, (2) prevent states from collecting of funds above what will be spent directly on 9-1-1 services, and (3) exclude diverting states from Commission Advisory Committees.[202] The Commissioner also noted that Congress is fully capable of "diverting states practices either by directly applying existing law or by exerting necessary leverage via its extensive grants and funding regimes."[203] Thus, developing a remedy to ensure that 9-1-1 surcharge funds are actually spent on the maintenance and development of 9-1-1 services could be an essential factor in securing funding for a risk-based CAD system.

V. CONCLUSION

Computer-Aided Dispatch Systems could have a significant effect on reducing police use of excessive force in metropolitan communities. By employing a risk-rating mechanism to classify the types of 9-1-1 calls and the level of police violence required to gain control of an incident, police officers are less likely to respond with more violence in situations that require less violence. Re-vamping the thought process behind CAD will help police officers' mental health and workplace behavior, while also making our largest cities safer places to live and restoring confidence in local law enforcement.

201. *See id.*
202. *See* O'Rielly, *supra* note 179.
203. *Id.*

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

ACA Int'l v. FCC

Ali Kingston

885 F.3D 687 (D.C. CIR. 2018)

In *ACA Int'l v. FCC*[1], the United States Court of Appeals for the District of Columbia Circuit, granted in part and denied in part the petition for review by a number of regulated entities of a 2015 FCC order in which the FCC sought to clarify aspects of the Telephone Consumer Protection Act of 1991 (TCPA).[2] The FCC's order concerned the TCPA's general bar against using automated dialing devices to make uninvited calls.[3] This suit encompassed four issues regarding the FFC's order: (1) what automatic telephone dialing systems (ATDS) are subject to TCPA's restrictions, (2) whether the caller violates the act if the consenting party's wireless number has been reassigned to a party that has not provided consent, (3) procedures for a consenting party to revoke said consent, and (4) the TCPA's consent requirement for certain healthcare-related calls.[4] The D.C. Circuit upheld the FCC's approach on the last two issues and vacated the FCC's approach on the first two issues.[5]

Consumers have been subject to automated telemarketing calls and text messages that they have not wanted to receive for years.[6] Congress addressed this issue with the TCPA, which prohibits the use of certain ATDS absent consent from the party receiving the call.[7] The FCC issued a Declaratory Ruling and Order in 2015, which was at issue here, that addressed several petitions for rulemaking or requests for clarification on the TCPA.[8] The petitioners challenged the FCC's interpretation and implementation of the TCPA regarding ATDS.[9]

The FCC attempted to clarify that devices qualify as ATDS if the device's "capacity" includes the potential to function as an ATDS with a software modification.[10] If the FCC were to regulate every device with the potential to be an ATDS, any smartphone with the addition of certain software would qualify.[11] Under this approach, any uninvited text message or phone call from a smartphone would violate the statute.[12] The court

1. ACA Int'l v. FCC, 885 F.3d 687 (D.C. Cir. 2018).
2. *Id*. at 691.
3. *Id*.
4. *Id*. at 691-92.
5. *Id*. at 692.
6. *Id*. at 690.
7. *Id*. at 690-91.
8. *Id*. at 693.
9. *Id*. at 692.
10. *Id*. at 693-94 (citing *2015 Declaratory Ruling,* 30 FCC Rcd. at 7974 ¶ 16).
11. *Id.* at 696.
12. *Id*. at 697.

found it unreasonable for the TCPA to render every smartphone an ATDS and therefore subject to the TCPA's restrictions.[13] Even if the FCC's ruling does not conclude that smartphones are ATDS, the reasoning does not satisfy APA arbitrary and capricious review.[14]

The TCPA allows for ATDS calls "made with the prior express consent of the called party."[15] The FCC allowed for one liability-free call after a number was reassigned under the concept that the caller had a reasonable basis to believe they had consent because of a lack of knowledge that the number had been reassigned.[16] The FCC defined the "called party" as the individual who was actually reached by the caller.[17] The court found that the FCC could have adopted the Seventh Circuit's approach that instead deems the "called party" to actually be the "intended recipient" of the call.[18] The FCC's allowance for one liability-free call did not support the notion of reasonable reliance as the time period was indefinite, and the court explained—reasonable reliance could be better achieved by allowing numerous calls during a defined period of time.[19]

Under the TCPA, the FCC allows a consenting party to revoke consent at any time by any reasonable means.[20] Despite the Petitioners' objection that the FCC's approach is arbitrary and capricious, the FCC's ruling does not require the callers to adopt a system that would cause an undue burden.[21] The called party may revoke consent at any time orally or in writing as long as it makes the desire to no longer receive calls clear.[22] The court held that this interpretation is acceptable.[23]

The FCC exempts calls that have a healthcare treatment purpose from requiring consent.[24] For the public interest, the FCC does not apply the TCPA to healthcare-related calls such as: appointment and exam confirmations and reminders, wellness checkups, hospital pre-registration instructions, pre-operative instructions, lab results, post-discharge follow-up intended to prevent readmission, prescription notifications, and home healthcare instructions.[25] This exemption for wireless lines does not apply to healthcare-related solicitations, advertisements, or debt-collections.[26] Rite Aid asserted that the exemption violated the Health Insurance Portability and Accountability Act (HIPAA), but the court rejected this argument.[27]

13. *Id*. at 697-98.
14. *Id*. at 700.
15. *Id*. at 694 (citing 47 U.S.C. § 227(b)(1)(A)).
16. *Id*. at 694.
17. *Id*. at 705.
18. *Id*. at 706 (citing Soppet v. Enhanced Recovery Co., 679 F.3d 637 (7th Cir. 2012)).
19. *Id*. at 707-08.
20. *Id*. at 694.
21. *Id*. at 709.
22. *Id*. at 709.
23. *Id*. at 709-10.
24. *Id*. at 694.
25. *Id*. at 710-11.
26. *Id*. at 711.
27. *Id*.

The Court decided that the FCC was empowered to adopt the approach regarding consenting parties revoking consent and the healthcare exemption, and it adequately explained are subject to TCPA regulation and whether a caller violates the act if the consenting party's wireless number has been reassigned to a party that has not provided.

Alexander v. Verizon Wireless Servs. LLC

Laura Nowell

875 F.3D 243 (5TH CIR. 2017)

In *Alexander v. Verizon Wireless Servs. LLC*, the Fifth Circuit Court of Appeals affirmed the district court's judgement dismissing the plaintiff's complaint for failing to state a claim against the defendant, Verizon Wireless, under the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 – 2712.[28] The Fifth Circuit applied an objective standard to the good faith requirements found in the SCA, sections 2702(c)(4) and 2707(e)(1). The Court held that Verizon acted in an objectively reasonable manner after construing the facts in the light most favorable to the plaintiff.[29]

I. BACKGROUND

In 1986, Congress passed the Stored Communications Act, a part of the Electronic Communications Privacy Act, to regulate the privacy of stored communications within the United States and to control the disclosure of stored electronic communications by service providers.[30] The general purposes of the SCA include: 1) prohibiting unauthorized access to certain electronic communications, 2) restricting service providers from voluntarily disclosing the contents of customer records to certain entities and individuals, and 3) permitting a governmental entity to compel a service provider to disclose customer communications or records in certain circumstances.[31] Section 2707(c)(4) of the SCA, referred to as the "emergency exception" states, "a service provider may divulge a record or other information pertaining to a subscriber to or customer of such service…to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency…"[32]

In 2014, Verizon released subscriber records to a detective pursuant to the "emergency exception" of the SCA, which in part provided the basis for the plaintiff's arrest and the charge of aggravated arson and two counts of

28. Alexander v. Verizon Wireless Servs. LLC, 875 F.3d 243, 246 (5th Cir. 2017).
29. *See id.* at 254.
30. *See id.* at 249-50.
31. *See id.* at 250.
32. *See id.* at 251.

attempted second degree murder.[33] The detective provided Verizon with a form indicating that the information requested pertained to an arson, where a house was set on fire with two individuals inside, and the detective certified that the request potentially involved "the danger of death or serious physical injury to a person, necessitating the immediate release of information relating to the emergency."[34] Verizon subsequently provided the detective with the requested information, which included the identity of the subscriber, location information, incoming and outgoing call details, and SMS details.[35] The District Court held that Verizon is entitled to statutory immunity and a complete defense because it relied in "good faith" on an officer's representations regarding the existence of an emergency.[36] The plaintiff challenged the District Court's decision that Verizon is protected from liability under section 2703(e) and 2707(e), the "emergency exception" because the detective's request to Verizon to disclose information lacked the necessary specificity about the alleged emergency for Verizon's reliance to be in good faith.[37] Further, the plaintiff argued that Verizon failed to take additional steps to challenge the detective's assessment of the situation as an "emergency."[38]

The case did not pertain to whether the information obtained by the detective could be used against the plaintiff in any criminal proceeding brought against him, but the Court answered the following question: Could the plaintiff recover damages against Verizon through a civil lawsuit under the SCA?[39]

II. ANALYSIS

The court analyzed whether Verizon violated the SCA when it To determine if the plaintiff can recover damages against Verizon, the Court analyzed if Verizon violated the SCA by failing to act in "good faith" in its reliance on the detective's provided information to determine that the "emergency exception" allowed for Verizon to divulge certain information.[40] The Court analyzed the meaning of "good faith" under the SCA in section 2702(c)(4) and 2707(e)(1) to determine what the statute requires to constitute an act of "good faith."[41] First, pursuant to 2702(c)(4), for a provider to qualify under the emergency exception, the provider must in "good faith, believe that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of

33. *See id.* at 246-47.
34. *See id.* at 247.
35. *See id*.
36. *See id.* at 246.
37. *See id.* at 251.
38. *See id.*
39. *See id.* at 249.
40. *See id.* at 251.
41. *See id.*

information relating to the emergency."[42] Second, 2707(e)(1) requires a "good faith reliance" to trigger a complete defense.[43]

The Fifth Circuit relied on the decisions of the Seventh and Tenth Circuits to apply an objective standard of "good faith" in both contexts of the statute.[44] The Court maintained that the "objective standard" approach strikes the right "balance between providing a recourse for subscribers whose rights under the SCA have been violated and minimizing social costs."[45]

The Court concluded that Verizon relied acted in an objectively reasonable manner because Verizon only divulged non-content information and did not provide any information until the detective provided a signed and certified form which indicated that the request included the following: 1) "the danger of death or serious physical injury to a person, necessitating the immediate release of information relating to that emergency, 2) an alleged arson, and 3) victims who were within the home when it was set on fire."[46] Because the form given to Verizon included these three elements and the detective's title of senior investigator, the court found that Verizon acted reasonably.[47] In addition, the Court found that the statute does not require an element of "bad faith" nor requires Verizon to show why it had a motive to violate the statute because the plain language of the statute requires that the violation be "knowing and intentional."[48]

III. CONCLUSION

The Fifth Circuit Court of Appeals held that Verizon is entitled to statutory immunity, pursuant to the Stored Communications Act (SCA), 18. U.S.C. §§ 2701 – 2712, and is entitled to a complete defense because it relied in "good faith" on an officer's representations regarding the existence of an emergency.[49]

42. *See id.* (quoting 18 U.S.C. § 2702(c)(4) (2018)).
43. *See id.*(quoting 18 U.S.C. § 2707(e)).
44. *See id.* at 252-53.
45. *See id.* at 254.
46. *See id.*
47. *See id.*
48. *See id.* at 255 (quoting 18 U.S.C. § 2707(a)).
49. *See id.* at 246.

All American Telephone Company, Inc. v. FCC

Senrui Du

867 F.3D 81 (D.C. CIR. 2017)

I. INTRODUCTION

In *All American Telephone Company, Inc. v. FCC*,[50] the Court of Appeals for the District of Columbia Circuit granted in part and denied in part petitions for review of the FCC's order awarding damages and treading on the merits of the companies' state law claims.[51]

II. BACKGROUND

The FCC regulates common-carrier providers of wired telephone services, including the fees for "exchange access services" rendered for long distance telephone calls.[52] Those fees are often referred to as "access charges."[53] When a person places a long-distance call, a local exchange carrier operating in the caller's geographic area will route the call to an interexchange carrier.[54] That exchange carrier will connect the call to the recipient's local exchange carrier and pay an access charge to the local carrier for the connection service.[55]

Some local exchange carriers sought to artificially inflate the number of local calls they could connect, thereby increasing both the call volume and the rates that they could charge; this scheme is known as "traffic pumping."[56] Specifically, a local exchange carrier would enter into a relationship with a company that generates a high volume of telephone calls.[57] The local carrier would forgo charging its partner for the phone calls that came in, and would even pay the partner share of long-distance access rates it charged the interexchange carriers.[58] Though the local carrier and its phone-call-generating partner benefited from traffic pumping, the public and the interchange carriers bore the loss by paying significant amounts to the local exchange carriers in the form of artificially inflated access charges to

50. All Am. Tel. Co., Inc. v. FCC, 867 F.3d 81 (D.C. Cir. 2017).
51. *Id.* at 84.
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.* at 85.
57. *Id.*
58. *Id.*

complete the long-distance calls.[59] In 2010, the FCC issued a series of orders concluding that such traffic-pumping schemes were unlawful under Section 201(b) and 203(c) of the Communications Act, 47 U.S.C. §§ 201(b), 203(c).[60] The Commission ruled in particular that carriers could not charge interexchange carriers to connect long-distance calls to a non-paying end user.[61]

In the early 2000s, Beehive Telephone Company, Inc. (Beehive) created competitive local exchanges—All American Telephone Co., e-Pinnacle Communications, Inc. and Chasecom (collectively, "the Companies").[62] then had the Companies engage in a traffic-pumping scheme.[63] The Companies have only served conference-calling companies, and have never charged them for their services.[64] Beehive not only was paid by the Companies, but also could charge interexchange carriers other types of fees associated with the inflated traffic.[65]

In 2007, the Companies filed a civil suit against AT&T Corporation, seeking recovery of those access fees under a tariff collection action and a state-law *quantum meruit* claim.[66] In response, AT&T filed a counterclaim alleging that the Companies existed for the sole purpose of executing traffic-pumping schemes, which was a violation of Section 201 and Section 203 of the Communications Act.[67] The district court referred AT&T's counterclaims arising under the Communications Act to the FCC.[68]

To effectuate the referral, AT&T filed a complaint with the FCC, alleging the Companies engaged in traffic-pumping as sham entities designed to unlawfully inflate the rate of access charges billed to AT&T.[69] The FCC ruled that the Companies violated Section 201(b) of the Communications Act and had no authority to charge AT&T for services.[70] The FCC further ordered the Companies to refund the $252,496.37 that AT&T had previously paid them in access charges.[71] The Companies filed a petition for review.[72]

III. ANALYSIS

The Companies first contended that, because FCC found them to be sham entities rather than genuine common carriers, the Commission's

59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.* at 86.
63. *Id.*
64. *Id.*
65. *Id.* at 86-87.
66. *Id.* at 87.
67. *Id.*
68. *Id.*
69. *Id.* at 88.
70. *Id.* at 88-89.
71. *Id.* at 89.
72. *Id.*

jurisdiction over them evaporated, leaving it powerless to award damages.[73] The Court found that FCC has jurisdiction over complaints alleging anything done or omitted to be done by any common carrier in contravention of the provisions of the Communications Act.[74] A "common carrier" includes entities providing services pursuant to an agreement filed with FCC, even if the agreements are subsequently determined to be invalid.[75] In addition, the Court recognized that one may be a common carrier under common law by holding oneself out as such.[76] Having held themselves out as common carriers and having charged AT&T for services under a common-carrier tariff, the Companies were engaged as a common carrier for hire, and thus were subject to the Commission's jurisdiction.[77]

Next, the Companies argued that the proper measure of damages should have been AT&T's actual pecuniary loss, not the rate they paid.[78] The Companies contended specifically that AT&T failed to prove that it suffered an actual pecuniary loss.[79] The Court held that AT&T met the burden of proof.[80] AT&T presented expert declarations evidencing the amount of money it paid for no actual access services authorized by the Communications Act.[81] AT&T also causally linked its damages to the Companies' traffic-pumping scheme, showing that they were sham entities that rendered no chargeable access services to AT&T.[82] The Court held that the FCC permissibly held the Companies financially responsible for the payments they received as a result of their own conduct.[83]

After determining the measure of damages, the Court assessed its ability to decide whether the Commission's analysis of the Companies' state-law *quantum meruit* claims was proper.[84] The Commission argued that the Companies lacked standing to raise authority arguments, because the Commission's statements did not injure them.[85] To establish standing, the Companies must demonstrate a substantial risk that the district court will credit the Commission's determinations in resolving their common law claims.[86] Since the Hobbs Act[87] vests exclusive jurisdiction to review final decisions of FCC in the federal court of appeals, not the district courts, the district court would be without authority to review the merits of FCC's decision.[88] Therefore, a substantial risk of injury to the companies existed

73. *Id.*
74. *Id.* at 90.
75. *Id.*
76. *Id.*
77. *Id.* at 91.
78. *Id.*
79. *Id.*
80. *Id.* at 92.
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.* at 92-93.
85. *Id.* at 93.
86. *Id.*
87. 28 U.S.C. § 2342(1) (2018).
88. *All Am. Tel. Co., Inc*, 867 F.3d at 93.

because, once the referral was completed, the Companies would have been powerless to challenge the merits of FCC's decision before the district court.[89]

The FCC further argued that the Companies' argument was foreclosed because they failed to file a petition for review raising their objection to the FCC addressing their common law claims.[90] The Court stated that a judicial review is permitted as long as the issue is "necessarily implicated by the argument made" to the FCC.[91] In the instant case, the Companies repeatedly argued to the FCC that it "lacked the authority to address the state-law claims."[92] Therefore, the Court held that it had the ability to decide the merits of the Companies' challenge to the FCC's decision.[93]

The Court then ruled that the FCC lacked the legal authority to discuss the merits of the Companies' state-law claims.[94] Congress vested the FCC only with the authority to address allegations of actions taken in contravention of the Communications Act.[95] A state common law claim did not arise under a violation of the Communications Act, and thus fell outside the scope of the FCC's jurisdiction.[96] Moreover, for over fifty years, the FCC has held that it lacks jurisdiction to determine "the carrier's rights against a subscriber."[97] Accordingly, FCC's decision that the Companies "did not provide any service to AT&T" was improper.[98]

IV. CONCLUSION

In sum, the Court affirmed the Commission's jurisdiction over the Companies and its award of damages. The Court also vacated the Commission's decision of the Companies state-law *quantum meruit* claims.[99]

89. *Id.*
90. *Id.*
91. *Id.* (quoting *EchoStar Satellite LLC v. FCC*, 704 F.3d 992, 996 (D.C. Cir. 2013)).
92. *Id.* at 94.
93. *See id.*
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.* (quoting *Thornell Barnes Co. v. Illinois Bell Tel. Co.*, 1 FCC.2d 1247, 1275 (1965)).
98. *Id.* at 95 (quoting 30 FCC Rcd at 8966 cd.).
99. *Id.*

FTC v. AT&T Mobility LLC

Millicent Usoro[100]

883 F.3D 848 (9TH CIR. 2018)

I. BACKGROUND

In *FTC v. AT&T Mobility*, the Ninth Circuit, sitting en banc, affirmed the district court's denial of AT&T's motion to dismiss an action brought by the Federal Trade Commission (FTC) under Section 5 of the FTC Act (Act), alleging that AT&T's data-throttling plan was unfair and deceptive.[101] Data throttling is a practice by which a company intentionally reduces customers' data speeds for exceeding the threshold usage of the customer's data plan, regardless of network congestion.[102] The court initially reversed the district court's denial of the motion to dismiss, but conducted a rehearing on the issue.

AT&T argued that it is exempt from Section 5 because it fell under the common carrier exemption of the Act.[103] In its view, AT&T is an entity that has the "status" of a common carrier and therefore, all of its acts are immune from FTC authority under Section 5, "regardless of whether the entity provides both common-carriage and non-common-carriage services."[104] Furthermore, while AT&T's motion to dismiss was pending, the FCC issued an order that would prospectively classify mobile data as a common-carriage service instead of a non-common-carriage service.[105] AT&T subsequently argued that the FTC no longer had the authority to bring suit against it because of this order.[106]

The FTC argued that the common-carrier exception only applies to the common-carrier activities of an entity – thus, an entity is still subject FTC regulation for its non-common carriage activities.[107] Additionally, the agency argued that because the FCC order only applies prospectively,

100. The author was previously employed at the Federal Trade Commission; however, the author's views are her own, she does not speak on behalf of the FTC, and she did not use any non-public information to prepare this article.

101. *See* 15 U.S.C. § 45(a)(2) (2018).

102. Fed. Trade Comm'n v. AT&T Mobility LLC, 883 F.3d 848, 851 (9th Cir. 2018).

103. *Id.* Section 5(a)(2) enumerates a list of industries that are exempt from FTC authority, such as airlines, banks, and federal credit unions, and of significance to this case, common carriers. 15 U.S.C. § 45(a)(2).

104. *AT&T Mobility*, 883 F.3d at 851-52.

105. *Id.* at 852 (citing In the Matter of Protecting and Promoting the Open Internet, 30 FCC Rdc. 5601, 5734 n.792, 2015 FCC LEXIS 731 (2015)).

106. *Id.*

107. *Id.*

mobile data was not considered a common carrier service when the FTC filed its suit against AT&T.[108]

II. ANALYSIS

As a threshold issue, the court held that the district court had federal question jurisdiction because the "dispute was one arising under federal law."[109] The court then began its statutory interpretation analysis by reviewing the text and history of FTC Act and the definition of "common carrier." The court concluded that the text and history of the Act gave limited guidance, but did point to an activity-based definition of a common carrier. The court noted that Congress intentionally gave the FTC broad enforcement powers through the Act when it was enacted in 1914, and that Congress established the common-carrier exemption to avoid "interagency conflict" with Interstate Commerce Commission, an agency established in 1887 that regulated common carriers.[110] While the court noted that Congress has never defined the term "common carrier," the Communications Act defined it as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy."[111] The definition was extended to telecommunications carriers in the Telecommunications Act of 1996.[112]

The court rejected AT&T's argument that Section 6 of the Act, which was enacted in 1973 and governs the FTC's investigative authority, illuminates on the scope of the FTC's enforcement capabilities because the amendment was passed "almost six decades after the FTC Act" and "does not modify Section 5."[113] The court also rejected AT&T's arguments that failed amendments of the FTC Act and a revision of another exempt entity of Section 5 authority shed light on the Act's meaning.

The court then turned to the judicial interpretation of "common carrier" and concluded that case law strongly suggests an activity-based interpretation of the exemption.[114] The court noted that "common carrier had a well-understood meaning by 1914" because of various Supreme Court cases that illuminated its view that "common carrier entit[ies] [were] not a unitary status for regulatory purposes."[115] The court also analyzed its own interpretations of "common carriers," noting cases where it held that an entity can be a common carrier "in some instances but not in others,

108. *Id.*

109. *Id.* at 853 (internal quotations and citations omitted).

110. *Id.* at 854-55. The ICC regulated telephone common carriers until Congress passed the Communications Act of 1934, which created the FCC with regulatory authority over telephone common carriers. *Id.* at 855.

111. *Id.* at 855 (citing 47 U.S.C. § 153(11) (2018)).

112. *Id.* at 856 (citing 47 U.S.C. § 153(51) (2018)).

113. *Id.* at 856-57.

114. *Id.* at 858.

115. *Id.* at 863 ("we afford the agencies some deference under *Skidmore* [].").

depending on the nature of the activity which is subject to scrutiny."[116] The court also noted cases involving common carriers in the D.C., Eleventh, and Second Circuits that suggested that the term "common carrier" is an activity-based status.[117]

Finally, the court gave weight to the FCC and FTC's interpretations of "common carrier."[118] The FCC in its amicus brief argued "the Communications Act and the FTC Act fit hand-in-glove to ensure there is no gap in the federal regulation of telecommunications companies" and a status-based interpretation could potentially "open a … substantial regulatory gap and greatly disrupt the federal regulatory scheme."[119] Because the FCC regulates common-carriage activities, the FTC Act fills in the regulatory gap of the Communication Act through its enforcement authority over telecommunications providers when they are not engaged in common-carriage activities, such as data-throttling at the time the FTC filed its action against AT&T.[120] The court recognized that agencies often have concurrent jurisdiction and share regulatory authority over entities, "as different federal agencies bring to the table discrete forms of expertise and specific enforcement powers."[121] The court also noted past activity-based interpretations by both agencies.[122] The court rejected AT&T's argument that the FCC order reclassifying mobile data service to common carriage service because the order explicitly stated a presumption against retroactivity, and the FTC brought the authority to pursue the case before the order was issued.[123]

III. CONCLUSION

The Ninth Circuit affirmed the denial of AT&T's motion to dismiss and adopted an activity-status based definition of the common carrier exemption after reviewing the legislative history of the FTC Act, judicial interpretations of the term "common carrier," and the FTC and FCC's own interpretations of and expertise on common carriers. The court concluded that the FTC did have enforcement authority over mobile data because

116. *Id.* at 860 (quoting McDonnell Douglas Corp. v. Gen. Tel. Co., 594 F.2d 720, 724-25 n.3 (9th Cir. 1979)).

117. *Id.* (citing Fed. Trade Comm'n v. Verity Int'l, Ltd., 443 F.3d 48, 58 (2d Cir. 2006) ("courts must examine the actual conduct of an entity to determine if it is a common carrier for purposes of the FTC Act exemption"); Eagleview Techs., Inc. v. MDS Ass'n, 190 F.3d 1195, 1197 (11th Cir. 1999) ("an entity is not considered a common carrier unless it is 'engaged' in rendering services"); Nat'l Ass'n of Regulatory Util. Comm'rs v. Fed. Commc'n Comm'n, 533 F.2d 601, 608 (D.C. Cir. 1976) ("one can be a common carrier with regard to some activities but not others.").

118. *Id.* at 861-62.

119. *Id.* at 862.

120. *See id.*

121. *Id.*

122. *Id.* at 862-63.

123. *Id.* at 864.

mobile data was not a common carrier service at the time the suit was filed.[124]

124. *Id.* at 850.

Latner v. Mount Sinai Health System, Inc.

Kimberly Hong

879 F.3D 52 (2D CIR. JAN. 10, 2018)

The Telephone Consumer Protection Act ("TCPA") states that the act of sending automated calls or text messages to cell phones is unlawful, except when certain exemptions are present or when the individual consented.[125] In *Latner v. Mount Sinai Health System*, the United States Court of Appeals for the Second Circuit reviewed and affirmed the United States District Court of the Southern District of New York's dismissal of the case, holding that automated text messages sent were part of the exceptions and the Plaintiff-Appellant consented to the automated messages.[2]

I. BACKGROUND

In 2003, Daniel Latner ("Plaintiff–Appellant") visited Mount Sinai Health Systems ("Defendants–Appellees") for a health examination.[3] During his visit, the Plaintiff–Appellant completed new patient forms.[4] As part of the new patient forms, the Plaintiff–Appellant signed the "New Patient health form containing his contact information" and the "Ambulatory Patient Notification Record" that allows the Defendants–Appellees to "use [the Plaintiff–Appellant's] health information 'for payment, treatment and hospital operations purposes.'"[5]

In June 2011, the Defendants–Appellees hired PromptALERT, Inc. to send phone and/or text messages such as flu shot reminders to clients.[6] During the month of November 2011, the Plaintiff–Appellant visited the Defendants–Appellees office and "declined any immunizations."[7] Then, on September 19, 2014, the Plaintiff–Appellant received an automated text message from the Defendants–Appellees stating to schedule a flu shot appointment along with a number to call.[8] The Plaintiff–Appellant claims

125. *See* Telephone Consumer Protection Act, 47 U.S.C. § 227 (2015).

[2] *See* Latner v. Mount Sinai Health Sys., 879 F.3d 52, 55 (2d Cir. 2018).

[3] *See id.* at 53.

[4] *See id.*

[5] *Id.*

[6] *See id.*

[7] *Id.* at 54.

[8] *See id.* ("Its flu season again. Your PCP at WPMG is thinking of you! Please call us at 212–247–8100 to schedule an appointment for a flu shot. (212– 247–8100, WPMG).").

that the Defendants–Appellees violated Section 227(b)(1)(A)(iii) of the TCPA by sending the automated flu shot reminder.[9]

The United States District Court for the Southern District of New York granted the Defendants–Appellees' motion for judgment on the pleadings and dismissed the case.[10] The Plaintiff–Appellant timely appealed the decision to the United States Court of Appeals for the Second Circuit.[11] The Second Circuit reviewed the District Court's holding to grant the Defendants–Appellees' motion for judgment on the pleadings *de novo*.[12]

II. ANALYSIS

The central issue presented before the court was whether the act of sending out an automated text message that reminded individuals to obtain a flu shot violated the TCPA.[13] The TCPA "makes it unlawful to send texts or place calls to cell phones through automated telephone dialing systems, except under certain exemptions or with consent."[14]

The court first began looking at the legislative history.[15] First, the court explained that "Congress delegated authority to issue regulations under the TCPA to the Federal Communications Commission ("FCC")."[16] Second, in a 1992 Order, the FCC construed the "TCPA's prior-express consent provision" to mean that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary."[17] Third, in 2008, the FCC extended the interpretation to cellular devices.[18] Fourth, in 2012, the FCC created a "Telemarketing Rule" that required "prior *written* consent for autodialed or prerecorded telemarketing calls."[19] Under the "Telemarketing Rule," the FCC also stated that one is exempt from the requirement of written consent for calls to cellular devices if the message "delivers a 'health care' message made by, or on behalf of, a 'covered entity' or its 'business associate,' as those are defined in the HIPPA Privacy Rule.'"[20] The HIPPA Privacy Rule laid out the meaning of

---

[9] *See id.*; *see also id.* at n. 1 (stating "47 U.S.C. § 227 (b)(1)(A)(iii) provides that, '[i]t shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States . . . to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or prerecorded voice... to any telephone number assigned to a . . . cellular telephone service.'").

[10] *See id.* at 54.

[11] *See id.*

[12] *See id.*

[13] *See id.* at 53.

[14] *Id.* at 54 (citing 47 U.S.C. § 227 (b)(1)(A)(iii) (2018)).

[15] *See id.*

[16] *Id.* (citing 47 U.S.C. § 227(b)(2) (2018)).

[17] *Id.* at 54.

[18] *See id.*

[19] *Id.* (quoting In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 27 FCC Rcd. 1830, 1838, ¶ 28 (2012)) (internal quotations omitted).

[20] *Id.* at 54–55 (quoting 47 C.F.R. § 64.1200(a)(2) (2018)).

health care "to include 'care, services, or supplies related to the health of an individual' . . . [and] exempts from its definition of marketing all communications made '[f]or treatment of an individual by a health care provider . . . or to direct or recommend alternative treatments' to the individual."[21]

The District Court held that the text message sent to the Plaintiff–Appellant by PromptALERT, Inc. on behalf of the Defendants–Appellees was an exception under the HIPPA Privacy Rule.[22] The Second Circuit held that although the District Court correctly determined this matter, the District Court's analysis was incomplete, as it did not determine whether the Plaintiff–Appellant gave prior express consent.[23] The Second Circuit affirmed the District Court's holding "on the grounds that, considering 'the facts of the situation,' the text message did indeed fall within 'the scope of [Plaintiff–Appellant's prior express] consent.'"[24] The court reached this conclusion because the Plaintiff–Appellant (1) gave his cell phone number to the Defendants–Appellees and (2) he signed a form acknowledging receipt of "various privacy notices."[25] The court held that when the Plaintiff–Appellant provided his signature on the form, he "agreed that [the Defendants–Appellees] could share his information for 'treatment' purposes."[26] The privacy notices that the Plaintiff–Appellant signed also stated that the Defendants–Appellees could use the Plaintiff–Appellant's "information 'to recommend possible treatment alternatives or health-related benefits and services.'"[27]

III. CONCLUSION

The United States Court of Appeals for the Second Circuit affirmed the United States District Court of the Southern District of New York's decision granting the Defendants–Appellees' motion for judgment on the pleadings and dismissal of the case because the Plaintiff–Appellant provided prior express consent to be sent an automated text message "about a 'health-related benefit[ ]' that might have been of interest to him and the message was covered by an exemption under the TCPA."[28]

---

[21] *Id.* at 55 (citing Public Welfare Act, 45 C.F.R. §§ 160.103, 164.501 (2014)).
[22] *See id*.
[23] *See id.*
[24] *Id.* (citing 29 FCC Rcd. at 3446, ¶ 11).
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

Nueva Esperanza, Inc. v. FCC

Brooke Thompson

863 F.3D 854 (D.C. CIR. 2017)

I. INTRODUCTION

In *Nueva Esperanza, Inc. v. FCC*,[126] the United States Court of Appeals for the District of Columbia Circuit affirmed the Commission's decision to dismiss the Appellant's application to construct and operate a LPFM radio station in Philadelphia, PA. The Court held the Appellant forfeited its argument regarding fair notice because it incorrectly interpreted a blog post authored by the Chief of the Media Bureau, which was intended to provide guidance to applicants,.

II. BACKGROUND

In 2000, the Federal Communications Commission introduced the Low Power FM Radio (LPFM) service designed "to create opportunities for new voices on the air waves and to allow local groups, including schools, churches and other community-based organizations, to provide programming responsive to local community needs and interests."[127] Licenses for LPFM stations are limited to "noncommercial, educational entities and public safety entities."[128]

To resolve "mutually exclusive" LPFM applications by commercial applicants, the Commission is required to use a competitive bidding system.[129] However, the Commission instead uses a noncommercial method of resolving mutually exclusive LPFM applications through a point system.[130] Under that system, the Commission awards an applicant one point for each of six characteristics, such as having an "established community presence of at least two years."[131]

During the October 2013 filing period, several community organizations applied to construct an LPFM station in Philadelphia, PA.[132] Among these organizations was the Appellant, Nueva Esperanza, Inc., a

126. Nueva Esperanza, Inc. v. FCC, 863 F.3d 854 (D.C. Cir. 2017).

127. *Id.* at 856 (citing Creation of Low Power Radio Service, 15 FCC Rcd. 2205, 2213 (2000)).

128. *Id.* (quoting 15 FCC Rcd. at 2209)

129. *Id.* (citing 15 FCC Rcd. at 2213).

130. *Id.* (citing 15 FCC Rcd. at 2258).

131. *Id.* (quoting *Commission Identifies Tentative Selectees in 111 Groups of Mutually Exclusive Applications Filed in the LPFM Window*, 29 FCC Rcd. 10847, 10848 (2014)).

132. *Id.* (citing *Media Bureau Identifies Mutually Exclusive Applications*, 28 FCC Rcd. 16713, 16715 (2013)). (case name should not be in italics)

nonprofit organization based in Philadelphia.[133] Eleven of those applications, including the Appellant's, were deemed mutually exclusive.[134] The Appellant, along with six other applicants were awarded five points each, thus creating a seven-way tie. To break the tie, two or more of the tied applicants may propose to share use of the LPFM station by filing a time-share proposal.[135] The point totals of those applicants will be aggregated if they submit an acceptable time-share proposal.[136]

Four of the tied applicants, not including the Appellant, received twenty points by filing a joint timeshare application.[137] This group was comprised of G-Town Radio, Germantown United Community Development Corp., Germantown Life Enrichment Center, and South Philadelphia Rainbow Committee Community Center, Inc. ("Timeshare Applicants").[138] The Appellant received a total of ten points by filing a timeshare application with just one other applicant, the Social Justice Law Project of the Philadelphia NAACP, Inc.[139] Because they had a higher point total, the Timeshare Applicants were awarded the LPFM station license.[140]

Just two months before the Timeshare Applicants filed their joint agreement, the Appellant petitioned the Commission to deny several applications for violating the Commission's rule prohibiting multiple applications by or on behalf of the same applicant.[141] Among those applications the Appellant petitioned the Commission to deny were three of the Timeshare Applicants and another Germantown applicant: G-Town Radio, Germantown United Community Development Corp., Germantown Life Enrichment Center, and Historic Germantown. The Appellant alleged the parties were acting on behalf of G-Town Radio. However, the parties filed an opposition, claiming they were all independent entities with the intention of operating the LPFM station on their own. They recognized that "their best chance at operating a station dedicated to Germantown was by working together at the outset with plans to potentially aggregate points during the mutually exclusive. . .stage so that they might share time on a single station."[142]

The Appellant replied by arguing that the pre-application collaboration by the parties was prohibited according to a blog post, authored by William T. Lake, the Chief of the Media Bureau, which was released to give applicants guidance concerning the application process for

133. *Id.*
134. *Id.*
135. *Id.* (citing 29 FCC Rcd. at 10852).
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.* at 856–57.
142. *Id.* at 857.

the then-upcoming October 15, 2013 to November 14, 2013 application window.[143] Mr. Lake noted in paragraphs three and four of the blog post:

> Third, we will permit organizations in a community to work together to file a single. . . application. Alternatively, organizations in a community could apply separately — for the same or different frequency — knowing that they may decide later to aggregate points so they can negotiate a time-share agreement if the Commission determines that they are tied with the highest point total in the same mutually exclusive group . . .[144]
>
> Fourth, please bear in mind that it is the *specified* applicant on the application who must intend to carry out the station construction and operation described in the application. Therefore, multiple groups should not attempt to maximize the chances of receiving an LPFM construction permit by submitting multiple applications under the different groups' names with a prior understanding that the groups will later share time or ownership with each other if just one applicant succeeds in getting a construction permit. If this prior understanding does exist, then all the applicants must be listed as parties to the application, and only one application can be filed (our rules only allow for one application per organization). The FCC requires applicants to be truthful when listing all the parties that have control over the applicant entity and, in the event the application is granted, would have control over the future LPFM station.[145]

The Media Bureau responded by denying the Appellant's petition to deny the applications of the four Germantown parties.[146] The Bureau concluded that the Appellant failed to demonstrate that the Germantown parties violated any of the Commission's rules in conjoining their applications with the intent of filing a joint time-share or that the applications were filed for the benefit of just G-town.[147]

First, the Bureau found no evidence of common control among the Germantown parties, as each functioned independently.[148] Second, the Bureau noted the benefit of the final time-share group could not have been for the sole benefit of Germantown because of the inclusion of a non-

143. *Id.* (citing *Updated: The Low Power FM Application Window Is Fast Approaching*, FCC BLOG (Oct. 21, 2013, 3:13 PM), https://www.fcc.gov/news-events/blog/2013/10/21/updated-low-power-fm-application-window-fast-approaching).

144. *Id.* at 857 (citing *Updated: The Low Power FM Application Window Is Fast Approaching*, *supra* note 19).

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

Germantown Applicant as well as the exclusion of Historic Germantown.[149] Furthermore, the Bureau noted the third paragraph of the Blog Post specifically approved of agreements to collaborate: "there is no rule prohibiting LPFM applicants from filing separate applications with the goal of arriving at a timeshare agreement, provided that each applicant remains under *separate control* and intends to construct and operate the proposed station if its application is granted."[150]

The Appellant petitioned the Media Bureau for reconsideration, opposed by the Timeshare Applicants, which the Bureau denied.[151] The Bureau stated that the Appellant misinterpreted the blog post.[152] The Appellant then sought review from the Commission, which the Commission denied for the same reasons given by the Bureau.[153]

III. ANALYSIS

A. Commission's Interpretation of the Blog

The Appellant argued the blog post stated that entering into time-sharing arrangements by applicants was prohibited before the applicants filed their applications and until the Commission announced the points awarded to each applicant.[154] The Appellant relied on the fourth paragraph of the post, that stated:

> [M]ultiple groups should not attempt to maximize the chances of receiving an LPFM construction permit by submitting multiple applications under the groups' names with a prior understanding that the groups will later share time or ownership with each other if just one applicant succeeds in getting a construction permit.[155]

The Commission argued, however, that this interpretation was inconsistent with the third paragraph of the blog post, which stated:

149. *Id.*
150. *Id.* at 858 (emphasis added).
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.* at 858–59.

> [O]rganizations in a community could apply separately – for the same or different frequency – knowing that they may decide later to aggregate points so they can negotiate a time-share agreement if the Commission determines that they are tied with the highest point total in the same mutually exclusive group.[156]

The Appellant then contended that the third paragraph merely explained that parties are "obviously allowed to *know*" that aggregation of points upon the awarding of tied point totals to multiple applicants was allowed.[157] However, the Appellant argued that the fourth paragraph prohibited applicants from entering into a "preexisting agreement to share points."[158] In other words, the Appellant claimed that "'know[ledge] that [the applicants] may decide later to aggregate points, as permitted by the Third Paragraph,' [wa]s different from a 'prior understanding that the groups will later share time,' as prohibited by the Fourth Paragraph."[159] However, because the record did not show the Germantown applicants entered into any sort of binding agreement, the court held that this distinction by the Appellant was irrelevant.[160]

Furthermore, the Appellant argued that its understanding of the blog post was more sensible than the Commission's. The Appellant contended that the Germantown applicants essentially "stack[ed] the deck in their favor. . .virtually ensur[ing] they would win the license from the outset."[161] They argued that while the Commission's reading of the blog post allowing agreements to aggregate points before selectees were announced would invite "gamesmanship," the Appellant's reading would level the playing field for applicants acting in good faith.[162] The Commission, however, accepted the risk of some gamesmanship because it proved to be one of "the most efficient and effective means of resolving mutual exclusivity among tied LPFM applicants."[163]

Finally, the Appellant petitioned the Bureau for reconsideration, arguing the blog post established a Commission policy prohibiting LPFM applicants from filing individual applications with the goal of aggregating points.[164] The Bureau contended that the blog post constituted only the "informal writings of [an] individual[], not [a] formal statement[] of agency policy," and therefore "would be non-authoritative even had it expressed the proposition [Esperanza] allege[s]."[165] The Bureau rejected the Appellant's argument that Mr. Lake's blog post should have been deemed authoritative simply because he served as the Chief of the Media Bureau, explaining that

156. *Id.* at 859.
157. *Id.*
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.* at 860.
162. *Id.*
163. *Id.* (citing 27 FCC Rcd. 15402, 15474 (2012).
164. Nueva Esperanza, Inc. v. FCC, USCA Case #15-1500 at 15 (filed June 13, 2016) (appellee's brief).
165. *Id.*

the "[a]dvice of a Bureau Chief, while that of a high level staffer, remains that of a staffer," and nothing more.[166]

B. Fair Notice

The Appellant argued it did not have fair notice of the Commission's interpretation of the blog post.[167] To preserve its argument for appellate review, the Appellant was required to present it to the Commission in its application for review of the Media Bureau's decision. The appellant argued that made the argument when it said it would have tried to make a similar time-sharing agreement "[h]ad the policy on pre-application and pre-mutually exclusive phase agreements to aggregate points and agree to timeshare agreements been clear."[168] However, the court ruled the Appellant forfeited its fair notice argument and did not provide a valid objection to the Commission's decision.[169]

IV. CONCLUSION

Because the Appellant's interpretation of the Blog Post was incorrect and the Appellant forfeited its fair notice argument, the decision of the Commission was affirmed.

166. *Id.* at 15-16.
167. *Id.* at 860.
168. *Id.* at 860-61.
169. *Id.* at 861.

Press Communications, LLC v. FCC

Kimberly Hong

875 F.3D 1117 (D.C. CIR. 2017)

In *Press Commc'ns, LLC v. FCC*, the United States Court of Appeals for the District of Columbia Circuit declined to review an FCC Order that rejected a radio station's request to swap channels with another radio station because it violated the FCC's channel spacing requirements.[170]

I. BACKGROUND

Section 301 of the Communications Act of 1934 ("Act") "confers on the United States control 'over all the channels of radio transmission,'"[171] and Section 303 of the Act gives the Federal Communications Commissions ("FCC") the power to "implement[] a licensing scheme pursuant to the Act . . . and sets 'public convenience, interest, or necessity as the [FCC's] guiding principles."[172] Furthermore, every radio station requires a license provided by the FCC,[173] and a license term cannot last for more than eight years.[174] However, a license can be renewed and must follow the FCC's regulations.[175] Under Section 73.3539, a renewal application must be sent "at least four months before the expiration of their current license term."[176]

The FCC must also authorize any modification of a radio station's license.[177] Modification of a radio station includes a "'major change' such as new ownership" or a "'minor change' such as change to adjacent channel."[178] In order to comply with the FCC rules and regulations, each application for modification must be "accompanied by an appropriate request for waiver."[179] A license modification is handled on a "'first come/first serve' processing sequence"[180] Under this processing sequence, "the first acceptable application cut[s] off the filing rights of subsequent applicants."[181]

170. *See* Press Commc'ns, LLC v. FCC, 875 F.3d 1117, 1118 (D.C. Cir. 2017).
171. *Id.* at 1118 (citing Communications Act of 1934, 47 U.S.C. § 301 *et seq.* (1934)).
172. *Id.* at 1118 (citing 47 U.S.C. § 303 (2018)).
173. *Id.* at 1118 (citing 47 U.S.C. §§ 301, 307(a)–(d)).
174. *See id.* at 1119.
175. *See id.*
176. *See id*. (citing Federal Communications Commission Regulations, 47 C.F.R. § 73.3539 (2012)).
177. *See id.* at 1118 (citing 47 C.F.R. § 73.3573 (2018)).
178. *Id.* (citing 47 C.F.R. § 73.3573).
179. *Id.* (citing 47 C.F.R. § 73.3566).
180. *Id.* at 1119 (citing 47 C.F.R § 73.3573(f)(1)).
181. *Id.* (citing 47 C.F.R. § 73.3573(f)(1)).

Additionally, each radio station must meet the "minimum separation requirements for FM radio stations" provided under Section 73.207 of the FCC's regulations.[182] Every radio station has a "home on the ground (its transmitter), and on the dial (its frequency)."[183] There needs to be sufficient spacing between each station's home and dial in order to avoid any interference between stations.[184] The distance needed between a station's "transmitters on the ground corresponds inversely to the distance between their frequencies on the dial."[185] However, exemptions to Section 73.207 is provided in Section 73.213, which states that "stations operating at locations authorized prior to 1964 or 1989 are thereby 'grandfathered.'"[186] These "grandfathered" spaces "may be modified or relocated," but even a "minor modification such as a change in channel 'must' satisfy 'the minimum spacing requirements of § 73.207.'"[187]

A radio station, WBHX, ran by Press Communications ("Press") submitted an application for a minor modification on August 27, 2010.[188] Press wanted to move the transmitter for WBHX to a new location and to avoid the issue of WBHX being short spaced with another station, Press requested to switch their frequency with that of Equity's Station ("Equity"), WZBZ. Under Press's request, Press would move frequencies from 99.7 to 99.3 and Equity would move from 99.3 to 99.7.[189] Equity would keep its transmitters at the same spot, while Press would be able to "move its physical transmitters inland without short spacing itself to stations adjacent to 99.7."[190]

The FCC responded to Press's application illustrating two short spacing issues. First, if Equity's station were to move their frequency, it would create a short space with Atlantic City Board of Education station's ("Board of Education"), WAJM, frequency at 88.9.[191] In their application, Press recognized the issue of short space between Equity and the Board of Education stations.[192] However, Press argued that this issue was "moot," as the Board of Education's license expired in June 2006 and it "failed to renew its broadcast license . . . until three weeks *after* Press submitted its minor application."[193] Although the Board of Education's broadcasting license expired, "the Media Bureau recognized WAJM as an operational

182. *Id.* at 1119-20 (citing 47 C.F.R. § 73.207).

183. *Id.* at 1120.

184. *See id.*

185. *Id.* ("For example, for our purposes, the transmitters of 'first-adjacent' channels, such as 99.3 and 99.5 or 100.7 and 100.9, must be at least 113 kilometers apart; transmitters for 'second-adjacent' channels, such as 99.3 and 99.7 or 100.7 and 101.1, must have at least 69 kilometers between them. As a general matter, an application that fails to meet these spacing requirements, both on the ground and between frequencies, is said to create short spacing and is therefore defective.") (citing 47 C.F.R. § 73.207(b)(1)).

186. *Id.* (citing 47 C.F.R. § 73.213(a), (b)).

187. *Id.* at 1119 (citing 47 C.F.R. § 73.203).

188. *Id.* at 1119.

189. *See id.* at 1120.

190. *Id.*

191. *See id.*

192. *See id.*

193. *Id.* (emphasis added).

station (albeit broadcasting unlawfully) and disagreed with Press's contention that the minimum distance requirement between WZBZ and WAJM was 'moot' or otherwise immaterial."[194]

Second, Equity's frequency switch would cause the station to be short spaced to a Delaware station, WJBR, located at 99.5.[195] Currently, Equity is short spaced to WJBR, but was grandfathered in and therefore exempted from the FCC's spacing requirements.[196] Equity's frequency switch with Press would not change the spacing distance between Equity and the Delaware station nor would it change the physical location between the stations.[197] However, the Media Bureau stated that "the conventional spacing rules of Section 73.207 applied to Equity's move" causing "Equity . . . [to] not meet those minimum spacing requirements with respect to WJBR at its new location."[198] The Media Bureau also stated the failure of Press "to cite any precedent for proposing an *involuntary* channel substitution to a grandfathered short-spaced station."[199]

The Media Bureau provided Press with thirty days to correct the two short spacing issues that accompanied their application and explained that any failure to complete the changes would result in a dismissal of their application.[200] Press did not make any corrective changes "insisting that its initial application was not defective because it 'would not result in any unacceptable channel separations'" nor did Press request a "waiver of the spacing rules."[201] Therefore, in an FCC order that granted the Board of Education's license renewal, the Media Bureau dismissed Press's modification application.[202] In response to the dismissal, Press submitted to the full Commission an application for review of the Media Bureau decision.[203] The Commission "denied the application" and Press followed with an appeal to the District of Columbia Circuit Court.[204]

II. ANALYSIS

In a request to reverse the FCC's decision to dismiss Press's minor modification application, Press provided two arguments and Press had to prevail on both arguments for the court to set aside the Commission's order.[205]

194. *Id.*
195. *See id.*
196. *See id.*
197. *See id.*
198. *Id.*
199. *Id.*
200. *See id.*
201. *Id.*
202. *See id.*
203. *See id.* at 1121.
204. *See id.* (citing In re Applications of Atl. City Bd. of Educ. & Press Commc'ns, LLC, 30 FCC Rcd. 10583 (2015)).
205. *See id.*

The first issue presented before the Court was whether the spacing between Equity and the Delaware station remained "grandfathered" in.[206] Press stated that under 47 C.F.R. § 73.213, a "transfer of a grandfathered short spaced station is permitted" making the short spacing between Equity and the Delaware station acceptable.[207] Press relied on Section 73.213(b), which states that modifications may be made to "[s]tations at locations authorized prior to May 17, 1989, that did not meet the . . . separation distances required by § 73.207 and have remained short-spaced since that time"[208] However, the FCC's regulation does not mandate an issuance of a modification application that places an "involuntary relocation on a third party, nor does it grandfather that third party's short spacing in the absence of a request to waive the short spacing prohibition."[209] Furthermore, the Court relied on the plain language of Section 73.203 that expressed "that a short spaced station grandfathered under the rule is not necessarily permitted to rely on its prior grandfathering when it transfers channels."[210] In addition, the Court found that the FCC followed customary practices when enforcing short spacing rules on Press's application.

Second, Press argued that since the Board of Education applied for a renewal after their license had already expired, "the FCC was required to give Press the benefit of the cut-off rule and deny WAJM's subsequent, late-filed renewal application."[211] Due to the Court's holding that a short spacing issue between Equity and the Delaware station existed, the Court does not go into detail regarding this second argument. The Court did provide that "the Media Bureau . . . adopted a new policy for processing license renewal applications that makes lapses like the Board of Education's less likely to recur."[212]

III. CONCLUSION

The United States Court of Appeals for the District of Columbia affirmed the FCC's order dismissing Press's minor modification application because the channel switch with Equity violated the spacing requirements.

206. *See id.*
207. *Id.*
208. *Id.* at 1122 (citing 47 C.F.R. § 73.213(b)).
209. *Id.* (citing 47 C.F.R. § 73.213(b)).
210. *Id.* (citing 47 C.F.R. § 73.203).
211. *Id.* at 1124.
212. *Id.* (citing 31 FCC Rcd. at 9384 n.30)

SNR Wireless License Co, LLC v. Federal Communications Commission

Tess Macapinlac

868 F.3D 1021 (D.C. CIR. 2017)

In *SNR Wireless LicenseCo, LLC v. FCC*[213], the District of Columbia Circuit Court of Appeals held that the FCC had reasonably applied precedent when considering whether or not DISH had a disqualifying degree of *de facto* control over SNR Wireless LicenseCo (SNR) and Northstar Wireless, LLC (Northstar).[214] However, the Court also held that the Commission did not give SNR and Northstar sufficient notice regarding the possibility that if their relationships with DISH cost them their bidding credits, the FCC would also deny them the opportunity to get discounted [?].[215] The Court then remanded the case to the FCC in order to give SNR and Northstar the chance negotiate a cure for the control that DISH has over them.[216]

I. BACKGROUND

Under the Communications Act of 1934 (the Act), the Federal Communications Commission (FCC) has the ability to grant licenses to private companies for the use of the electromagnetic spectrum.[217] This spectrum consists of "the electromagnetic radio frequencies used to transmit sound, data, and video across the country"[218] and can be used by private companies to provide television, cellphone, and wireless internet services to consumers.[219] In 1993, Congress gave the FCC the power to award licenses through auctions.[220] FCC regulations allow the Commission to give "bidding credits," or discounts, to designated entities, including small businesses, to cover part of the cost of licenses that these entities may win.[221]

213. 868 F.3d 1021 (D.C. Cir. 2017).
214. *Id.* at 1025.
215. *Id.*
216. *Id.*
217. *Id.* (citing 47 U.S.C. §§ 307, 309 (2004)).
218. *Id.* (quoting FCC, *About the Spectrum Dashboard*, http://reboot.fcc.gov/reform/systems/spectrum-dashboard/about (*About the Spectrum*)).
219. *Id.*
220. *Id.* at 1025-26 (citing Omnibus Budget Reconciliation Act of 1993, Pub. L. No. 103-66, 107 Stat. 312).
221. *Id.* at 1026 (citing 47 C.F.R. § 1.2110(a), (f) (2012)).

This case began with Auction 97, announced by the FCC on May 19, 2014 and held on July 23, 2014.[222] The Notice for the Auction (Notice) explained that small businesses were eligible for bidding credits in this auction, with the size of the bidding credits depending on the entities' "attributable" revenue over the preceding three years.[223] Entities that had less than $40 million in attributable revenue got a fifteen percent discount on the license price, while entities with less than $15 million in attributable revenue got a twenty-five percent discount.[224]

Notably, attributable revenue of an entity included the revenues of both the small business itself and any other entity with *de facto* control over the small business. While the FCC does not set a clear line between acceptable influence and *de facto* control, in the past, the FCC has considered factors such as the authority of someone other than the small business to determine the nature, types, or prices of services offered, as well as control over appointments to the board, and general involvement in management decisions.[225] In the Notice in question, the FCC directed entities to examine the Commission's earlier decisions regarding the definition of designated entities, and pointed to the context dependent definition of *de facto* control on which the Commission had long relied.[226]

To verify the entities' qualifications for bidding credits, prior to the auction, each entity filled out a short form listing its attributable revenue, under punishment of perjury.[227] After the auction concluded, each entity that successfully obtained a license filled out a long, more comprehensive form that would be reviewed by the FCC to ensure eligibility for bidding credits.

SNR Wireless LicenseCo, LLC ("SNR") was formed two weeks before the application deadline for this auction, while Northstar Wireless, LLC ("Northstar") was formed eight days before the application deadline.[228] Neither company had officers, directors, or revenue, and both claimed they qualified for the twenty-five percent discount on licenses.[229] Both companies also disclosed on their short applications that their capital for the auction came from DISH, in exchange for an indirect eighty-five percent ownership interest of each company, a position as operations manager at both entities, and adopted various joint bidding protocols and agreements with each entity.[230]

Both SNR and Northstar had successful bids at the auction, gaining 43.5% of the licenses available.[231] With the designated twenty-five percent discount, SNR and Northstar together would save a little over $3 billion

222. *Id.*

223. *Id.* (citing Auction of Advanced Wireless Servs. (Aws-3) Licenses Scheduled for Nov. 13, 2014, 29 FCC Rcd. 8386, 8411-12 (2014)).

224. *Id.* (citing 29 FCC Rcd. 8386, 8411-12 (2014)).

225. *Id.* (citing 47 C.F.R. § 1.2110(c)(2) (2018)).

226. *Id.* at 1026-27 (citing 29 FCC Rcd. at 8411).

227. *Id.* at 1027 (citing 29 FCC Rcd. at 8407).

228. *Id.*

229. *Id.* (In re Northstar Wireless, LLC, 30 FCC Rcd. 8887, 8893 (2015)).

230. *Id.*

231. *Id.* at 1027-28.

dollars.[232] SNR and Northstar then filled out the longer, more thorough applications required by the FCC.[233] Once these applications became public, eight parties, including less successful auction competitors and other parties, petitioned the FCC to deny the bidding credits to SNR and Northstar, since both were essentially controlled by DISH, a large business.[234]

The FCC dismissed six petitions and considered the two petitions from a.235The FCC held that DISH revenue was attributable to both SNR and Northstar, so neither SNR nor Northstar were eligible to keep the bidding credits.236concluded that both SNR and Northstar could keep the licenses if they were able to pay full price for them.237SNR and Northstar chose to pay for some licenses at full price and defaulted on others.238 bids and the eventual price of the license after re-auction.239The companies also had to pay fifteen percent of either the original bid or the eventual price of the license, whichever was lower.240

II. ANALYSIS

The petitioners, SNR and Northstar, claimed that the FCC departed from precedent without reasoning regarding *de facto* control, and that even if the FCC had kept with precedent, the Commission did not provide fair notice that the petitioner's relationship with DISH could cost them bidding credits and implement a penalty.[241] The court started with the claim that the FCC had departed from precedent without reasoning.[242] The court noted that their review was narrow and only meant to ensure that the FCC had a "satisfactory explanation" for its action.[243]

The court first focused on the six-factor *de facto* control test presented in *Intermountain Microwave*,[244] which discusses factors that examine whether one entity has control over another entity.[245] The factors are "(1) who controls the daily operations of the business, (2) who employs, supervises, and dismisses the small business's employees; (3) whether the small business has "unfettered" use of all its facilities and equipment; (4) who covers the small business's expenses, including its operating costs; (5) who receives the small business's revenues and profits; and (6) who makes

232. *Id.* at 1028.
233. *Id.*
234. *Id.*
235. *Id.* (30 FCC Rcd. at 8904-05).
236. *Id.* (citing 30 FCC Rcd. at 8940-48).
237. *Id.*
238. *Id.*
239. *Id.* at 1029 (citing 30 FCC Rcd. at 8950-51).
240. *Id.* (citing 30 FCC Rcd. at 8950-51; 47 C.F.R. § 1.2104(g)(2)(ii
241. *Id.*
242. *Id.*
243. *Id.* (citing *Motor Vehicle Mfrs. Ass'n, Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983)) (internal quotations omitted).
244. Nonbroadcast and General Action Report No. 1142, 12 FCC 2d 559 (1963) [hereinafter *Intermountain Microwave*].
245. 868 F.3d 1021 at 1030.

and carries out the policy decisions of the small business."[246] The FCC found that DISH, through "the substance of the terms of DISH's control,"[247] had *de facto* control over both SNR and Northstar.[248] The Court found that the FCC had applied the test in similar ways in other FCC cases, and so the Commission's conclusion that DISH had *de facto* control over the petitioners was appropriate and consistent with earlier law.[249]

The FCC also considered the case of the petitioners under the *Fifth Memorandum Opinion & Order* ("Fifth MO&O")[250], which sought to ensure that only small businesses that participate in the wireless industry receive benefits, rather than small businesses that are proxies for or will soon become subsidiaries of larger businesses.[251] *Fifth MO&O* explained that when an investor uses finances to force a small company into a sale, then the investor effectively takes control of the small company.[252] The FCC found that DISH placed severe restrictions on SNR and Northstar, leaving the two companies with few options to avoid financial failure, and the Commission used *Fifth MO&O* as further evidence to support the conclusion of DISH's *de facto* control over the petitioners.[253] The Court found the FCC properly applied *Fifth MO&O* to strongly support the FCC's conclusion that DISH had *de facto* control over the petitioners.[254]

The petitioners pointed to two auction bids authorized by the Wireless Bureau as precedent that the FCC departed from without reason.[255] Over ten years ago, the Wireless Bureau granted a small company called Denali Spectrum bidding credits without opinion.[256] However, Cricket Communications and its affiliates provided Denali Spectrum with the capital needed to participate in the auction, in exchange for an eighty-five percent interest in Denali Spectrum and a position as Denali Spectrum's manager.[257] Similarly, the Wireless Bureau granted another small company, Salmon PCS, bidding credits without explanation, though Cingular Wireless had an eighty-five percent interest in Salmon and the ability to weigh in on Salmon's business decisions.[258] The petitioners claimed their agreements with DISH mirrored many agreements that were present in the Denali and Salmon agreements, and so the FCC departed from existing precedent when it determined that DISH had *de facto* control over the petitioners.[259]

246. *Id.* at 1031 (citing 12 FCC. 2d at 560).
247. *Id.* at 1033.
248. *See id.* at 1031-33.
249. *Id.* at 1033
250. Fifth Memorandum Opinion & Order, 30 FCC Rcd. 403 (1994) [hereinafter *Fifth MO&O*].
251. 868 F.3d at 1034.
252. *Id.*
253. *Id.*
254. *Id.* at 1035.
255. *Id.*
256. *Id.* at 1036.
257. *Id.*
258. *Id.*
259. *Id.* at 1036-37.

The Court noted that the FCC is not bound to treat the Denali and Salmon agreements as binding precedent from which the FCC cannot deviate without reasonable explanation.[260] Additionally, the Court held in *Comcast v. FCC*[261] that a "lower component of a government agency"[262] does not bind the agency as a whole, unless the agency has endorsed those actions.[263] Thus, the Wireless Bureau's approval of the Denali and Salmon bidding credits does not force the Commission to follow in a similar way, and the Commission does not have to explain deviations from those decisions.[264]

Petitioners argued that because the Wireless Bureau exercises powers delegated by the Commission, and those powers have the same effect as actions coming from the Commission, the Bureau's decisions should be considered the Commission's decisions.[265] However, the court held that this similarity does not mean that rules implied from case-specific actions can be interpreted as the position of the Commission.[266] The petitioners then pointed to 47 C.F.R. § 0.445 (2012), which provides that when staff, using powers delegated by the FCC, does not publish opinions or orders, those opinions or orders can be used as precedent against the Commission.[267] By this reasoning, the petitioners claimed that the unpublished orders by the Wireless Bureau can be used as precedent against the Commission.[268] The Court did not agree with this point of reasoning, noting that the purpose of Section 0.445 was to prevent parties from using documents against another party, such as the Commission, when the latter party has no notice of the document.[269]

The petitioners then differentiated their case from the *Comcast* case, stating that while *Comcast* referenced "sporadic action" by the Media Bureau that the FCC did not review or endorse, the case at hand dealt with the Wireless Bureau, which the FCC has referred to in order to state the Commission's position.[270] The Court did not find this persuasive, as the Denali and Salmon decisions were "sporadic" actions that were not reviewed or endorsed by the FCC.[271] The petitioners next claimed that the FCC had an obligation to follow Wireless Bureau precedent because the Auction Notice pointed participants to Bureau precedent for guidance on the issue of control.[272] The Court pointed out no reasonable participant could

260. *Id.* at 1037.
261. Comcast Corp. v. FCC, 526 F.3d 763 (D.C. Cir. 2008).
262. *Id.* at 769.
263. 868 F.3d at 1037.
264. *Id.*
265. *Id.*
266. *Id.*
267. *Id.* (quoting 47 C.F.R. § 0.445(a) (2018)).
268. *Id.* at 1038.
269. *Id.*
270. *Id.* at 1037-38.
271. *Id.*
272. *Id.*

read those references to mean that the every principle from a past Wireless Bureau action represented the position of the Commission.[273]

Next, the petitioners pointed to a footnote in their case where the FCC disavowed the actions of the Wireless Bureau staff, claiming that this footnote implies that without that disavowal, the actions would be considered full Commission acts.[274] However, the Court notes that the disavowal was meant to foreclose inconsistencies that could be implied from past actions, and did not carry the implication that the petitioners claimed.[275] The petitioners also claimed that since *Intermountain Microwave* and *Fifth MO&O* do not provide clear guidance regarding *de facto* control, the FCC intended for auction participants to look at specific application forms and successful agreements, like the Denali and Salmon agreements, for clear guidance.[276] The court noted that the petitioners did not cite to a case where such a situation has occurred, and held that the Commission was free to determine qualifications for bidding credits based on the facts at hand.[277]

The Court also held that even if the Denali and Salmon agreements were held as precedent, the two agreements are materially different from the cases of SNR and Northstar.[278] The Court noted that both SNR and Northstar would be forced to sell to DISH, rather than scramble to build a nationwide network over the course of five years in order to repay their multibillion dollar loans.[279] Denali and Salmon's agreements with their respective investors differed from that of the petitioners in that Denali and Salmon had more control and ability to build their networks and collect revenue before payments on the loans were due.[280]

Additionally, the court observed that during the auction, SNR and Northstar seemed to coordinate bids in a way that was detrimental to each company individually, but when examined as though the companies were "acting as two arms of DISH," the bid coordination made economic sense.[281] The petitioners argued that this did not violate any FCC bidding rules.[282] The Court instead pointed to this as another indicator of DISH's *de facto* control over the petitioners.[283] The Court held that the FCC had acted reasonably and consistently with Wireless Bureau decisions when deciding the issue of DISH's *de facto* control over the petitioners.[284]

The petitioners lastly argued that the Chairman of the FCC told Congress that in resolving this case, the FCC applied new rules developed after Auction 97, and claimed that it was unfair that they would be held to

273. *Id.* at 1038.
274. *Id.*
275. *Id.* at 1039.
276. *Id.*
277. *Id.*
278. *Id.* at 1040.
279. *Id.*
280. *Id.* at 1040-41.
281. *Id.* at 1041-42.
282. *Id.* at 1042.
283. *Id.*
284. *Id.*

rules that did not exist at the time of the auction.[285] However, the court found that the Chairman's statement was not an admission that the Commission was applying new rules to the petitioners, and points out that all rules and precedent from the FCC's order pre-dated the auction. [286]

However, the court noted that the petitioners could only be sanctioned by the FCC if they had fair notice, or notice that allowed the petitioners to "identify, with reasonable certainty, the standards with which the agency expect[ed] [them] to conform."[287] The court agreed with the FCC that there was sufficient notice regarding the possibility that DISH may have had *de facto* control, and that that control would prevent petitioners from qualifying for bidding credits.[288] However, the court also held that the FCC did not give sufficient notice that this degree of *de facto* control would prevent petitioners from the chance to seek to negotiate a cure with the FCC.[289]

The FCC argued that the *Intermountain Microwave* test should have shown the petitioners that their understanding was far from compliant with FCC rules.[290] However, the court noted that this was not enough to show that petitioners were given fair notice that they would not have the chance to cure.[291] The court noted that in *In re Application of ClearComm, L.P.,*[292] the FCC allowed a petition for consideration regarding a company's *de facto* control over an entity with questionable designated-entity status.[293] The court analogized the petitioners' case to *ClearComm*, where the companies in question wanted to be eligible for bidding credits, and all companies failed, making the petitioners' case for the chance to cure even stronger.[294]

While the FCC expressed concerns that offering the chance to cure would stop companies from attempting to comply with designated-entity rules before the auction, the court pointed out that there is no requirement for the FCC to cure.[295] The court held that the Commission, however, must give reasonable notice that an entity may not have an opportunity to cure.[296]

III. CONCLUSION

The Court remanded the case back to the FCC in order give petitioners the chance to renegotiate their agreements with DISH. [297]

285. *Id.*
286. *Id.* at 1043.
287. *Id.* (quoting Trinity Broad., Inc. v. FCC, 211 F.3d 618, 628 (D.C. Cir. 2000)).
288. *Id.*
289. *Id.*
290. *Id.* at 1045.
291. *Id.*
292. In re Application of ClearComm, L.P., 16 FCC Rcd. 18627 (2001).
293. 868 F.3d 1021 at 1045.
294. *Id.* at 1046.
295. *Id.*
296. *Id.*
297. *Id.*

United States v. Thompson

Senrui Du

866 F.3D 1149 (10TH CIR. 2017)

In *United States v. Thompson*,[298] the United States Court of Appeals for the Tenth Circuit affirmed the District Court's decision to grant the government's application for orders requesting Thompson's historical cell-service location information (CSLI) and admitting some of that CSLI evidence at a pretrial proceeding.[299] The Court held that cell phone users lacked a reasonable expectation of privacy in their historical CSLI, which users voluntarily conveyed to third-party cell-service providers.[300]

I. BACKGROUND

Thompson was arrested after an investigation into a drug-trafficking operation.[301] Agents gathered evidence through a confidential informant; monitoring telephones used by certain of the co-conspirators; and conducting searches of Thompson's residence.[302] Before trial in the district court, Judge Platt, a state court judge sitting in the Eighth Judicial District of Kansas, had issued wiretap orders for target phones used by Thompson and his co-conspirators.[303] Based in part on information derived from intercepts conducted pursuant to the wiretap orders, law enforcement applied for search warrants of Thompson's residence.[304] Officers seized cell phones, cash, miscellaneous documents, drug paraphernalia, and credit cards at Thompson's residence.[305]

Thompson filed a motion to suppress the intercepted calls, "arguing law enforcement had intercepted his communications outside the territorial jurisdiction of the Eighth Judicial District."[306] The government filed an application for orders pursuant to § 2703(d) of the Stored Communications Act (SCA), asking the court to require the electronic service providers for Thompson and his co-conspirators to disclose historical CSLI for their phones.[307] The District Court granted the government's application.[308]

298. United States v. Thompson, 886 F.3d 1149 (10th Cir. 2017).
299. *Id.* at 1160.
300. *Id.*
301. *Id.* at 1151.
302. *Id.*
303. *Id.* at 1152.
304. *Id.*
305. *Id.* at 1152-53.
306. *Id.* at 1153.
307. *Id.*
308. *Id.*

"After obtaining the CSLI, the government sought to establish the location of the intercepted phone calls by showing that a call had 'pinged' certain cell towers in and around the Junction City area within the Eighth Judicial District."[309] "At a pretrial evidentiary hearing, the government presented the CSLI and testimony from two experts who agreed that if the CSLI showed a phone connected to one of the Junction City towers, then it was highly likely the phone was physically located in the Eighth Judicial District."[310] The District Court found the government's evidence sufficient.[311] The court, therefore, admitted calls that had pinged on one of the towers.[312]

In the instant case, Thompson contended that § 2703(d) was unconstitutional, because cell phone users had a reasonable expectation of privacy in their historical CSLI.[313] And because collecting CSLI constituted a search, Thompson argued, the Fourth Amendment required the government to procure a warrant before obtaining a cell phone user's historical CSLI.[314]

II. ANALYSIS

The Court first reviewed Thompson's challenge to the constitutionality of § 2703(d).[315] Since 1967, the Supreme Court has recognized a privacy-based approach to the Fourth Amendment.[316] Under that approach, a court asks: "(1) whether the individual asserting an expectation of privacy exhibited an actual (subjective) expectation of privacy; and (2) whether that expectation 'is one that society is prepared to recognize as reasonable.'"[317] Where an expectation of privacy satisfies both requirements, government invasion of that expectation is generally a search.[318]

The Supreme Court analyzed the constitutionality of § 2703(d) in a pair of cases dealing with business records created by a third party.[319] In *United States v. Miller*,[320] the Supreme Court held the defendant did not have a legitimate expectation of privacy in the subpoenaed bank records, reasoning the records were business records of the banks and related to transactions to which the bank was a party.[321] The Supreme Court explained that the Fourth Amendment does not forbid "the obtaining of information revealed to a third party and conveyed by [that third party] to Government authorities, even if the information is revealed on the assumption that it will

309. *Id.*
310. *Id.*
311. *See id.*
312. *Id.*
313. *Id.* at 1152.
314. *Id.*
315. *Id.* at 1154.
316. *Id.*
317. *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).
318. *Id.*
319. *Id.* at 1155.
320. 425 U.S. 435 (1976).
321. 886 F.3d at 1156 (citing *Miller*, 425 U.S. at 440-41).

be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[322]

Several years later, in *Smith v. Maryland*,[323] the Supreme Court held the third-party doctrine applied to the warrantless installation of a pen register used to record telephone numbers dialed from the defendant's home.[324] The Court reasoned that telephone users typically know that they must convey numerical information to the phone company; that the phone company had facilities for recording this information; and that the phone company did in fact record this information for a variety of legitimate business purposes.[325] Because the defendant voluntarily turned over his numerical information to a third-party phone company, he lacked a legitimate expectation of privacy in that information.[326]

Here, the court noted that it was third-party cell service providers who created CSLI records for their own business purposes.[327] Under the same rationale the Supreme Court articulated in *Miller* and *Smith*, cell phone users voluntarily turned over their CSLI to service providers, thus relinquishing any reasonable expectation of privacy.[328] Any cell phone user must know that her phone exposed its location to the nearest cell tower by seeing the phone's strength fluctuate.[329] The court held that "[e]ven if this cell phone-to-tower transmission was not common knowledge, cell phone service providers' and subscribers' contractual terms of service and providers' privacy policies expressly state[d] that a provider uses a subscriber's location information to route his cell phone calls."[330] These documents also informed subscribers that the providers not only used the information, but collected it and would turn over these records to government officials if served with a court order.[331]

Thompson contended that the third-party doctrine has no application here, because that doctrine presumed a voluntary relinquishment of information and individuals did not voluntarily disclose their CSLI to service providers.[332] The court disagreed, stating that users voluntarily entered arrangements with service providers knowing that they "'must maintain proximity to the provider's cell towers' in order for their phones to function."[333] Furthermore, the court held that "like the phone numbers recorded by the pen register in *Smith*, CSLI [wa]s not a record of conversations between individuals, but rather a record of the transmission of

322. *Id.* (quoting *Miller*, 425 U.S. at 443) (internal quotations omitted).
323. 442 U.S. 735 (1979).
324. 886 F.3d at 1156 (citing *Smith*, 442 U.S. at 743-46).
325. *Id.* (citing *Smith*, 442 U.S. at 743).
326. *Id.* (citing *Smith*, 442 U.S. at 743-44).
327. *Id.*
328. *Id.* at 1157.
329. *Id.* (citing United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016)).
330. *Id.* (citing In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) (internal quotations omitted).
331. *Id.* (citing *In re Application of the United States for Historical Cell Site Data,* 724 F.3d at 613).
332. *Id.*
333. *Id.* (quoting United States v. Graham, 824 F.3d 421, 430 (4th Cir. 2016) (en banc)).

data that occur[red] to facilitate those conversations."[334] Thus, the court found, CSLI was not protected by the Fourth Amendment.[335]

Finally, Thompson relied on Justice Sotomayor's concurrence in *United States v. Jones* to argue that societal expectations of privacy have changed.[336] Thompson cited Justice Sotomayor's statement that an individual should have reasonable expectation of privacy in information voluntarily disclosed to third parties.[337] The court rejected Thompson's argument, explaining that Justice Sotomayor's concurrence was not the opinion of the Supreme Court.[338] The court held that until a majority of justices on the Supreme Court decides otherwise, courts are "still bound by the third-party doctrine."[339]

III. CONCLUSION

The United States Court of Appeals for the Tenth Circuit concluded that cell phone users lack a reasonable expectation of privacy in their historical CSLI, because users voluntarily convey their CSLI information to third-party cell-service providers.[340]

334. *Id.* at 1158.
335. *Id.*
336. *Id.*
337. *See id.*
338. *Id.* at 1159.
339. *Id.*
340. *Id.* at 1160.