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.