ORGANIZATIONAL DOXING: DISASTER ON THE DOORSTEP

COLIN J.A. OLDBERG*

Many organizations store massive amounts of personally identifiable information (PII) in large databanks on the Internet. In recent years, the number of hacks suffered by organizations has increased dramatically, from 157 in 2005 to nearly 800 in 2014. Using a process called doxing, hackers typically target vulnerable PII, and then publish that PII online. This note examines the devastating harm that doxing causes and argues that effective action must be taken. Ultimately, this note concludes that a system of strict liability—whereby organizations would be held liable for any harm caused when PII in their possession escapes—would most effectively prevent doxing harms. Alternatively, state information privacy statutes could become a viable method of preventing doxing harms.

* Colin J.A. Oldberg, M.M. & B.M., Northwestern University Bienen School of Music, is a J.D. Candidate for 2017 at the University of Colorado Law School. He interned in the Telecommunications Policy Division at Common Cause (Washington, D.C.), where he developed a passion for telecommunications law and policy. He also helped his team win the National Telecommunications Law Moot Court Competition in 2016 (Washington, D.C.). He will be clerking for the Honorable Anthony Navarro of the Colorado Court of Appeals after graduation. He wishes to thank the many brilliant people who helped make this note possible, including Blake Reid, Esq., Paul Ohm, Esq., Dan Carlin, Anna Adams, Eric A. Spaulding, John E. Oldberg, and the incredible team at the Colorado Technology Law Journal. Colin continues to perform as a trumpeter and would like to thank the wonderful musicians who made his journey to law school possible, including Barbara Butler, Charlie Geyer, Dr. Ryan T. Nelson, and Dr. Mallory Thompson.

INTRODUCTION

Current statutory and common law regimes do not effectively protect consumer data from individuals and entities with nefarious purposes (such as hackers) who wish to distribute private, potentially embarrassing data over the Internet. Doxing, sometimes spelled 'doxxing,' is the process of using the Internet to research and publish specific information about individuals, usually called personally identifiable information (PII).[1] Companies and organizations that deal with PII on a regular basis often do not have policies or systems in place that adequately protect consumers from the specific dangers of doxing at the organizational level. Recent examples of organizational doxing include the Edward Snowden revelations, the Ashley Madison affair website hack, and the alleged North Korean hack of Sony.

The first section of this note outlines the very real dangers that organizational doxing poses and the modern harms that victims suffer from doxing. The second section examines five frameworks that have developed in the United States to combat the threats of doxing: (1) federal legislation; (2) federal agency action; (3) state legislation; (4) negligence suits; and (5) strict

1. *See* Mat Honan, *What Is Doxing?*, WIRED (Mar. 6, 2014, 1:03 PM), http://www.wired.com/2014/03/doxing/ [https://perma.cc/62AD-TDYL]; *see also* RONEY MATHEWS, SHAUN AGHILI, & DALE LINDSKOG, A STUDY OF DOXING, ITS SECURITY IMPLICATIONS AND MITIGATION STRATEGIES FOR ORGANIZATIONS 1 (last visited Nov. 13, 2016), http://infosec.concordia.ab.ca/files/2013/02/Roney_Mathews.pdf [https://perma.cc/KD5J-YUJB]; *see generally* David M. Douglas, *Doxing: A Conceptual Analysis*, ETHICS AND INFO. TECH., Sept. 2016, at 199, 200.

liability. The final section analyzes each framework to determine its effectiveness in combating organizational doxing. Currently, none of these frameworks effectively prevents the doxing problem, but state legislation is making the largest strides in protecting consumer data. Ultimately, strict liability would serve as the best response to doxing threats, though its implementation in the United States is unlikely to occur anytime soon.[2]

BACKGROUND

"Doxing," in its modern form, is the process of using the Internet to research and publish (without authorization) an individual's PII.[3] Evolving from 1990s hacker culture, where an angry computer user might "drop dox" on someone for revenge, the modern term still carries a negative connotation.[4] The process has made its way into the public sphere, and today it is unfortunately all too familiar. For example, in the last two years the amount of stolen data published on the Internet is staggering, and the most famous "dumps," such as those released by Edward Snowden, the Sony hackers, and the Ashley Madison hackers, have become household names. Doxing has grown from a seldom-used revenge tactic into a recurring nightmare for individuals, governments, and organizations. Given the massive amount of PII that organizations routinely collect, organizations are particularly vulnerable to doxes, so much so that an entirely new term has been born: "organizational doxing."

Organizational doxing is the process of hacking into an organization's network, obtaining PII about the organization's customers and employees, and publishing it on the Internet.[5] In recent years, this activity increased dramatically.[6] In 2013,

2. The author recognizes that doxing harms are not unique to the United States, but international organizational doxing is beyond the scope of this article.

3. *See* Honan, *supra* note 1; *see also Rules and Policies - Protecting PII - Privacy Act*, U.S. GEN. SERVS. ADMIN., http://www.gsa.gov/portal/content/104256 [https://perma.cc/2CXQ-N5JV] (last visited Oct. 26, 2016) ("The Office of Management and Budget (OMB) defines personally identifiable information as: 'information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.'").

4. U.S. GEN. SERVS. ADMIN., *supra* note 3; *see also* Megan Garber, *Doxing: An Etymology*, THE ATLANTIC (Mar. 6, 2014), http://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/ [https://perma.cc/S3BD-9ZZE] ("'Doxing' derives . . . from the word 'docs' [short for documents]. It refers to the fact that, often, it is documents (public or not) that lead to a formerly anonymous person's identity being revealed.") Thus, to "drop dox" means to publish someone's documents on the Internet.

5. Bruce Schneier, *Organizational Doxing*, SCHNEIER ON SECURITY (July 10, 2015, 4:32 AM), https://www.schneier.com/blog/archives/2015/07/organizational_.html [https://perma.cc/ESN9-W9WQ].

6. *See id.*

Edward Snowden stole a huge number of documents from the United States government, many of which implicated the National Security Agency (NSA) in illegal spying.[7] The United States government is still reeling from the revelations, and reporters are still sifting through the mountain of data released.[8] In 2014, the North Korean government allegedly hacked Sony in response to a movie that the entertainment giant released poking fun at Kim Jong-un, the nation's leader.[9] The hackers published many documents on the Internet,[10] some of which included troubling data indicating that Sony paid its top female executives considerably less than their male counterparts.[11] Last year, hackers gained access to Ashley Madison, the website that (supposedly) anonymously linked people interested in cheating on their spouses with other like-minded individuals.[12] Hackers released a massive list of users and credit card transactions, which led to many ruined marriages and even several suicides.[13]

Although the individual harms resulting from organizational doxing are significant, it is possible that organizations' overall levels of transparency are increasing in light of the obvious vulnerabilities that their networks face.[14] For example, perhaps Sony would have paid its male and female employees equally knowing that the practice would be revealed for everyone to see.[15] Perhaps the NSA would have modified its surveillance practices had the agency known that the program would face public

7. *See, e.g.*, *id.*; *see also* Glenn Greenwald, et. al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/8SPJ-7DZJ]. Notably, this particular dox occurred via a credible news source and not by traditional hacker methods. Snowden contacted reporter Glenn Greenwald and supplied him with thousands of classified documents, and Greenwald revealed the information via The Guardian.

8. Catalin Cimpanu, *Snowden Documents to be Released in Full After Panama Papers Success,* SOFTPEDIA (May 16, 2016, 10:45 PM), http://news.softpedia.com/news/snowden-documents-to-be-released-in-full-after-panama-papers-success-504134.shtml [https://perma.cc/GM43-BW4U].

9. *See* Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Jan. 5, 2015, 12:36 PM), http://usat.ly/1AMohtO [https://perma.cc/NY8Q-YJTM]. North Korea still publically denies any involvement in this hack.

10. *See, e.g.*, David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ [https://perma.cc/T7BR-BKFT].

11. *Id.*

12. Schneier, *supra* note 5.

13. *Id.*; *see, e.g.*, Alex Cramer, *Ashley Madison Suicide? Married Baptist Teacher Exposed by Hack Takes Own Life*, HOLLYWOOD LIFE (Sept. 9, 2015, 10:19 PM), http://hollywoodlife.com/2015/09/09/ashley-madison-suicide-married-baptist-pastor-john-gibson/ [https://perma.cc/S9D3-WV7A].

14. Schneier, *supra* note 5.

15. *See, e.g.*, Juliet Lapidos, *The Sony Hack and the Gender Pay Gap*, N.Y. TIMES: TAKING NOTE (Jan. 12, 2015 11:33 AM), http://nyti.ms/1y4uQcY [https://perma.cc/B5UJ-MYB7].

scrutiny.[16] Perhaps these would be good results. After all, the government and the corporations entrusted with sensitive data should operate with a high level of transparency; that is, individuals should generally know what government agencies and corporations are doing with PII.[17]

But at what cost? Individuals trust corporations to keep data safe. Users of the Ashley Madison website used the site under the impression that it was completely anonymous. Many users paid an extra fee for the "full delete" button, a service that would wipe out any trace of their involvement with the site.[18] Unfortunately, the dox revealed that the site was not fully anonymous, and the full delete button to be little more than a sham. Because of security vulnerabilities, people committed suicide, and countless lives were ruined.[19] Not surprisingly, many lawsuits arose from the incident.[20]

Individuals trust the government to keep data safe, and ironically, the Snowden dox revealed that the government was doing the opposite: illegally spying on Americans and collecting "private" data.[21] Although these particular revelations seem to cut the other way, the government should operate with some level of nondisclosure.[22] State Department officials need to be able to criticize foreign leaders without fear of immediate leakage because disclosure could result in homeland security disasters.[23] Emails or memoranda drafted, but never actually sent, should not be revealed and used against elected officials and corporate executives because these authors should be allowed the flexibility to change their minds in order to reach better decisions. Executive officials and members of the judiciary should be allowed the

16. Schneier, *supra* note 5.

17. *See id.*

18. Joseph Bernstein, *Ashley Madison's $19 "Full Delete" Option Made the Company Millions,* BUZZFEED (Aug. 19, 2015, 11:56 AM), https://www.buzzfeed.com/josephbernstein/leaked-documents-suggest-ashley-madison-made-millions-promis?bftwnews&utm_term=.upjVBdeJb#.nyvo64a5E [https://perma.cc/Z72G-BS2A].

19. *See, e.g.*, Kristen V. Brown, *Recapping the Aftermath of the Ashley Madison Hack: Suicide, Fembots, Cracked Passwords and More*, FUSION (Sept. 10, 2015, 3:19 PM), http://fusion.net/story/195787/whats-going-on-with-ashley-madison/ [https://perma.cc/S4TR-UMVC].

20. *Id.*; *see also Ashley Madison Privacy Breach*, SUTTS STROSBERG, https://www.strosbergco.com/class-actions/ashleymadison/ [https://perma.cc/243Z-47WZ] (last visited October 25, 2016) ("On August 20, 2015, Sutts, Strosberg LLP and Charney Lawyers commenced a proposed national class action in the Ontario Superior Court of Justice against Avid Life Media Inc. and Avid Life Dating Inc., who own and operate Ashley Madison. The action seeks damages for breach of contract, breach of consumer protection statutes, negligence, intrusion upon seclusion, breach of privacy and publicity given to private life for Ashley Madison customers whose personal information was publically disclosed on August 18, 2015.").

21. Greenwald, *supra* note 7.

22. Schneier, *supra* note 5.

23. *Id.*

discretion to discuss their opinions in closed circles before announcing decisions to the public to increase the probability that they make well-informed, thoughtful decisions.[24]

In sum, the organizations entrusted with PII have a duty in the modern world to keep that data private, and sometimes need to operate with a certain level of nondisclosure in order to better serve the public and their shareholders. But right now, organizations are not doing enough to keep data safe from the potential threats of organizational doxing. These threats far outweigh any potential advantages gained by dox-induced organizational transparency,[25] as the following examples demonstrate.

I. ORGANIZATIONAL DOXING IS A MENACE TO SOCIETY.

Doxing harms are very real and potentially life altering.[26] Almost every business maintains a digital database containing user information and sensitive data such as screen names, email addresses, and other biographical information.[27] Advances in computer processing speed and data-storage efficiency have led private and nonprofit corporations, governments, universities, hospitals, law enforcement agencies, and many other organizational entities to maintain digital records.[28] These databases are at risk, and sensitive data such as social security numbers and biometric information are routinely exposed.[29] In the United States, the number of data breaches to organizations has increased from 157 in 2005 to nearly 800 in 2014.[30] There is no indication that this upward trend

24. For further discussion on national security issues in the wake of the Snowden revelations and why the government should operate with some level of nondisclosure, *see, e.g.*, John Bolton, *Edward Snowden's Leaks Are a Grave Threat to US National Security*, GUARDIAN (June 18, 2013 7:30 AM), https://www.theguardian.com/commentisfree/2013/jun/18/edward-snowden-leaks-grave-threat [https://perma.cc/FK84-BG7F].

25. Organizations have a duty to operate transparently and an organization can and should protect PII while *at the same time* operating with an acceptable level of transparency. The two concepts are not mutually exclusive. For example, organizational transparency should reveal how an organization is governed for the benefit of the voting public or shareholders, but it should not lead to publication of sensitive client data. The scales have tipped too far toward organizational failure to protect PII.

26. *See, e.g.*, Ann Marie Awad, *Life After Doxing*, LIFE OF THE LAW (Jan. 27, 2015), http://www.lifeofthelaw.org/2015/01/lifeafterdoxing/ [https://perma.cc/2DD3-8TFS] (explaining one woman's nearly 10-year, ongoing battle with stalkers who stole her Facebook photos and continually post them on the Internet).

27. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 244 (2007).

28. *See id.*

29. *Id.* at 248–1.

30. *2005-2014 Breach Analysis*, IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf [https://perma.cc/CHL2-EDYU] (last visited Nov. 13, 2016).

will slow down anytime soon; indeed, the number of hacking breaches has doubled since 2007 to nearly 30% of all data breaches.[31]

Although companies suffer from hacking breaches,[32] the unwitting consumer often has no idea how much PII companies are collecting. For example, armed with a consumer's social security number (SSN), name, and birth date, a cyber-thief can easily empty bank accounts, procure credit cards and lines of credit, secure loans, sign up for online services, and enroll in government programs, just to name a few.[33] It is obvious that any one of these forms of identity theft can have a grievous impact on a person's life, and in extreme cases, it can even lead to death.[34]

A. Edward Snowden and Ashley Madison

In 2013, Edward Snowden shocked the world when he published documents that implicated the Federal government in a plethora of questionable (indeed, unconstitutional) spying tactics.[35] Documents revealed that major telecommunications companies were forced, through secret court orders, to provide the NSA with Americans' phone records.[36] The NSA also collected hundreds of millions of text messages every day and tapped hundreds of foreign leaders' cell phones, including that of German Chancellor Angela Merkel.[37] Also troubling was the NSA's practice of tapping the private fiber optic cables that connect the world's biggest search engines: Yahoo and Google.[38] Through this practice, the NSA enjoyed unfettered access to the biggest information pipelines in the world. Technology companies, upon learning of this invasion, were "outraged,"[39] and Google vowed to improve its

31. *Id.*

32. *See* Larry Ponemon, *Lessons Learned from 11 Years of Cost of Data Breach Research,* SECURITYINTELLIGENCE (June 15, 2016), https://securityintelligence.com/cost-of-a-data-breach-2016/ [https://perma.cc/3GF6-FRRT].

33. Citron, *supra* note 27, at 252.

34. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 100–06 (N.H. 2003) (In this tragic case, an information broker sold a woman's SSN and employment information to a stalker, who tracked the woman down and eventually killed her.).

35. Lorenzo Franceschi-Bicchierai, *The 10 Biggest Revelations from Edward Snowden's Leaks*, MASHABLE (June 5, 2014), http://mashable.com/2014/06/05/edward-snowden-revelations/#.Oxd3MZb8iqS [https://perma.cc/PA96-FKNS]; *see also* Obama v. Klayman, 800 F.3d 599 (D.C. Cir 2015) (granting Plaintiff's request for injunction to stop NSA from collecting metadata as part of its Bulk Telephony Metadata Program and ruling that Plaintiff likely has standing to challenge the constitutionality of this form of governmental spying).

36. Franceschi-Bicchierai, *supra* note 35.

37. *Id.*

38. Lorenzo Franceschi-Bicchierai, *New Snowden Leak: NSA Tapped Google, Yahoo Data Centers*, MASHABLE (Oct. 30, 2013), http://mashable.com/2013/10/30/nsa-google-yahoo-data-centers/#umV6sVO4YgqF [https://perma.cc/TDD5-5EQ6].

39. *See, e.g.*, Newsy Tech, *Google, Yahoo! React to NSA's MUSCULAR Program*, YOUTUBE, (Oct. 31, 2013), https://www.youtube.com/watch?v=DWR1dCLipTg [https://perma.cc/BJD5-Z8PA].

encryption to prevent further government-sponsored monitoring.[40] This particular revelation, along with the NSA's PRISM program propelled technology companies to implement stronger customer privacy protections.[41] The PRISM program compelled companies by law to turn over sensitive data to the NSA.[42]

Although companies have adjusted their practices somewhat to improve protection measures, they have not curbed doxing. In 2015, hackers went after the Ashley Madison website[43] and published 60 gigabytes of PII on the Internet, including a member list and user credit card information.[44] The hackers, calling themselves "The Impact Team," blamed Avid Life Media (ALM), the Toronto-based firm that owned Ashley Madison and other dating websites, for lying about the so-called "full delete" button.[45] ALM made $1.7 million off the service, whereby customers could pay about $20 to completely remove all traces of involvement on the site.[46] But as the hackers revealed, that data was never fully deleted.[47] The Impact Team exposed the fraudulent practice and demanded that ALM take down the site, and when their demands went unfulfilled, it noted "[w]e have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data."[48]

The full ramifications of the breach proved disastrous. Several suicides in the United States were directly linked to the dox, including a pastor and a police captain.[49] Countless spouses and others used a search engine that was designed specifically to

40. *See id.*

41. Matt Sledge, *The Snowden Effect: 8 Things That Happened Only Because of the NSA Leaks*, HUFFINGTON POST: POLITICS (June 5, 2014, 7:31 AM), http://www.huffingtonpost.com/2014/06/05/edward-snowden-nsa-effect_n_5447431.html [https://perma.cc/ZU3N-QTSR].

42. *Id.*

43. ASHLEY MADISON, www.ashleymadison.com (last visited Nov. 13, 2016) (an online dating website for individuals looking for "discreet" relationships).

44. *Online Cheating Site Ashley Madison Hacked*, KREBS ON SECURITY (July 19, 2015, 11:40 PM), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/ [https://perma.cc/9GZS-UFMC].

45. *Id.*

46. Megan Geuss, *Paying $20 to Delete Your Ashley Madison Profile Was Probably a Bad Idea*, ARS TECHNICA (July 20, 2015, 3:21 PM), http://arstechnica.com/business/2015/07/cheaters-hook-up-site-ashley-madison-makes-account-deletion-confusing/ [https://perma.cc/PME7-7YYW].

47. *Id.*

48. Samuel Gibbs, *Ashley Madison Condemns Attack as Experts Say Hacked Database is Real*, GUARDIAN (Aug. 19, 2015, 6:35 AM), http://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports [https://perma.cc/LP6N-8H92].

49. Sara Malm, *Two Suicides Are Linked to Ashley Madison Leak: Texas Police Chief Takes His Own Life Just Days After His Email is Leaked in Cheating Website Hack*, DAILY MAIL (9:59 AM, Aug. 24, 2015), http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html [https://perma.cc/C2AK-C8LM]; *see also* Brown, *supra* note 19.

comb through the published data.[50] Several class action lawsuits have been filed against ALM, in connection with the full delete button, for fraudulently indicating that users could completely wipe out any trace of a connection to the site.[51] In short, the hack has devastated the company, and its users' privacy.

B. Organizational Doxing as International Terrorism

As the Ashley Madison website case demonstrated, organizational doxing is used to retaliate against subjectively immoral behavior. The practice is also used as a form of terrorism,[52] as shown by the recent release of over half a million Saudi Arabian government "cables," or official documents.[53] A group calling itself the Yemen Cyber Army claimed that it hacked the Saudi government "as retaliation to the House of Saudi's war against Yemen."[54] Although the perpetrator's identity has not been officially confirmed, the fact remains that hackers infiltrated a sovereign nation's security system and published documents detailing classified government operations.

Similarly, a terrorist group named Guardians of Peace ("Guardians"), hacked Sony Pictures Entertainment's databases in response to a recently released movie poking fun at Kim Jong-un, North Korea's leader.[55] The United States government alleged that the North Korean government was responsible for the hack.[56] The Guardians claimed to possess over 100 terabytes of data from Sony,[57] including sensitive employee data and an archive of emails

50. Chris Silver Smith, *For Ashley Madison Users, What's Next? Reputation Apocalypse, Phase 2*, MARKETING LAND (Sept. 9, 2015, 9:21 AM), http://marketingland.com/ashley-madison-users-whats-next-reputation-apocalypse-phase-2-141104 [https://perma.cc/MK6W-VBCQ].

51. *Ashley Madison Class Action Lawsuit*, SCHMIDT FIRM (Aug. 19, 2015), https://www.schmidtlaw.com/ashley-madison-class-action-lawsuit/ [https://perma.cc/T9PR-RNN6]; *see also Ashley Madison Privacy Breach, supra* note 20.

52. The United States Criminal Code defines "international terrorism" in relevant part as "[a]ctivities that . . . would be a criminal violation if committed within the jurisdiction of the United States or of any State; appear to be intended to intimidate or coerce a civilian population. . . . and occur primarily outside the territorial jurisdiction of the United States ." 18 U.S.C. § 2331 (2012). Although this particular hack did not target the United States, if it had it would have fit easily into the incredibly broad definition of terrorism that Congress crafted.

53. *See* Mahdi Darius Nazemroaya, *The Ridiculous Nature of Saudi Intelligence: What the Saudi Cables Released by WikiLeaks Say and Don't Say*, GLOBAL RESEARCH (June 23, 2015), http://www.globalresearch.ca/what-the-saudi-cables-released-by-wikleaks-say-and-dont-say/5457713 [https://perma.cc/LP8F-K8MZ].

54. *Id.*

55. James Cook, *Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes so Far*, BUSINESS INSIDER (Dec. 16, 2014, 2:19 PM), http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12 [https://perma.cc/KC43-78PD].

56. *Id.* The true identity of Guardians has never been confirmed, but this act definitely fits the definition of terrorism outlined in the U.S. Code. *See* 18 U.S.C. § 2331 (2012).

57. *Id.*

from Sony executives. According to a letter addressed to all Sony employees, the company admitted that during the cyber-attack hackers may have obtained its employees': (1) basic biographical data, including driver license and social security numbers; (2) financial data, including credit card information for corporate travel and expense; (3) user names and passwords; (3) health insurance information; and (4) compensation data, including the embarrassing revelation that Sony paid its female executives significantly less than their male counterparts.[58] The hacked information included data not only about Sony's employees, but also their dependents and individuals connected with employees.[59] If hackers meant to target Sony and its supposedly immoral business practices, they got what they sought and then some.

In an ironic example of organizational doxing, a firm called Hacking Team was itself hacked in July of 2015.[60] Hacking Team is an Italian firm that specializes in selling "intrusion and surveillance tools" to governments worldwide, including the United States.[61] The hackers who infiltrated Hacking Team gained access to a large internal database and published information incriminating Hacking Team for doing business with totalitarian regimes, something that it flatly denied when questioned by the United Nations in 2014.[62] In particular, a $480,000-euro contract between Hacking Team and Sudan was released, which likely means serious repercussions for the group (and Sudan), if proven true.[63] Hacking Team responded with a statement: "Don't believe everything you see. Most of what the attackers are claiming is simply not true . . . . The attackers are spreading a lot of lies about our company that is [sic] simply not true. The torrent contains a virus."

Whether or not the information published about Hacking Team is true, the dox and others like it raise serious and terrifying questions about future doxes.[64] What is the real motivation behind a

58. Schneier, *supra* note 5.

59. Letter from Sony Pictures Entertainment to Sony Pictures Employees (Dec. 8, 2014), http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf [https://perma.cc/LQ64-ULXZ] (informing employees of the hack and that much of their PII was compromised).

60. Steve Ragan, *Hacking Team Responds to Data Breach, Issues Public Threats and Denials*, CSO (July 6, 2015, 2:20 AM), http://www.csoonline.com/article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html [https://perma.cc/Y6A8-WAQQ].

61. *Id.*

62. *Id.*

63. *Id.*

64. There will, without doubt, be more examples of organizational doxing in the future. Many networks are simply not secure and remain highly vulnerable to online attacks. One blogger has gone so far as to say that "[i]f someone sufficiently skilled, funded and motivated wants to steal an organization's secrets, they will succeed." Schneier, *supra* note 5.

hacking group's actions? Is it terrorism?[65] How much of the published data can be trusted? Has the hacking group, or publishing source, altered data in strategic places to ensure that readers draw specific conclusions? At least one American thinker has asked similarly tough questions that this note considers below.

C. The Worst-Case Scenario

Dan Carlin is a political commentator, amateur historian, and professional podcaster. In one episode of his podcast, *Common Sense*, he elaborates on a hypothetical situation that could destroy privacy in the modern world.[66]

Imagine that a "shadowy hacker group" releases a gigantic trove of PII.[67] The people targeted are the 1,000 most influential, powerful, or important people in the world. Their data is dumped on the Internet for the world to scrutinize. This data includes anything and everything: subscriptions to pornographic websites, skeletons in the closet, personal emails, records of political campaign donations, credit card information, etc. Carlin hypothesizes that these 1,000 people would be outraged, and would likely demand that politicians change the law to improve Internet privacy. In one sense, this reaction is human nature—individuals not yet harmed are not threatened by data breaches. However, once a data breach happens to them, it becomes a much more serious concern.

A large-scale dox could raise awareness amongst movers and shakers, and improve data security nationally. But Carlin's hypothetical goes further—he imagines that hackers might decide to throw in a lie or two to alter the data. Imagine that every twenty or twenty-fifth person's data is altered at random. Carlin makes the point that if enough of the data were true, it would be next to impossible, when combing thousands of gigabytes of information, to distinguish the true data from the false data.[68] This would create many problems and likely involve "important" people in false scandals.

Carlin notes that during the 1960's, it is alleged that Federal Bureau of Investigation (FBI) sent Dr. Martin Luther King a tape recording of his illicit affairs. The FBI threatened that if Dr. King continued to incite social unrest, the tape would be released.[69]

---

65. This question raises a whole host of legal issues well beyond the scope of this paper, namely how and when the United States government could be authorized to respond. *See* 18 U.S.C. § 2331.

66. *See* Dan Carlin, *Backdoors to Glass Houses*, COMMON SENSE (July 13, 2015), http://www.dancarlin.com/product/common-sense-294-backdoors-to-glass-houses/ [https://perma.cc/272R-UKET].

67. *Id.* The hypothetical is drawn exclusively from Carlin's podcast.

68. *Id.*

69. *Id.*; *see also* Beverly Gage, *What an Uncensored Letter to M.L.K. Reveals*, N.Y. TIMES (Nov. 11, 2014), http://nyti.ms/1pMgTP8 [https://perma.cc/X3PY-VQTZ].

Essentially this was extortion, and the FBI knew that if the tape were released, Dr. King's reputation would be irrevocably damaged—whether or not it was actually Dr. King on the tape. Today, all that is necessary to achieve the same effect is to plant evidence that someone indulges in child pornography or an equally abhorrent habit.[70] It would be very difficult for one of these 1,000 important people to refute digital "evidence" that he or she reads or engages in child pornography, even if it was not true. A similarly disastrous result might occur if hackers planted false data about a famous politician. The most alarming issue is that large amounts of this evidence could *easily* be planted along with the trove of data released during a dox.[71]

Carlin argues that part of what makes this hypothetical situation possible, perhaps even probable, is that companies have installed (or have been forced by the government to install) network vulnerabilities known as "backdoors."[72] In a debate between the federal government and technology companies such as Apple and Google, the FBI argues that in order to protect the public interest and thwart criminals, it needs backdoor access to PII that companies store on their servers.[73] For example, the government took the position that to catch criminals, it needs access to encrypted files found on phones and computers, and that technology companies should provide backdoor access.[74] Apple, Google, and hundreds of other companies responded with a letter to President Obama urging him to "reject any proposal that U.S. companies deliberately weaken the security of their products."[75] The companies requested, in contrast, that the government promote policies that encourage strong encryption technology, noting that "[s]uch policies will in turn help to promote and protect cybersecurity, economic growth, and human rights."[76] The

70. As an example of our society's strong desire to punish sex offenders, Jared Fogle, the famous Subway Restaurants advertising actor, was recently sentenced to 15 years in prison for sex with minors and possession of child pornography. *See* Bill Chappell, *Jared Fogle Sentenced to 15 Years in Prison for Sex With Minors, Child Pornography*, NPR (Nov. 19, 2015, 10:55 AM), http://www.npr.org/sections/thetwo-way/2015/11/19/456622271/jared-fogle-to-learn-sentence-for-sex-with-minors-child-pornography [https://perma.cc/2G5F-WWNX].

71. Carlin, *supra* note 66. The possibilities for destruction seem endless. For example, politically motivated hackers could silence their opposition; governments could silence their opposition; governments could extort other governments; individuals could extort other individuals; individuals could extort governments; and so on.

72. *Id.*

73. *See, e.g.*, Paul Sawers, *Apple, Google, and 140 Others Ask Obama to Reject 'Backdoor' Access to Encrypted Data*, VENTURE BEAT (May 19, 2015, 3:19 AM), http://venturebeat.com/2015/05/19/apple-google-and-140-others-ask-obama-to-reject-backdoor-access-to-encrypted-data/ [https://perma.cc/46HZ-H4KF].

74. *Id.*

75. Letter from Civil Soc'y Orgs., Cos., & Trade Ass'ns to Barrack Obama, President of the United States (May 19, 2015), https://static.newamerica.org/attachments/3138—113/Encryption_Letter_to_Obama_final_051915.pdf [https://perma.cc/L7QU-JGQJ].

76. *Id.*

White House responded favorably by overruling law enforcement agencies and deciding not to pursue policies that would require companies to provide backdoor access.[77] However, until companies begin implementing strong encryption and other dox-prevention measures throughout their networks, Dan Carlin's hypothetical worst-case scenario may turn out to be closer to fact than fiction.

II. FRAMEWORKS DEVELOPED TO COMBAT THE THREATS OF DOXING.

In the face of the growing doxing problem, many solutions have been proposed and implemented with varying degrees of success.[78] First, Congress has tried its hand at legislation to help organizations prevent doxing disasters, most recently with the Cybersecurity Information Sharing Act (CISA). Second, federal agencies such as the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have expanded their jurisdictions to include enforcement for data breaches caused by lax data security systems. Third, many states have enacted laws with varying structures that aim to combat the dissemination of PII. Fourth, victims of organizational doxing have brought common law negligence suits against companies whose databases have been breached. Finally, strict liability regimes have been proposed as a way to most efficiently and least expensively prevent further doxing disasters.

A. Federal Legislation

Currently, a patchwork of federal legislation covers some areas of data protection, but there is no all-inclusive law regulating the collection and use of PII.[79] The Gramm-Leach-Bliley Act (GLBA)[80] obliges financial institutions to "protect the security and confidentiality of [their] customers' nonpublic personal information."[81] The GLBA further mandates that each financial institution shall "establish appropriate standards" (1) to ensure customer information security and confidentiality; (2) to protect against anticipated threats to that information; and (3) to protect against unauthorized use of that information that may harm the customer.[82]

The Health Insurance Portability and Accountability Act (HIPAA) regulates healthcare policy, and applies broadly to health

77. Andy Greenburg, *Cops Don't Need a Crypto Backdoor to Get Into Your IPhone*, WIRED (Oct. 12, 2015, 2:14 PM), http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/ [https://perma.cc/QDA5-FTFE].

78. *E.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 93 (2014).

79. Ieuan Jolly, *Data Protection in the United States: Overview*, PRACTICAL LAW (July 1, 2016), http://us.practicallaw.com/6-502-0467 [https://perma.cc/QA5N-R786].

80. 15 U.S.C. §§ 6801–09 (2012).

81. 15 U.S.C. § 6801.

82. *Id.*

care providers, pharmacies, health care insurance providers, and other entities that deal with medical information.[83] Similar to financial institutions, health care institutions are required to maintain safeguards "to ensure the integrity and confidentiality of [health] information."[84] The Sony dox, where hackers obtained the sensitive health information of nearly 30,000 employees and their families,[85] implicates HIPAA; Sony recently settled a class action lawsuit brought by victims of the breach.[86] This is the first time that victims of a large-scale dox have brought a class action suit for damages resulting from a dox, and the plaintiff-favorable settlement "could serve as a precedent for the consequences organizations and corporations could face following a HIPAA breach."[87]

Several other federal laws regulate how personal data is collected and stored. First, the Federal Information Security Management Act mandates that the heads of each executive agency provide "information security protections" for all information collected or maintained by the agency.[88] Second, the Fair Credit Reporting Act directs credit reporting agencies (including credit card companies) to "adopt reasonable procedures . . . with regard to . . . confidentiality" when dealing with customer credit information.[89] Finally, the Cybersecurity Act of 2015 (the "Act") creates a voluntary framework that allows companies to share "cyber threat" information with the Department of Homeland Security ("DHS").[90] The DHS stated that "many cyber intrusions can be prevented if we share cyber threat indicators [among companies and government]," and further stated, "[s]haring this kind of information in real-time, and swiftly applying defensive measures, will allow both the government and private sector to more effectively prevent attacks."[91] Several privacy advocacy groups have voiced serious concerns about the repercussions of such

83. 42 U.S.C. § 1320d-2(d)(2) (2012).

84. *Id.* § (d)(2)(A).

85. Letter from Sony, *supra* note 59.

86. Erin McCann, *Sony HIPAA Breach Lawsuit Approaches Settlement*, HEALTHCARE IT (Sept. 4, 2014, 11:04 AM), http://www.healthcareitnews.com/news/sony-hipaa-breach-lawsuit-approaches-settlement [https://perma.cc/YP2E-S4KC].

87. *Id.*

88. 44 U.S.C. § 3554(a)(1)(A)(i-ii) (Supp. 2015).

89. 15 U.S.C. § 1681(b) (2012).

90. 6 U.S.C. § 1502(a)(1-5) (Supp. 2015); *see also* Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015, 2:59 PM), https://www.lawfareblog.com/cybersecurity-act-2015 [https://perma.cc/34W2-VHQC]; David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NATIONAL LAW LAW REV.IEW (Dec. 20, 2015), http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015 [https://perma.cc/N4A4-8CF5].

91. Statement by Secretary Jeh C. Johnson on Implementation of the Cybersecurity Act of 2015, DEP'T OF HOMELAND SEC. (Feb. 16, 2016), https://www.dhs.gov/news/2016/02/16/statement-secretary-jeh-c-johnson-implementation-cybersecurity-act-2015 [https://perma.cc/VP85-AX7T].

an expansive bill,[92] and it remains to be seen how effective the Act will be in preventing large-scale data breaches.

B. Federal Agency Action

Some federal agencies have attempted to prevent inadvertent disclosure of PII and the dangers of doxing by expanding their jurisdictions.[93] Chiefly, the FTC has expanded its unfair trade practices jurisdiction to include "any private entity's failure to provide 'appropriate' information security."[94] Since 1996, the FTC has brought hundreds of privacy and data security cases and has protected billions of consumers,[95] and since 2002, the FTC has used its unfair trade practices jurisdiction to bring over 50 cases against companies.[96] One such case was against Snapchat, Inc., where the FTC alleged the company had deceived consumers about the security measures it took to ensure that sensitive data was protected from misuse and unauthorized disclosure.[97] Snapchat's failure to secure its users' data allowed hackers to compile a database of 4.6 million Snapchat user names and phone numbers.[98]

The FCC also protects telecommunications customer data (consumer proprietary network information, or CPNI) from unlawful and inadvertent disclosure.[99] Telecommunications carriers must protect the confidentiality of CPNI, and are prohibited from disseminating information obtained from customers solely "by virtue of [their] provision of a telecommunications service" to third parties.[100] In other words, the PII that telecommunications providers collect from customers in the ordinary course of business is subject to strict confidentiality requirements, and may not be sold to third parties.

The Congressional grant of authority found in § 222 of the Telecommunications Act is indeed broad, and in April 2015, the FCC flexed its enforcement muscles when it fined AT&T $25 million for an internal data breach.[101] Three employees at a call center with systems operated by AT&T used their login credentials to steal and sell SSNs

92. 6 U.S.C. § 1503(d) (Supp. 2015); *but see Omnibus Funding Bill is a Privacy and Cybersecurity Failure*, OPEN TECH. INST.: NEW AM. (Dec. 16, 2015), https://www.newamerica.org/oti/press-releases/omnibus-funding-bill-is-a-privacy-and-cybersecurity-failure/ [https://perma.cc/GND3-K5DD].

93. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 886 (2002); *see also* Citron, *supra* note 27.

94. Citron, *supra* note 27, at 256.

95. 2014 PRIVACY AND DATA SECURITY UPDATE, FTC 1 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [https://perma.cc/GQ83-KCXE].

96. *Id.* at 5.

97. *Id.*

98. *Id.*

99. *See* 47 U.S.C. § 222 (2012).

100. *Id.* § 222(c)(1).

101. Sam Pfeifle, *FCC Fines AT&T $25m for Data Privacy Lapse; Who Will Be Next?*, IAPP (Apr. 9, 2015), https://iapp.org/news/a/fcc-fines-at-who-will-be-next/ [https://perma.cc/H2GD-BB2B].

and other PII from over 50,000 customers.[102] In the Consent Decree, AT&T agreed to pay the hefty fine, hire a privacy policy compliance officer, create a privacy compliance plan to be submitted to the FCC, and file compliance reports for the next three years.[103] This was *big* news in the privacy industry because the FCC was following through with its promise to more rigorously enforce its § 222 rules, as it had begun to do in 2014 with fines against Dialing Services, Sprint, Verizon, Terracom, and YourTel America.[104] The FCC action against AT&T may indicate the way the wind is blowing: the FCC is (allegedly) going to crack down hard on inadequate data security regimes to prevent future data breaches and doxes.[105]

Perhaps even more ominous for the telecommunications industry, the FCC recently reclassified the provision of online services as common carrier activity. Thus a gigantic new slice of private industry is now subject to the § 222 CPNI privacy requirements.[106] Before this ruling, broadband Internet access providers (BIAS), such as Comcast, AT&T, and Verizon, were classified as "information service" providers and were not subject to the FCC's CPNI rules. But now, essentially any provider of Internet connectivity will be classified as a "telecommunications service," and thus will be subject to the stringent requirements of § 222 and the FCC's new (perhaps ferocious) enforcement policy.[107]

C. State Information Privacy Statutes

Because there is no overarching federal information privacy law and only limited executive agency action in the area, states have tried to fill the statutory gap to protect PII from data breaches and doxing.[108] As of 2015, forty-seven states enacted laws that require

102. *AT&T Services, Inc.*, DA Dkt. No. 15-399, Order, 30 FCC Rcd. 2808, 2808 (adopted April 8, 2015).

103. *Id.* at 2815–20.

104. Pfeifle, *supra* note 101. The fines against all the other telecommunications firms totaled $25 million, making the AT&T fine by far the largest.

105. *Id.* ("This enforcement action is a warning shot across the bow that the FCC will not tolerate lax data security practices . . . ." said S. Jennell Trigg, member of the FCC's Federal Advisory Committee on Diversity for Communications in the Digital Age).

106. *Protecting and Promoting the Open Internet*, GN. Dkt. No. 14-28, Report & Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, para. 337 (adopted Feb. 26, 2015) [hereinafter *Open Internet Order*]. It should be noted that the FCC's Open Internet Order is embroiled in several legal battles, and it remains to be seen how much, if any, of the Order is here to stay. If the language changes, for example, and the courts limit the FCC's definition of broadband Internet access service providers, it could hamper the FCC's enforcement strategy. *See* Klint Finley, *Net Neutrality Is in More Danger Than Ever*, WIRED (Mar. 1, 2016, 7:00 AM), http://www.wired.com/2016/03/despite-fcc-net-neutrality-danger-ever/ [https://perma.cc/5A8Z-4WH9].

107. *See Open Internet Order*, *supra* note 106; *see also* Pfiefle, *supra* note 101.

108. *See* Citron, *supra* note 27, at 256–57; *see also* Reidenberg, *supra* note 93, at 888–89.

entities to notify their customers of any sort of network security breach involving PII.[109] Further, twenty-nine states require entities to destroy PII, or else render it unreadable or undecipherable.[110]

California has historically spearheaded this effort to protect PII. Indeed, many states have modeled their statutes to resemble California's.[111] Most relevant is California's data security law,[112] which requires organizations to provide "reasonable security" to protect PII from "unauthorized access, destruction, use, modification, or disclosure."[113] The statute also mandates that if a company discloses PII to a non-Californian third party, the company must "require by contract" that the third party maintain reasonable security measures to protect that PII.[114] Even further, the statute requires entities to disclose to customers any breach of network security that results in stolen PII.[115]

Other states are experimenting with expanding legislation, and recently the Massachusetts legislature enacted a bill giving the state's Department of Consumer Affairs and Business Regulation (the "Department") wide latitude to regulate information security systems in the state.[116] The Department developed a highly detailed list of technical specifications that "[e]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain."[117] This is a very broad swath—businesses that possess even one customer's PII from Massachusetts must comply with all the technical specifications. The entity must also keep a written record of every specification it complies with, presumably for agency inspection.[118]

D. Negligence Suits

Privacy tort doctrine presents another way of allocating liability for doxing disasters and potentially preventing them in the future. In 1890, Samuel D. Warren and Louis D. Brandeis published *The Right to Privacy*, calling for tort law to protect an individual's "right to be let alone."[119] The tort action would give each individual the right to decide, "to what extent his thoughts, sentiments, and emotions shall

109. Jolly, *supra* note 79.
110. *Data Disposal* Laws, NCSL (Jan. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx [https://perma.cc/FFE6-WGKD].
111. *See* Jolly, *supra* note 79.
112. CAL. CIV. CODE §§ 1798.80–84 (2016).
113. *Id.* § 1798.81.5.
114. *Id.* § 1798.81.5(c).
115. *Id.* § 1798.82.
116. *See* MASS. GEN. LAWS ANN. ch. 93H, § 2(a) (West 2016).
117. 201 MASS. CODE REGS. 17.03 (West 2016).
118. *Id.*
119. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

be communicated to others."[120] It would also protect each individual's right to determine how much PII is revealed to others, and ultimately allow every person to develop his or her own personality, free from interference.[121]

Although many courts embraced the Warren and Brandeis view and recognized a broad common law right of privacy,[122] the privacy-tort landscape narrowed in 1960 when William L. Prosser published his influential work, *Privacy*.[123] Prosser defined four privacy torts: (1) intrusion upon seclusion, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places the plaintiff in a false light; and (4) appropriation of the plaintiff's name or likeness.[124] In contrast to Warren and Brandeis's emphasis on an individual's right "to be let alone," Prosser's reformulation of the right of privacy focuses, to limiting effect, on the conduct and injuries involved in privacy invasions and less on the overarching purpose of the right of privacy.[125]

As Danielle Citron—a professor at the University of Maryland School of Law—notes, Prosser's four branches of the privacy tort do not encompass many privacy harms individuals face in the modern world, including the varied mental, reputational, and economic injuries that digital network breach and doxing can inflict.[126] Most harmful, perhaps, is the permanent nature of information published on the Internet. Public disclosures of the past were more easily forgotten, such as a newspaper article whose audience was limited to a geographic region on a specific day, and those willing to tediously sift through library records. In contrast, public disclosures made on the Internet are here to stay.[127] Search engines allow for near-instantaneous results available to anyone with an Internet connection. Harms that once upon a time may have faded along with people's memories are now enshrined in the digital world forever.

One recent case seems to contemplate a legitimate remedy. In *Lone Star Bank v. Heartland Payment Systems*, a large payment processing company was hacked, and several banks suffered severe economic loss compensating consumers for fraudulent charges resulting from the hack.[128] On appeal, the Fifth Circuit held that the

120. *Id.* at 198.

121. *See* Danielle Keates Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1807 (2010) (citing Warren & Brandeis, *supra* note 119).

122. *Id.* at 1821 (citing Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 977–979 (1964)).

123. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

124. *Id.* at 389.

125. *See* Citron, *supra* note 121.

126. *See id.* at 1811–19.

127. *Id.* at 1813.

128. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., 729 F.3d 421, 423 (5th Cir. 2013).

economic loss rule[129] did not bar recovery from the payment processing company under a traditional negligence theory.[130] Further, if the banks proved that the payment processing company acted negligently during the cybersecurity failure, then they could recover for purely economic loss.[131] This is significant because the Fifth Circuit effectively created an exception to the economic loss rule in the context of a large data breach. If more courts lean this direction, future plaintiffs injured only financially would likely bring more traditional negligence suits against companies that fail to protect PII. This might incentivize companies to implement stronger security systems to prevent liability.

E. Strict Liability

Under a theory of strict liability, an organization would be liable for harm, including purely economic harm, caused by cybersecurity breaches. Organizations would be liable whether or not they act negligently. The products liability doctrine from the Second[132] and Third[133] Restatements of Torts could be used as a model for the creation of an entirely new provision, stating that organizations are liable for any harm to consumers caused by security breaches on their networks. Because consumers often have limited knowledge of how much PII a given organization collects about them, the organizations themselves are in the best position to prevent PII leaks. A strict liability regime would ensure that organizations take PII protection seriously by imposing significant monetary penalties for all harms caused by hacks and doxes.[134]

---

129. Traditionally, tort remedies are reserved only for plaintiffs who have suffered a physical harm, and the economic loss rule bars recovery for economic loss alone. *See id.* at 423.

130. *Id.* at 427.

131. *Id.*

132. "One who sells any product in a defective condition unreasonably dangerous to the consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if (a) the seller is engaged in the business of selling such a product, and (b) it is expected to and does reach the user or consumer without change in the condition in which it is sold." RESTATEMENT (SECOND) OF TORTS § 402(A)(1) (AM. LAW INST. 1965).

133. "One engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by that defect." RESTATEMENT (THIRD) OF TORTS § 1 (AM. LAW INST. 1998). Section 2 goes on to describe three defects that fit the definition in § 1: manufacturing, design, and warranty defects. *Id.* § 2.

134. Of course, the argument could be made that perfect cybersecurity is impossible. *See, e.g.*, Steve Banker, *If Preventing a Cybersecurity Attack is Impossible. . .*, FORBES (Mar. 3, 2015, 7:27 AM), http://www.forbes.com/sites/stevebanker/2015/03/03/if-preventing-cybersecurity-attacks-is-impossible/#37532ec31af0 [https://perma.cc/4AAN-D2A8]. Because information technology changes so rapidly, some hacks are probably inevitable given sufficient resources. But even so, a strict liability regime would do the most to adequately allocate the damages of organizational doxing. Companies that implement strong network security are less likely to suffer hacks. If a hack does occur, those companies with intelligent contingency plans are more likely to be able to stop the

The case for strict liability against organizations that cause doxing harm by leaking PII, intentionally or not, is strong. Citron again leads the way in this area with a potent metaphor derived from the famous 19th century English case *Rylands v. Fletcher*.[135] In that case, Rylands, a textile mill owner in Lancaster, England, hired a contractor to build a large reservoir to aid in production at his mill.[136] When the reservoir failed, water escaped and infiltrated a nearby mine, ruining it. The mine's owner, Fletcher, sued Rylands for the damage caused by the escaping water, and the House of Lords eventually ruled in Fletcher's favor, holding that "the person who, for his own purposes, brings on his land and collects and keeps there anything likely to do mischief if it escapes . . . is *prima facie* answerable for all the damage which is the natural consequence of its escape."[137] The Lord Chancellor went on to surmise:

> the neighbour who has brought something on his own property (which was not naturally there), harmless to others so long as it is confined to his own property . . . should be obliged to make good the damage which ensues if he does not succeed in confining it to his own property.[138]

Essentially, the House of Lords imposed strict liability on Rylands (who had "brought" the reservoir onto his land) when it failed and destroyed Fletcher's mine. It made no difference to the Lord Chancellor that the contractor who had installed the reservoir had done so negligently—Rylands was held liable for the escaping water under a theory of strict liability, despite the possible presence of intervening negligence.[139]

III. STATE INFORMATION PRIVACY STATUTES VERSUS A SYSTEM OF STRICT LIABILITY.

This note has examined five frameworks that address the problem of organizational doxing: (1) federal legislation; (2) federal agency action; (3) state information privacy statutes; (4) negligence suits; and (5) strict liability. State information privacy statutes, such as the one implemented in Massachusetts, may ultimately become an effective method to combat doxing because the executive agencies in

damaging effects (for example, by shutting down the part of the network that was infiltrated). Preventing all hacks may be impossible, but a strict liability regime would still incentivize companies to develop stronger protections.

135. Rylands v. Fletcher, [1868] UKHL 1, LRE & I. App. 330 (HL) (appeal taken from Eng.), http://www.bailii.org/uk/cases/UKHL/1868/1.pdf [https://perma.cc/87K7-MA6N]; Citron, *supra* note 27, at 268.

136. Citron, *supra* note 27, at 270.

137. Rylands, *supra* note 135, at 339–40.

138. *Id.* at 340.

139. *Id.*

charge of developing technical rules could respond much more quickly than Congress or the courts. However, strict liability is likely to be the most effective in preventing future doxing harms because it would compel organizations, through the threat of economic impairment, to develop better cybersecurity systems. Strict liability is also one of the few regimes that is proactive, rather than reactive, in dealing with doxing harms. If every consumer who suffered harm because of a data breach were guaranteed recourse from the organization that jeopardized the security of that data, organizations would have to beef up security, or risk going out of business.

Bolstering the strict liability argument, the *Rylands* case[140] provides a good metaphor for modern cybersecurity breaches, and the rule of law is eerily applicable in today's information-driven, data-obsessed world.[141] The water reservoir from *Rylands* is just like a modern database.[142] Rylands collected water on his land, knowing that it was "likely to do mischief if it escape[d]," and when it did, he was held strictly liable for the damage. In the same way, organizations collect PII and store it in vast databases. These organizations know, and this note demonstrates, that if that information escapes, it is likely to cause serious harm, potentially to millions of people.

It could be argued that hackers are a superseding cause to doxing harm. Hackers are the malicious force behind identity theft and doxing, and it generally takes a hacker to cause a security breach. In this way, organizations may argue they should be exempt from liability because they are not the *direct* cause of harm. *Rylands* contemplated this idea over a hundred years ago and disposed of it. The contractor hired by Rylands built the reservoir negligently, but it made no difference to the House of Lords. Storing large amounts of water on one's property was a sufficiently dangerous activity to warrant strict liability, if one failed to keep that water confined.[143]

Similarly, if organizations fail to keep PII confined to their databases, strict liability should be imposed. Organizations should be held accountable for the damage caused by data breaches under the same theory as *Rylands*—anyone who collects information that is likely to be destructive if it escapes should be liable for the damage caused when that information escapes. Society depends on organizations to maintain accurate records of private information in order to conduct business, execute transactions, preserve healthcare records, deliver financial statements, and so much more. The world is information-driven. The need for safe, reliable databases is increasing every day, and the last 20 years have shown that something more

140. *Id.*
141. *See* Citron, *supra* note 27, at 278; *but see* Banker, *supra* note 134.
142. *See id.*
143. *See* Rylands, *supra* note 135, at 339–40.

drastic than simple negligence liability is necessary to ensure that organizations adequately protect PII from the threats of doxing. Strict liability modeled after *Rylands* is a viable model to this end.

Although strict liability would be most effective in preventing future doxing harms, its implementation may not be realistic in the short-term. The next best method to prevent doxing harms is legislation at the state level, which could be implemented almost immediately. Traditionally, California has been the standard-bearer for much privacy-related legislation. California's data security law was novel at its inception, and served as a model for many other state laws, but it is generally reactive in nature.[144] That is, companies are forced to disclose a breach *after* it happens. Entities are required to take reasonable steps to protect customer data, but if they don't, plaintiffs must sue *after* the fact.[145] By that time, the damage is probably already done and hackers may have already posted stolen PII. Some states, however, are experimenting with a more proactive, preventative statutory regime, and Massachusetts leads the way.

The Massachusetts law,[146] which directs its Department of Business Affairs to come up with a comprehensive cybersecurity policy that organizations must follow if they wish to conduct business in the state, is forward-thinking legislation. The legislature wanted the citizens of Massachusetts to be better protected from the very real threats of data breach[147] and directed one of the state's executive agencies to develop actual technical specifications to be implemented by organizations. This is highly effective because unlike federal legislation that may take years to actually get to the floor of either house (during which time hackers may have changed tactics many times), a state executive agency is adaptable enough to propose and implement effective regulation relatively speedily. Entities in Massachusetts must comply with the regulations, even if those entities are based elsewhere in the world, but have customers in Massachusetts, or risk litigation.[148] Because of its practicality and

144. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [https://perma.cc/CC4M-KLT6]; *see generally* CAL. CIV. CODE § 1798.82(a) (West 2016) ("[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach . . . to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"). Some parts of the statute, however, are designed to be *proactive* in nature. *Id.* § 1798.81.5(b) ("[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information").

145. *Id.* § 1798.84(b) ("any customer injured by a violation of [California's data security statute] may institute a civil action to recover damages").

146. MASS. GEN. LAWS ANN. ch. 93H, § 2(a) (West 2016).

147. *See id.*

148. *See, e.g.*, Mark Paulding, *Massachusetts Continues Aggressive Information*

effectiveness, more states should adopt a system like the one in place in Massachusetts.

Aside from strict liability and state legislation, traditional negligence suits may have a small impact on ridding the world of doxing threats. Although it is a reactive remedy, *Lone Star Bank's* holding is significant, nonetheless, for several reasons.[149] First, the economic loss rule has traditionally served as a bar to recovery for non-physical tortious conduct, and the Fifth Circuit in *Lone Star Bank* essentially created an exception in the data breach context. Although it is true that under Prosser's formulation of the four privacy torts, economic loss is not necessarily a requirement, many states have erected economic loss rules to prevent recovery, thereby making it more difficult for plaintiffs to recover for invasions of privacy. This case could serve as a precedent to dismantle the economic loss rule in the face of cybersecurity failures.

Second, if the Fifth Circuit's treatment of the economic loss rule in the wake of hacking harms sets a precedent, there might be a shift in the way organizations conduct business.[150] If corporations were liable under traditional negligence theories for cybersecurity failures, their executives might think more carefully when deciding what sorts of security systems to install.

Third, although this case extends only as far as hacking harms, it is probable that if embraced by more circuit and state courts, it would eventually encompass doxing harms. Doxing harm is, after all, a form of hacking harm—a hack must transpire,[151] and then the harm itself occurs when the hackers decide to disseminate PII on the Internet.

The Fifth Circuit in *Lone Star Bank* is heading in the right direction. If courts continue to build on this precedent, a new privacy tort regime could be implemented to deal with the threats of doxing by combining (1) Warren and Brandeis's idea of the right to be left alone; (2) a broader interpretation of Prosser's privacy torts; and (3) an exception to the economic loss rule in the data breach context. For example, a return to the Warren and Brandeis mentality (whereby the right to privacy protects an individual's decision to portray himself however he pleases to the world, free from interference) would encompass doxing harms. During a dox, PII is typically used

---

Security Enforcement Agenda, INFORMATION LAW GROUP (July 25, 2014), http://www.infolawgroup.com/2014/07/articles/encryption/massachusetts-continues-aggressive-information-security-enforcement-agenda/ [https://perma.cc/QX42-3QZ8].

149. *See* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013).

150. Paul Rosenzweig, *When Companies Are Hacked, Customers Bear the Brunt. But Not for Long*, NEW REPUBLIC (Oct. 15, 2013), https://newrepublic.com/article/115187/cybersecurity-liability-court-cases-are-changing-blame-game [https://perma.cc/63QZ-D2HH].

151. In the case of the Snowden revelations, a public dissemination via a published news source must transpire. *See* Greenwald, *supra* note 7.

maliciously and against victims' wills, thereby denying victims the chance to present themselves to the world however they please. When an organization negligently interferes with that chance (i.e., fails to protect PII from hackers), victims lose the right to portray themselves to the world however they please, and the Warren and Brandeis right of privacy is violated.

Similarly, two of Prosser's four torts can easily be expanded to include doxing harms. First, an organization's cybersecurity failure could be construed as an intrusion into private affairs. The consumer has a right to expect that her PII will remain private, and indeed much of her PII is directly related to her private affairs (i.e., financial data, birth year, and SSN). Second, the definition of "embarrassing" in the second tort (public disclosure of embarrassing private facts) could extend to sensitive PII. PII is potentially embarrassing anyway (many individuals would not want their financial or cyber-subscription information leaked to the world at large), and invoking liability for public disclosure of personally identifiable information is not such a far stretch from liability for disclosing embarrassing information.

Courts may ultimately revert back to a Warren and Brandeis-like approach, whereby the right of privacy encompasses the right to be left alone, and would logically extend to the right to be free from doxing harms. It is also possible that several of Prosser's privacy torts could be extended to include hacking and doxing harms. But unfortunately, there are obstacles that will prevent many jurists from progressing that far.

First, *stare decisis* prevents the filing of many lawsuits simply because most states have not extended the right of privacy beyond Prosser's limited formulation.[152] Second, the economic loss rule still exists in most states.[153] Unless more courts follow the lead of the Fifth Circuit, the rule will continue to block many suits brought against organizations for doxing harms because there is naturally, in most cases, not any physical harm to accompany the devastating financial and emotional effects.

Beyond torts, Congress is trying to keep up with the threats of doxing. Not surprisingly, federal law is seriously lacking, and currently, only a few areas (mainly healthcare and finance) are statutorily required to protect PII. Even so, the legal language outlining what organizations must do to protect PII is far from clear.

Finally, federal agencies, particularly the FTC and FCC, have

152. *See* Neil M. Richards and Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1904 (2010); *see also* ROBERT M. O'NEIL, THE FIRST AMENDMENT AND CIVIL LIABILITY 77 (2001).

153. DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS § 449 (2d. ed. 2011).

tried for years to prevent PII from falling into the wrong hands. By expanding its unfair trade practices jurisdiction, the FTC has done much to combat the growing threat.[154] But it is not enough, and one federal agency will never be able to enforce penalties for every single organizational cybersecurity failure. The FCC, likewise, has attempted to regulate in the area of data privacy, most significantly with the recent Open Internet Order. Pursuant to § 222, common carriers must protect customer proprietary network information, and if the Open Internet Rules are upheld,[155] a large swath of private companies would suddenly find themselves subject to § 222 jurisdiction, as well. This would be a small victory, as the FCC would still have to tediously monitor every organization, and enforce sanctions on a case-by-case basis. But it would be a step in the right direction.

CONCLUSION

In sum, the threats to world society from organizational doxing are too real to ignore. In just the last few years, the number of cybersecurity attacks has increased dramatically. In the wake of Edward Snowden's revelations, organizational doxes like Ashley Madison and Sony have disrupted lives all over the world. In the extreme, doxes like Sony function as acts of terrorism. Without due care, doxing harms could spin out of control, and without preventative measures, Dan Carlin's hypothetical is likely very close to reality.

To that end, a few individuals are taking action. But much, much more must be done if potential doxing disasters are to be avoided. Federal legislation is a far cry from where it ought to be. At the moment, only a patchwork of laws protects PII from the threats of doxing. Federal agencies like the FTC and the FCC are more flexible than Congress and can do a bit more to protect consumers. The FTC has had some success through its unfair trade practices jurisdiction, but it is still a laborious process, and cannot keep up with the rate of technological change. The FCC, likewise, may be stepping up its enforcement using the Open Internet Order and § 222 of the Telecommunications Act, but it is still too slow to respond effectively to hacks and doxes.

Similarly, private negligence suits are not well positioned to have any real effect on the doxing problem. Prosser's privacy torts do not typically encompass the sorts of harm that doxing victims suffer. But it is possible, by returning to Warren and Brandeis's formulation of the privacy tort, and cementing an exception to the economic loss rule, that private negligence suits could shift liability for doxing disasters to the organizations that fail to protect our PII. However, the problem

154. 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 95, at 1.
155. *See* Finley, *supra* note 106.

persists that this remedy is, at least initially, still reactive in nature.

Two methods, thankfully, are viable in the fight against doxing disasters. First, state legislation, especially when modeled after Massachusetts, may end up being an effective way to force organizations to update network security, at least in the short-term. By providing technical specifications that organizations must follow if they wish to conduct business, Massachusetts may be protecting its citizens' PII better than any other state. Second, although it is not currently in effect anywhere, a strict liability regime would take care of the organizational doxing problem most effectively: if an organization allows PII to escape its database, that organization would be liable for harms that result. Strict liability would incentivize organizations to upgrade network security systems, and consumers all over the world would benefit.