PROTECTING THE GOOD, THE BAD, AND THE UGLY: "EXPOSURE" DATA BREACHES AND SUGGESTIONS FOR COPING WITH THEM

Yasmine Agelidis[†]

Samuel Warren and Justice Louis Brandeis recognized the right to be "let alone" in their famous article *The Right to Privacy* over a century ago.[1] They discussed "the desirability—indeed . . . the necessity—of some such protection" for all persons in their private affairs.[2] While the majority of state legislatures have passed security breach notification (SBN) laws to help protect victims from the economic harms that flow from identity theft data breaches,[3] none have enacted protocols to shield individuals from the newer family of "exposure" data breaches. Today, hackers are turning to exposure breaches—hacks involving the public disclosure of private information resulting in reputational harm to victims—with growing frequency.[4] Because reputational harms leave victims' private information accessible to others for a very long time, if not indefinitely, the law should protect individuals from exposure breaches. The exposure breach family consists of extortion hacks, in which hackers threaten to expose individuals' private information in an effort to make money, and hacktivist attacks, which cover the broad category of hacking for a social or political purpose.[5] Unlike identity theft data breaches, exposure breaches implicate victims' reputations. Given the permanent nature of Internet content, this harm

DOI: http://dx.doi.org/10.15779/Z38F28K

† J.D. Candidate, 2017, University of California, Berkeley, School of Law.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195, 205 (1890).

2. *Id.* at 196.

3. *See Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/3H2A-4DJA].

4. While anecdotal evidence may be offered in support, see Part II, *infra*, it is difficult to find statistical support for this assertion because data breaches often go unreported. "One of the main problems in quantifying the precise impact of cybercrime is that computer attacks are not always detected, or reported." Alvaro Cardenas et al., An Economic Map of Cybercrime 1 (Aug. 15, 2009) (conference paper presented at TPRC), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997795 [https://perma.cc/8Z7N-2B4N].

5. *See* TIM JORDAN & PAUL TAYLOR, HACKTIVISM AND CYBERWARS 1 (2004).

remains with the victim practically forever. Thus, exposure breaches result in harm that simply cannot be undone.

This Note proposes an expansion of data security protocols to account for the permanent reputational damage that flows from exposure data breaches. Because these data breaches implicate permanent reputational concerns as opposed to just repairable economic ones, the ex-post approach SBN laws set forth cannot correct the harm from these attacks. But exercising ex-ante approaches such as establishing mandatory heightened security protocols for companies, state legislatures, and the Federal Trade Commission (FTC) can prevent reputational harm before it occurs. Using the "public disclosure of private information" privacy tort proposed by the Restatement (Second) of Torts as a foundation, the FTC should consider formally adopting a broadened definition for personally identifiable information (PII) that can account for reputation-implicating information. This updated definition can serve to put entities on notice of the significant threat exposure breaches pose. Also, the updated definition can provide a launching point for the FTC to police companies under its Section 5 Authority for unfair or deceptive data management practices involving reputation-implicating information. Moreover, because exposure breaches will likely continue to occur even with heightened security protocols in place, state legislatures should consider the ex-post approach of requiring companies to enroll in cyber liability insurance. This measure would ensure that victims of exposure breaches at least have the opportunity to recover financially for reputational harms resulting from disclosure.

Part I of this Note describes the laws currently governing data breaches and briefly discusses privacy tort law. These frameworks might be helpful for the FTC to consider in reassessing its Section 5 enforcement authority under the modern data breach landscape. Part II explains what extortion breaches and hacktivist attacks are, how they came about, and the harms that flow from them. Finally, Part III proposes a primarily ex-ante legal framework that better protects potential victims of exposure breaches from reputational harms that are practically impossible to correct.

I. LAWS GOVERNING DATA BREACHES

The data security[6] framework in the United States is largely governed by state laws and the FTC. Almost all state legislatures have enacted SBN

6. Data security is traditionally considered through the lens of a three-pronged "CIA" framework: confidentiality, integrity, and availability. Ioannis V. Koskosas & Ray J. Paul, *Information Security Management in the Context of Goal-Setting*, 6 RISK MANAGEMENT 19, 21 (2004). A hacker compromises confidentiality if she gains

laws that govern an entity's obligations when hackers successfully break into its security network.[7] Under these laws, breached entities must notify affected parties if certain information was, or could have been, disclosed.[8] In addition, the FTC has authority under Section 5 of the Federal Trade Commission Act to protect consumers from "unfair" or "deceptive" data security practices, and carries out this mission by, in part, bringing enforcement actions.[9] Moreover, while current data security protocols do not rely on privacy tort law, it can be a helpful launching point for developing a framework to address exposure data breaches.

A. SECURITY BREACH NOTIFICATION LAWS

The vast majority of states have enacted SBN laws to address the economic harms that flow from identity theft data breaches, the oldest and most prevalent type of data breach.[10] Identity thief hackers steal personal information and exploit the data to mimic the victim's identity, or sell it to someone who can.[11] They are interested in accessing "another person's social security number, date of birth, or other personal information [to assume] the data subject's identity in order to secure goods and services on the data subject's accounts."[12] As long as individuals, companies, and governments use credit cards, Social Security numbers (SSNs), and driver's licenses and store financial and medical information online, the practice of identity theft will remain profitable.[13]

SBN laws address the economic harms flowing from identity theft data breaches by requiring companies and government agencies to notify all affected individuals when a breach has occurred and stored PII was or could

unauthorized access to information, threatens integrity by altering or deleting information, and compromises availability by overloading a network, such as in a denial of service attack. *See* NICK GIFFORD, INFORMATION SECURITY: MANAGING THE LEGAL RISKS 7–10 (2009).

7. *See Security Breach Notification Laws, supra* note 3.

8. *See* David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 INTELL. PROP. & TECH. L.J. 5, 6 (2007).

9. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (1914).

10. *See Security Breach Notification Laws, supra* note 3; GEMALTO, FINDINGS FROM THE BREACH LEVEL INDEX, 2015: FIRST HALF REVIEW 3 (2015), http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf [https://perma.cc/AWX6-BV6L].

11. *See* Cardenas et al., *supra* note 4, at 8.

12. Timothy Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J. L. & TECH. 1, 3 (2004).

13. *See* Cardenas et al., *supra* note 4, at 1, 11.

have been compromised.[14] These laws vary from state to state, but all typically define PII as a last name, or first name and last initial, in combination with one of four pieces of unencrypted information: (1) SSN, (2) driver's license or state identification number, (3) account, credit card, or debit card number with any password or code required to access the account, or (4) protected health information, which is any information relating to an individual's health status, health care, or payment for health care.[15] For example, California, a leader in privacy and data security, has an SBN law stating in part:

> Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[16]

The logic behind these disclosure laws is that notification allows the individual to dissociate herself from the stolen PII and essentially walk away from the breach unharmed.[17] For instance, an identity theft victim can cancel credit cards, flag a driver's license, freeze an SSN, or monitor medical information. State SBN laws represent the primary legislative protection for victims of data breaches. In addition, enforcement agencies like the FTC regulate how entities store and manage personal information.

B. FTC REGULATION OF ENTITIES STORING PERSONAL INFORMATION

Congress tasks the FTC with "protect[ing] consumers' personal information and ensur[ing] that consumers have the confidence to take advantage of the many benefits offered in the marketplace."[18] In *FTC v. Wyndham Worldwide Corp.*, the Third Circuit confirmed that the FTC has

14. *See* Silverman, *supra* note 8, at 6.
15. *See id.* at 5; CAL. CIV. CODE § 1798.29(a) (2016).
16. § 1798.29(a).
17. Paul Schwartz and Edward Janger note that, arguably, the primary purpose of SBN laws is "to allow the customer to take steps to safeguard her data." Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 937 (2007).
18. FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE (2014) 2 (2015).

authority to bring enforcement actions against companies regarding their data security practices.[19] The FTC holds a breached entity accountable for achieving a level of data security that is "reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[20] Although in theory hackers could be held accountable for their unlawful actions, it is impractical to do so because identifying, locating, and charging hackers can pose significant practical and jurisdictional concerns.[21]

The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices.[22] The FTC carries out its mission in part by "bring[ing] enforcement actions to stop law violations and requir[ing] companies to take affirmative steps to remediate the[ir] unlawful behavior."[23] The FTC has brought over fifty law enforcement actions against breached entities thus far, all resulting in "settlements—no findings have been made by a court—and the specifics of the orders apply just to those companies."[24] So, while these orders hold the force of law for the specific companies they refer to, they simply provide guidance to other entities.[25]

Under Section 5, the FTC has authority to bring an enforcement action against an entity if the company has deceptive or unfair practices, meaning that "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[26] The FTC has more readily relied on the deception prong, under which it "has developed a theory of deception that not only includes broken promises of privacy and security, but also a general theory of

19. 10 F. Supp. 3d 602 (3d Cir. 2014).

20. *Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/datasecurity [https://perma.cc/3GCC-94XM].

21. Robert J. Sciglimpaglia, Jr., Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 208–11 (1991).

22. PRIVACY AND DATA SECURITY UPDATE (2014), *supra* note 18, at 1; 15 U.S.C. §§ 41–58.

23. PRIVACY AND DATA SECURITY UPDATE (2014), *supra* note 18, at 1.

24. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 1 (2015).

25. *Id.*

26. 15 U.S.C. § 45(n) (2012); *see* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628 (2014).

deception in obtaining personal information and deception due to insufficient notice of privacy-invasive activities."[27]

Importantly, the FTC does not necessarily fault entities for all data breaches; rather, it "usually faults companies for failures to implement promised procedural protections, such as security protocols."[28] Satisfying a showing of deception requires that there be "(1) an act (representation, omission, or practice), (2) the likelihood of a reasonable consumer's deception, and (3) materiality."[29] The "broken promises of privacy and security" language has developed into a key source of authority for the FTC in bringing enforcement actions against entities on the basis of data security concerns.[30] Moreover, under the "general theory of deception" language, the FTC has found companies liable for inducing disclosure of personal information.[31]

By contrast, the FTC has taken a much more limited approach under the unfairness prong.[32] An unfair trade practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[33] In *FTC v. Wyndham Worldwide Corp.*, the Third Circuit held that the FTC has authority under the unfairness prong of Section 5 to bring an enforcement action against a company whose failure to protect sensitive data has resulted in financial harm to consumers.[34]

The FTC also has authority to investigate and prosecute privacy violations under a variety of sector- and information-specific laws.[35] For instance, under the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), financial institutions have an affirmative duty to protect customers' personal information and must provide customers

27. Solove & Hartzog, *supra* note 26, at 628.

28. *Id.* at 630. Likewise, "[e]ven vague promises of security such as providing 'reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information' can be the basis of an FTC action." *Id.* at 636.

29. *Id.* at 628.

30. *Id.* at 628–29.

31. *Id.* at 630.

32. *Id.* at 638 ("The FTC has exercised its unfairness enforcement power judiciously when it comes to privacy and security.").

33. 15 U.S.C. § 45(n) (2012); *see also* Solove & Hartzog, *supra* note 26, at 628.

34. 10 F. Supp. 3d 602 (3d Cir. 2014). For a more in-depth discussion of the FTC's authority to enforce data security, see William J. Binkley, Note, *Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement After* Wyndham, 31 BERKELEY TECH L.J. 1079 (2016).

35. *See* PRIVACY AND DATA SECURITY UPDATE (2014), *supra* note 18, at 5.

with written notice about their privacy practices.[36] Under the Health Insurance Portability and Accountability Act (HIPAA), entities must notify covered individuals of a breach of unsecured protected health information.[37] Further, the Disposal Rule, which applies to entities that receive consumer information such as credit reports and employee background screens, requires that the company "properly dispose of any such information stored on its digital copier, just as it would properly dispose of paper information or information stored on computers."[38]

Importantly, unlike state legislatures, the FTC has not explicitly set out a definition for PII. However, the FTC's treatment of the term suggests that it has adopted a narrow definition comparable to the definition set out in SBN laws.[39] As such, the FTC's treatment of PII does not cover reputation-implicating information. Accordingly, the FTC has yet to bring an enforcement action against a breached entity specifically on the basis of deceptive or unfair practices regarding reputation-implicating personal information, and it has yet to incorporate reputational personal information into its data breach protection framework.

SBN laws and the FTC govern identity theft data breaches. However, privacy tort law can provide a possible framework for governing a relatively new class of data breaches that has emerged in recent years: exposure breaches.

36. Pub. L. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801–6809 (1999)).

37. Pub. L. 104-191, 110 Stat. 1936 (1996). "Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance." *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/AQF9-FG4R].

38. FED. TRADE COMM'N, COPIER DATA SECURITY: A GUIDE FOR BUSINESSES 8 (2010).

39. *See* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 5 (2011) ("Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft."); START WITH SECURITY: A GUIDE FOR BUSINESS, *supra* note 24, at 2 (offering examples of PII throughout the guide, such as "personal data on employment applications to network files with customers' credit card numbers," without setting out a specific definition of PII).

C. PRIVACY TORT LAW

In 1960, William Prosser solidified privacy law into the four "invasion of privacy" torts recognized by the Restatement (Second) of Torts:[40] (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;[41] (2) public disclosure of embarrassing private facts about the plaintiff;[42] (3) publicity which places the plaintiff in a false light in the public eye;[43] and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[44] Most relevant to protection against exposure data breaches is the "public disclosure of private life" tort because it speaks to the private yet truthful nature of the embarrassing information at the center of these breaches. The Restatement (Second) of Torts defines the "public disclosure of private life" tort:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[45]

Courts have determined a matter to "concern[] the private life of another" if the information is not a widely known fact[46] and the plaintiff has retained a reasonable expectation of the privacy of that information.[47] Moreover, the Restatement recognizes "publicity" as communication "to the public at large" or "to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[48] By contrast, communicating the information "to a single person or even a small group of persons" does not constitute "publicity."[49] The means of communication

40. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); RESTATEMENT (SECOND) OF TORTS § 652(b)–(e) (1977).

41. RESTATEMENT (SECOND) OF TORTS § 652(d).

42. *Id.* at § 652(b).

43. *Id.* at § 652(e).

44. *Id.* at § 652(c).

45. *Id.* at § 652(d).

46. *See* Fisher v. Ohio Dep't of Rehab. & Corr., 578 N.E.2d 901, 903 (Ohio Ct. Cl. 1988) (holding that plaintiff telling four co-workers about encounters with her child that carried sexual overtones meant that the information was no longer private).

47. *See* Y.G. v. Jewish Hosp., 795 S.W.2d 488, 502–03 (Mo. Ct. App. 1990) (finding that plaintiffs retained an expectation of privacy because even though hospital employees knew they were pursuing *in vitro* fertilization, they had not told their friends or fellow churchgoers).

48. RESTATEMENT (SECOND) OF TORTS § 652(d) cmt. a.

49. *Id.*

"may be oral, written or by any other means."[50] Further, the "highly offensive to a reasonable person" standard is evaluated according to the relative customs of the time, place, occupation and habits of the plaintiff and "his neighbors and fellow citizens."[51] Interestingly, jurisdictions vary considerably in their interpretations of "custom."[52] Finally, "matters of legitimate concern to the public" are deemed newsworthy and therefore not subject to the tort.[53] So, the tort in its full form would not protect published information that is deemed to be newsworthy as a matter of law.[54] However, because data breach law is focused on protecting *all* stored PII, not just that which is not newsworthy,[55] this prong ought to be reconsidered in this context.

Privacy tort law offers a helpful framework that can be applied to the data breach context. Yet, because applying the "public disclosure of private life" tort in its traditional ex-post sense would not help to prevent reputational harm from occurring in the first place, potential victims would be better protected if the underlying principles of the tort were absorbed into an ex-ante FTC enforcement framework. Accordingly, the "public disclosure of private life" privacy tort may not itself be able to address reputational harm, but it can offer a launching point for coping with the reputational harm that flows from exposure data breaches.

---

50. *Id.*

51. *Id.* at cmt. c.

52. *Compare* Gill v. Hearst Publ'g Co., 253 P.2d 441, 445 (Cal. 1953) (finding that "there [does not] appear to be anything 'uncomplimentary' or discreditable in the photograph" of a young couple showing affection in a confectionary shop), *with* Daily Times Democrat v. Graham, 162 So. 2d 474, 477 (Ala. 1964) (noting that a photo taken of a woman's exposed undergarment would be highly offensive to a reasonable person because she had not consented to the publicity of this involuntary conduct).

53. *Compare* Shulman v. Group W. Prods., Inc., 18 Cal. 4th 200, 228 (Cal. 1998) (finding that the public broadcast of a nurse's private conversation with a patient in an emergency situation was newsworthy because it was germane to the telling of the story), *with* Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1234–35 (7th Cir. 1993) (noting that even though personal facts published in a book were newsworthy because they were germane to the book's subject matter, protection would not extend to publication of "intimate physical details the publicizing of which would be not merely embarrassing and painful but deeply shocking to the average person").

54. *See id.*

55. *See* Schwartz & Janger, *supra* note 17, at 916 (noting that data breach statutes "seek to punish the breached entity and protect consumers by mandating corporate information disclosure" based only on the fact that the data falls into the PII category, and regardless of the data's specific content).

II. UNDERSTANDING EXPOSURE BREACHES

Identity theft continues to make up the largest portion of data breaches,[56] but a new family of breaches is on the rise: exposure breaches. Exposure breaches include both extortion data breaches, which offer simpler methods than identity theft for hackers to make money,[57] and hacktivism data breaches, which offer a means for achieving social or political goals.[58]

A. EXTORTION DATA BREACHES

Although identity theft may be profitable, it is more inefficient and burdensome than an onlooker might anticipate,[59] so some hackers have turned to extortion to profit from data breaches.

1. The Drawbacks of Identity Theft

Identity thieves face two critical drawbacks. First, turning stolen information into tangible cash involves several parties and a significant amount of time and effort.[60] Second, because of the nature of the stolen information, the hacked victim can dissociate herself from the kind of data that identity theft hackers are interested in, which renders the information useless to hackers looking to profit.[61] So, the kind of information identity theft hackers steal generally has only a finite lifespan before the victim dissociates herself from it and it becomes valueless.

Addressing the first drawback of identity theft, a hacker must gain access to the right type of information to profit.[62] There are many types of PII, and a hacker must transform each one from binary code to liquid cash

56. *See* GEMALTO, *supra* note 10, at 3.

57. *See infra* Section II.A.

58. *See infra* Section II.B. Hacking grew out of intellectual curiosity, but as the technological means became available, it developed into a tool to make money and promote social objectives. SUSAN BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES, AND OUTCOMES 17–18 (2012). "The popularization of hacking was the result of two innovations: One was the Internet, a new network that could support an unlimited number of computers and was available to anyone who could log on. . . . The other innovation was the personal computer: though the term first appeared in print in 1962, personal computers did not become a reality until the end of the 1970s." *Id.*

59. *See* Cardenas et al., *supra* note 4, at 2–8.

60. *See id.*

61. *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1248 (2002) (acknowledging that identity theft law "allows individuals to fix the damage caused by identity theft," but that these processes are "complicated by the profound lack of power individuals have over controlling their personal information").

62. *See* Cardenas et al., *supra* note 4, at 3–7.

in a different way.[63] Each of these processes is unique and time-consuming. For instance, the hacker may need to advertise the data through an online bulletin board; create fake credit cards; use the data to withdraw account funds from a local bank branch; file for unemployment benefits or a tax refund; urge banks and stores to open new accounts or make purchases over the phone; or use medical policy numbers, diagnosis codes, and billing information to create fake IDs to buy medical equipment or prescription drugs for resale.[64] In some ways, identity theft simply replaces a lawful nine-to-five job with an illicit one, making it a poor choice for those looking to make easy money.

Addressing the second major drawback of identity theft, a victim can strip the stolen information of its value at any time.[65] PII's economic value comes from its association with the individual victim; once victims learn that their information has been compromised—perhaps thanks to mandatory disclosure policies in place by SBN laws—victims can dissociate themselves from stolen PII.[66] It is true that some PII can be more difficult for victims to dissociate from than others. Cancelling a credit card just takes a phone call, and the payment processor or bank often reimburses the victim for the fraudulent transaction,[67] whereas getting a new SSN requires a more significant showing of fraud.[68] Even so, if the victim can prove that her SSN was stolen and improperly used, the government can place a fraud alert or security freeze on her number and she can monitor her credit reports regularly.[69] Likewise, even though an individual remains associated with her medical information, a victim of a medical data breach can monitor her medical records and related documents to confirm that her files remain accurate.[70] If she recognizes any fraudulent incidents or claims, such as false benefit cards or insurance reimbursement claims in her name, she can

63. *See id.* at 8–9.
64. *See id.*
65. *See* Solove, *supra* note 61, at 1248.
66. *See id.*
67. Moreover, the Fair Credit Billing Act and the Electronic Fund Transfer Act place a cap on the amount of money an individual victim of identity theft can be held liable for following a retailer's data breach, like the one Target experienced in 2013. *See* 15 U.S.C. § 1693(g) (2012); Kara Brandeisky, *4 Reasons Why You Should Shop at Stores That Got Hacked*, TIME, (Oct. 20, 2014), http://time.com/money/3524447/data-breach-target-home-depot-holiday-shopping [https://perma.cc/K3ZK-B97D].
68. *See* PRIVACY RIGHTS CLEARINGHOUSE, *Fact Sheet 17b: How to Deal with a Security Breach*, https://www.privacyrights.org/how-to-deal-security-breach#dl [https://perma.cc/ZRV4-RJRA].
69. *See id.*
70. *See id.*

contact her provider and dissociate from those claims.[71] So, the identity theft hacker's significant investment of time and resources may prove futile in the end.

2. The Ease of Extortion

Extortion breaches solve both of the drawbacks identity theft presents. First, extortion involves fewer steps and is more straightforward than identity theft. Second, and more importantly, victims cannot dissociate themselves from information stolen through extortion breaches.

Unlike identity theft, extortion involves few steps and parties. In order to profit from the hacked information, the extortionist need only communicate to the victim that unless she pays up, the hacker will publicly disclose her embarrassing information. The hacker typically requests payment in a virtual currency that she can then turn into cash.[72] Extortion hackers take advantage of personal information that the data owner would pay to keep private; accordingly, the hacker can demand huge sums in exchange for keeping the information out of the public eye.

Whereas victims of identity theft can dissociate from the stolen information, victims of exposure breaches, including extortion breaches, cannot.[73] Because of the nature of the information exploited in extortion hacks, the hacker does not have to worry that the stolen information will suddenly become useless because it retains its value as long as the victim has an interest in not being exposed. For instance, a hacker can feel confident that unsavory information regarding a potential victim's online browser history will be profitable today as well as ten years from now, particularly if the potential victim chooses to run for public office. Because extortion breach information has a longer life, it is not surprising that hackers are turning to extortion as an alternative or supplement to identity theft hacks.

Moreover, although these extortion data breaches likely come within the legal definition of extortion, this cause of action suffers from the same weakness as SBN laws—addressing reputational harm after the fact is less effective than mandating preventive measures. Extortion typically "consists

71. *See* Laura Shin, *Why Medical Identity Theft is Rising and How to Protect Yourself*, FORBES (May 29, 2015), http://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself [https://perma.cc/39RT-5369].

72. For instance, she may request payment in Bitcoin, which can then be bought and sold for traditional currency while bypassing bank charges and exchange rates. Misha Tsukerman, Note, *The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L.J. 1127, 1147 (2015).

73. *See infra* Section II.A.3 (discussing the Ashley Madison and Sony Pictures breaches as examples).

of a verbal or written or printed communication which is made maliciously and threatens to (1) accuse another of a crime, (2) injure another's person or property, or (3) use unlawfully one's power as a police officer . . . with the intent to extort money or any pecuniary advantage or compel any person to do any act against his will."[74] Courts are divided over whether a threat to a person's reputation or mental well-being constitutes a "threat to the person" within the meaning of federal and state extortion statutes.[75] However, "the weight of modern authority . . . includes a threat to one's mental well-being as a threat of injury to the person."[76] Extortion data breaches would likely be covered by these ex-post extortion laws; yet these laws would not provide an adequate remedy because victims would nevertheless remain permanently and publicly associated with their leaked information. Likewise, the target of these extortion laws, here the hacker, is difficult to locate and charge, so enforcing these extortion laws introduces other practical concerns.[77]

3. Examples of Extortion Data Breaches

The 2015 Ashley Madison breach is a prime illustration of an extortion data breach. In that case, a group of hackers self-titled The Impact Team stole the account and credit card information of thirty million Ashley Madison users who believed they were participating on the adultery website under private and secure conditions.[78] Over the course of several data dumps, the hackers posted the stolen user information online, and reached out to individual users requesting payment in exchange for removing the compromising information.[79] Moreover, once The Impact Team posted the user information online, secondary hackers echoed The Impact Team's efforts and extended the same extortive threats to users.[80] Hackers typically demanded several hundred dollars in Bitcoin in order to keep victims' association with the adultery website private.[81]

Similarly, in December 2014, the hacker group Guardians of Peace (GOP) targeted Sony Pictures Entertainment ("Sony"), and over the course

74. 14A Mass. Prac., Summary of Basic Law § 7:223 (5th ed.).

75. *Id.*

76. Thomas B. Merritt, *Injury to Reputation or Mental Well-Being as Within Penal Extortion Statutes Requiring Threat of "Injury to the Person,"* 87 A.L.R. 5th 715, 715 (2001).

77. *See* Sciglimpaglia, *supra* note 21, at 208–11.

78. David Bisson, *The Ashley Madison Hack—A Timeline (Updated 9/10/15)*, TRIPWIRE (Sept. 1, 2015), http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline [https://perma.cc/N4B3-BVXK].

79. *See id.*

80. *See id.*

81. *See id.*

of several data dumps, released a wide range of private information about the company, its employees, and its partners.[82] The stolen data included the names, addresses, SSNs, bank account and credit card information, medical diagnoses, disability codes, and medical ID numbers of employees; details about Sony's operations and communications; and five Sony films, four of which were previously unreleased.[83] One of the most notorious aftereffects of the hack was the release of extremely sensitive email chains. One included an exchange between Sony executives discussing whether President Obama's favorite films included African-American actors.[84] Another email thread revealed that Sony paid certain top female actresses less than their male counterparts.[85] Accompanying the information dumps were several threatening messages in which GOP promised to continue to disclose private information unless Sony agreed not to release the film *The Interview*.[86] GOP continued to disclose private information until Sony released a statement that it would no longer be releasing the film.[87] Sony postponed the film's release, but ultimately released *The Interview* in select theaters and via Video On Demand.[88]

These two data breaches affected thousands of individuals and several companies and received tremendous media attention. However, hackers can also carry out simple, small-scale extortion breaches. For instance, a hacker could threaten to expose someone's embarrassing browser history, broadcast that the victim shopped at a retailer that might place the individual in a bad light, or expose incriminating email or text messages unless the victim pays up. These disclosures can impact the careers and reputations of politicians, military personnel, and regular citizens.

82. *See* Kaleigh Simmons, *The Sony Data Breach: Full Timeline*, RIPPLESHOT BLOG (Jan. 6, 2015), http://info.rippleshot.com/blog/the-sony-data-breach-full-timeline [https://perma.cc/6U9P-6ZRW].

83. *See id.*

84. *See* THR Staff, *Sony Hack: Amy Pascal and Scott Rudin Joked About Obama's Race in Leaked Emails*, THE HOLLYWOOD REPORTER (Dec. 10, 2014), http://www.hollywoodreporter.com/news/sony-hack-amy-pascal-scott-756438 [https://perma.cc/UXC2-JJ3W].

85. Bryce Covert, *Sony Executive Blames Female Actresses For Their Own Unequal Pay*, THINK PROGRESS (Feb. 13, 2015), http://thinkprogress.org/economy/2015/02/13/3622743/sony-wage-gap-amy-pascal [https://perma.cc/JC49-MFA7].

86. David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501 [https://perma.cc/ERT6-XDBJ].

87. *Id.*

88. *Id.*

Individuals, governments, and businesses today are relaying highly private information over less-than-secure channels. Even though many of these technology users are sophisticated and often recognize that cloud-based applications, email, and instant messaging are not wholly secure pathways, many nevertheless participate in online activities that, if exposed publicly, could harm their reputation. Hackers have recognized the simplicity of extortion hacks, and they will most likely turn to them with growing frequency.

B. HACKTIVISM DATA BREACHES

In hacktivism data breaches, hacktivists engage in hacking for a social or political purpose by exposing private information to harm their victims' reputations.[89] Although the reasoning behind hacktivist attacks can be difficult to discern—they can feel logical, straightforward, and justifiable or appear to make no sense at all[90]—these breaches are analogous to extortion in the broader security breach context. Hacktivists embarrass their victims by disclosing compromising information; moreover, once this information is disclosed, it effectively remains in the public sphere forever.

For example, in 2006, Julian Assange is credited with launching Wikileaks, "an online repository for holding and publishing secret documents by whistle-blowers and journalists."[91] The premise behind the online forum is that "those in possession of confidential documents of public interest, which their governments or institutions wanted to hide from public scrutiny, would be able to upload them anonymously on the website for worldwide circulation and publicity."[92] In another case, the infamous hacker group Anonymous broke into the computer system at Stratfor Global Intelligence, a United States security agency, on Christmas Day in 2011 and exposed client lists, emails, and credit card information.[93] The hackers then used the credit card data to donate to a variety of charities, adding to the confusion around the hackers' motivations.[94]

All exposure breach victims experience the potential for reputational harm, but there are no legal frameworks in place working to prevent these

89. *See* JORDAN & TAYLOR, *supra* note 5, at 1.

90. *See* Dorothy Denning, *Cyberwarriors: Activists and Terrorists Turn to Cyberspace*, 23 HARV. INTL. REV. 70, 70 (2001).

91. *The Brave New World of Wikileaks*, 45 ECON. & POLITICAL WEEKLY 7, 7 (Dec. 11, 2010).

92. *Id.*

93. *See* Nicole Perlroth, *Hackers Breach the Website of Stratfor Global Intelligence*, N.Y. TIMES (Dec. 25, 2011), http://www.nytimes.com/2011/12/26/technology/hackers-breach-the-web-site-of-stratfor-global-intelligence.html [https://perma.cc/4M42-9LHG].

94. *Id.*

breaches from occurring in the first place. There are also no measures that can help make individuals whole once they have been made victims. Privacy tort law is one possible framework that can assist potential exposure breach victims.

III. A NEW LEGAL FRAMEWORK FOR EXPOSURE BREACHES

SBN laws necessarily adhere to an ex-post philosophy where entities are subject to affirmative duties only *after* PII has been compromised, or possibly compromised,[95] but this approach may not be particularly effective in addressing exposure data breaches. Victims of exposure breaches, unlike identity theft victims, face reputational harm that cannot be undone, and ex-post approaches are not capable of preventing this reputational damage from occurring in the first place. Thus, the emergence of exposure breaches calls for more robust ex-ante protocols that may help minimize the occurrence of reputational harm.

Accordingly, one effective measure may be for the FTC to hold entities accountable under a broadened definition of PII. This would put entities on notice of the threat of reputational harm from exposure breaches and incentivize companies to adopt stronger security protocols to limit the occurrence of breaches. In line with this ex-ante approach, state legislatures should consider adopting legislation requiring entities to establish heightened security when they relay reputation-implicating information in the course of business. These ex-ante measures can reduce the number of exposure breaches and thereby prevent reputational harm before hackers have the opportunity to affect people's lives.

A. SBN LAWS AND OTHER EX-POST APPROACHES FAIL TO ADDRESS REPUTATIONAL HARM

Because exposure breaches, unlike identity theft, result in permanent reputational consequences,[96] ex-post approaches to these attacks are not particularly effective. As noted in Section I.A, SBN laws fall under this ex-post approach. First, SBN laws would likely rarely be triggered by the release of exposure breach information because the valuable, reputation-implicating information at the center of exposure breaches could be practically anything, and need not be SBN-triggering PII.

95. *See* Silverman, *supra* note 8, at 6.

96. For instance, compare the reputational harm of being publicly exposed in affiliation with an adultery website with the economic harm and frustration from the leak of a SSN online. *See* Bisson, *supra* note 78; *see also Fact Sheet 17b: How to Deal with a Security Breach*, *supra* note 68.

Second, SBN laws would not correct the reputational harm that flows from exposure breaches. SBN laws do not require the removal of reputation-harming material posted through exposure breaches. Even if they did, they would be of limited use because removing such material from the Internet—and it is questionable whether that is possible—does not remove it from the minds or computers of anyone who saw or downloaded the material. Preventing such material from being posted in the first place is the only way to completely prevent reputational harm.

B. EX-ANTE APPROACHES CAN BETTER ADDRESS REPUTATIONAL HARM

The permanence of disclosed information at the center of exposure data breaches dictates the reliance on ex-ante protocols to help prevent data breaches from occurring in the first place.[97] First, by broadening the FTC's definition of PII and requiring certain entities to adopt the FTC's updated definition of PII as a baseline, the FTC can put entities on notice that it may bring Section 5 enforcement actions for deceptive or unfair practices regarding how entities store and manage reputation-implicating information. Second, state legislatures should consider enacting legislation requiring entities that store data falling into this broadened definition of PII to maintain heightened security measures for storing that data. These ex-ante measures echo the FTC's own statement that "[n]o one can steal what you don't have."[98] While an in-depth discussion of the FTC's authority to bring enforcement actions to protect consumers from reputational harm under the Administrative Procedure Act and other relevant administrative law is beyond the scope of this Note, these proposed measures represent steps toward protecting citizens against exposure breaches.[99]

1. The FTC Should Hold Entities Accountable Under a Broadened Definition of PII

As noted in Section I.B, the FTC's implicitly adopted definition for PII is confined to information at the center of identity theft breaches. However, as demonstrated in Part II, the data underpinning exposure breaches varies drastically from that at the center of identity theft breaches. As such, the FTC should consider formally broadening its definition of PII to more accurately reflect the latest data privacy concerns.

97. For a more in-depth discussion on the distinction between ex-post and ex-ante laws, see Barbara H. Fried, *Ex Ante/Ex Post*, 13 J. CONTEMP. LEGAL ISSUES 123 (2003).

98. FED. TRADE COMM'N, *supra* note 24, at 2.

99. For more background on this debate, see Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979 (2014).

One possibility is to broaden the definition of PII according to the already-accepted "public disclosure of private life" tort proposed by the American Law Institute. Under this approach, one possible definition of PII might be: "any personally identifiable information that concerns the private life of another such that its public disclosure would be highly offensive to a reasonable victim."[100] This definition is particularly well-suited here because it is broad enough to catch the reputation-based information at the heart of exposure breaches, but also sufficiently limited by the objective "highly offensive" standard.[101]

The FTC's formal adoption of this definition can serve two key purposes. First, it can help draw attention to the prevalence and significance of the exposure data breach family. Second, it can provide a launching point for the FTC to update the reach of its Section 5 authority to the modern data security environment. More specifically, the FTC should consider publishing a notice to all companies stating that the term PII, when used by any company in its privacy policies or communications with customers, encompasses the FTC's new, broadened definition as a baseline. This measure would ensure that entities consider consumers' reputational information in their privacy practices and would put companies on notice that the FTC can bring enforcement actions based on the deceptive or unfair treatment of reputational information under its Section 5 authority.

Practically speaking, the FTC should draft an updated data security guide for businesses, perhaps modeled closely on its publication *Start with Security: A Guide for Business*, with the revised definition of personal information in mind.[102] At the highest level, this guide can direct companies' attention toward the threat of exposure breaches. More specifically, it can urge companies to train their employees to identify sensitive information and learn how to manage it. The FTC can continue to emphasize that entities encrypt sensitive data and regularly and securely delete unnecessary information from their servers.[103]

The Ashley Madison breach provides an illustration of how the FTC could exercise this enforcement authority. Prior to the breach, Ashley Madison users were given the opportunity to delete their accounts for

100. *See* RESTATEMENT (SECOND) OF TORTS § 652(d) (1977); *see supra* Section I.C.
101. *See* RESTATEMENT (SECOND) OF TORTS § 652(d).
102. FED. TRADE COMM'N, *supra* note 24.
103. *See id.*

nineteen dollars.[104] However, the data breach demonstrated that while users' email addresses and phone numbers were deleted, their GPS coordinates, gender, ethnicity, relationship status, and other information about the users' sexual interests were not deleted.[105] Under the standard set out above, the FTC might have had authority to hold Ashley Madison accountable for deceptive or unfair practices regarding the storage of this reputation-implicating information.

In sum, by broadening the definition of PII, the FTC can bring awareness to the importance of exposure breaches and more effectively protect consumers.

2. State Legislatures Should Adopt Legislation Requiring Businesses to Implement Heightened Security for PII Used in the Course of Business

In conjunction with the proposed broadened definition for PII, state legislatures should consider enacting legislation requiring businesses to adopt heightened security measures when the information they store or manage in the regular course of business might carry reputation-implicating consequences and be highly offensive to a reasonable victim if disclosed. Legislative action addressing the reputational harms from data breaches can complement legislatures' similar involvement in passing SBN laws. Such action would therefore both strengthen security systems for consumers and validate the existence and significance of exposure data breaches and reputational harm.

The Ashley Madison case provides a relatively clear-cut illustration of how this legislation might look in practice. The company's business model is built on providing a secret forum for users to engage in behavior that would be highly offensive to a reasonable victim if made public.[106] Accordingly, under this statute, Ashley Madison would be required to invoke heightened security protocols for all systems storing or managing PII, according to the FTC's updated definition. These measures might include encryption and regular, secure deletion of unnecessary or archived information.

Likewise, in the Sony case, the embarrassing email correspondence between executives exposing the company's pay discrimination was related

104. Team Register, *What Ashley Madison Did and Did NOT Delete if You Paid $19—and Why it May Cost it $5m+*, THE REGISTER (Aug. 25, 2015), http://www.theregister.co.uk/2015/08/25/us_class_action_ashley_madison [https://perma.cc/V7V6-ML64].

105. *Id.*

106. *See id.*

to Sony's business.[107] Under this proposed legislation, Sony would be responsible for enacting heightened security for these messages.[108] By contrast, under this proposal, Sony may not have been required to more securely store the email correspondence in which Sony executives guessed whether President Obama's favorite films are those starring African-American actors because this correspondence does not relate directly to Sony's course of business.[109]

Given that reputation-implicating information, once released, essentially remains in the public sphere forever, ex-ante data security measures offer a suitable approach to managing exposure data breaches. By focusing on preventing the harms in the first place—via a minor reworking of the FTC's treatment of personal information and comparable state legislative action—ex-ante protocols can reduce data breaches and the reputational harms that flow from them altogether.

3. Addressing Counter-Arguments to Ex-Ante Measures

Admittedly, these ex-ante approaches introduce vagueness and judgment into what has traditionally been a cut-and-dry process of notifying affected parties that their easily defined PII has or could have been compromised. Nevertheless, in practice, the introduction of this case-by-case rule will likely push entities to achieve heightened security for *all* stored data, arguably a beneficial consequence.

The financial costs associated with invoking heightened security measures might pose a significant concern to companies and legislatures. Specifically, smaller, less profitable entities might feel the financial burden of these measures more than large, profit-driven companies. Moreover, this burden might have a chilling effect on start-up companies that are considering entering into data-intensive industries. These are genuine concerns. However, the financial and reputational impacts of data breaches have become increasingly palpable in today's society, and legislatures must allocate these legitimate concerns sufficient weight when balancing interests. In this environment, the financial implications of data security protocols may simply be one of the costs of doing business in a modern market.

---

107. *See* Covert, *supra* note 85.

108. Although this information would likely meet the newsworthiness standard set out in the original public disclosure tort, as noted in Section I.C, because data breach law, unlike privacy tort law, protects the security of data, whether the data here is "of legitimate concern to the public" is beside the point, and the tort should be modified accordingly when used in this context. Data breach law is interested in protecting *any* PII, regardless of its content. *See* Schwartz & Janger, *supra* note 17, at 916.

109. *See* THR Staff, *supra* note 84.

Finally, there is no denying that hackers will likely always find ways to permeate systems and that these data security protocols will need to continually evolve in response to hackers' increasing sophistication. This means that even with these measures, people will continue to be made victims of identity theft and exposure data breach. Although not ideal, the reality of hackers' persistence and sophistication cannot outweigh the costs of trying.

In sum, like practically any data security approach, these ex-ante measures have costs. However, the hacker and data breach realities today call for a more robust security approach, which these ex-ante measures ultimately provide.

C. MAKING VICTIMS OF EXPOSURE BREACHES WHOLE

While ex-ante security protocols help to decrease the incidence of exposure breaches, ex-post measures are well suited to help make individuals whole when they are made victims of an exposure breach.[110] Cyber liability insurance can be one way to do this. Cyber liability insurance can cover a variety of risks related to doing business electronically that may not be covered under commercial general liability policies.[111] By requiring that all entities purchase cyber liability insurance, state legislatures can ensure that exposure breach victims may recover monetarily, even if this cannot fully repair the reputational harm inflicted.

IV. CONCLUSION

Exposure data breaches are one of the latest manifestations of the continually evolving field of cybercrime. Unlike identity theft, exposure breaches result in the public disclosure of private information that implicates reputational concerns for individuals and companies. Because it is impossible to un-ring a bell, an ex-ante approach focusing on establishing strengthened security for all entities storing or managing possibly reputation-implicating information can give individuals the greatest opportunity to live free from the threat of exposure breaches.

The FTC can broaden its treatment of the term PII to accommodate the modern data breach landscape through its Section 5 authority. State legislatures can similarly require all entities storing or managing PII

110. For a more in-depth discussion of the broader legal debate surrounding making tort victims whole, see Stephen D. Sugarman, *Doing Away with Tort Law*, 73 CALIF. L. REV. 555, 591–596 (1985).

111. GPSolo, *Making Cents*, 17 NEGOTIATION 8, 8 (Oct./Nov. 2000). For a more in-depth discussion of cyber liability insurance policies see David R. Cohen & Roberta D. Anderson, *Insurance Coverage for "Cyber-Losses,"* 35 TORT & INS. L.J. 891 (2000).

(according to the FTC's updated definition) in the course of regular business to adopt heightened security protocols. These ex-ante measures can help to build a stronger security framework, and hopefully to minimize the occurrence of exposure breaches. Finally, states can require all entities to enroll in cyber insurance as an additional precautionary measure so that affected exposure breach victims at the very least have an opportunity to recover financially when their personal information is at the center of an extortion breach or hacktivist attack.

The proposed ex-ante framework offers a possible solution to coping with exposure breaches. These breaches will likely play a progressively larger role in the affairs of businesses and individuals as technology continues to evolve, and shifting from an after-the-fact focus to an anticipatory approach is a crucial step in managing these breaches over the long term.