DePaul Law Review

Volume 66
Issue 2 *Twenty-Second Annual Clifford Symposium on Tort Law and Social Policy*

Article 2

Perspectives on Privacy, Data Security, and Tort Law

Robert L. Rabin

PERSPECTIVES ON PRIVACY, DATA SECURITY AND TORT LAW

*Robert L. Rabin**

I. Introduction and Overview

In 2014, did you shop at any of these retailers who had consumer records compromised: Target (70 million records),[1] or EBay (145 million records),[2] or Home Depot (56 million records)?[3] Did you have a health insurance plan through Anthem or Blue Cross prior to 2015 (80 million records)?[4] Did you have a bank or credit card account with JP Morgan Chase prior to 2015 (83 million records)?[5] Have you applied to work in the federal government in the past fifteen years (21.5 million records)?[6] If you answered Yes to any of these questions, there is a good chance that your personal data has been stolen, leaked, exposed, or otherwise revealed to an unauthorized third party as part of a data breach.

Since 2005, more than 900 million records have been improperly exposed or accessed as a result of 5.041 million data breaches in the United States alone.[7] In 2015, $15 billion was stolen from 13.1 million American consumers who were victims of identity theft, much of

---

* A. Calder Mackay Professor of Law, Stanford Law School. My appreciation to Peter Davis and Natalie Lin for valuable research assistance.

1. Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times (Jan. 10, 2014), http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

2. Nicole Perlroth, *EBay Urges New Passwords After Breach*, N.Y. Times (May 21, 2014), http://www.nytimes.com/2014/05/22/technology/ebay-reports-attack-on-its-computer-network.html?_r=0.

3. Nicole Perlroth, *Home Depot Says Data from 56 Million Cards Was Taken in Breach*, N.Y. Times (Sept. 18, 2014, 6:00 PM), http://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach/.

4. Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. Times (Feb. 5, 2015), http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html; *see also How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services*, Anthem, https://www.anthemfacts.com (last visited Aug. 8, 2016).

5. *Id*.

6. Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

7. *Chronology of Data Breaches*, Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breaches (last visited Aug. 8, 2016).

which could be traced back to data breaches.[8] Corporations and governments also suffer: In 2014, the estimated cost per record lost or stolen due to data breach was $145.[9] Given that over 85 million records were lost or stolen in 2014,[10] corporations undoubtedly face substantial costs from data breaches. Even apart from data breaches, consumers face privacy risks from the misuse or misappropriation of their data by corporations.[11]

Data breaches can be traced to three main causes: (1) malicious or criminal attack; (2) system glitch or malfunction; or (3) human error.[12] In 2014, approximately 47% of data breaches resulted from malicious or criminal attacks, 29% from system glitches, and 25% from human error.[13] Breaches due to malicious attacks were more expensive to resolve ($170 per record) compared to those that stemmed from glitches ($142 per record) or human error ($137 per record).[14]

Certain industries are more affected by data breaches than others.[15] In 2014, 42% of data breaches stemmed from the education sector, though these breaches only resulted in 9.7% of the total number of exposed records.[16] In the same year, 33% of the total number of breaches came from the business sector (not including finance or healthcare), but these breaches resulted in nearly 80% of exposed records.[17] The remaining breaches fall within the financial, healthcare, or government sectors.[18] Unsurprisingly, data breaches affect each of these industries differently. The education and healthcare sectors, for example, suffer the greatest costs-per-record-per-breach, at

8. *Identity Theft and Cybercrime*, INS. INFO. INST., http://www.iii.org/fact-statistic/identity-theft-and-cybercrime (last visited Aug. 8, 2016).

9. PONEMON INST., 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (2015) [hereinafter 2015 COST OF DATA BREACH STUDY], https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf.

10. *See Identity Theft and Cybercrime*, *supra* note 8.

11. *See, e.g.*, Elizabeth Blosfield, *Dangers in Data Collection: How Much Is Too Much?*, INS. J. (Oct. 24, 2016), http://www.insurancejournal.com/magazines/coverstory/2016/10/24/429763.htm. For purposes of this Article, a data breach is defined as the unauthorized disclosure of private personal information. Generally, this personal information includes an individual's name combined with another piece of confidential or private information, such as a social security number, credit card number, or piece of medical information. Sasha Romanosky, David Hoffman, and Alessandro Acquisti use a similar definition in their paper, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL L. STUD. 74, 80 (2014).

12. 2015 COST OF DATA BREACH STUDY, *supra* note 9, at 2, 10.

13. *Id*. at 10.

14. *Id*.

15. *Id*. at 9.

16. *Data Breaches Pose a Threat Across All Industries*, CSID, https://www.csid.com/resources/stats/data-breaches-by-industry/ (last visited Aug. 8, 2016).

17. *Id*. This disparity can be the product of more records exposed per breach.

18. *Id*.

$300 and $363 per record respectively, where the average cost per record released for any given data breach is around $154.[19]

Estimating the effects of a data breach on individual consumers is more difficult. As noted, an increasing number of Americans have become victims of various forms of identity theft, which often results in monetary loss and a decrease in an individual's credit score. Beyond identity theft, data breach victims are likely to feel that they need to mitigate future harm by replacing credit cards, closing accounts, and obtaining continuous credit monitoring. At a more basic level, consumers who have been victims of data breaches feel that their privacy has been violated. Little survey work has been published on these subjects, but it seems beyond dispute that data breaches have tangible effects that are widely felt among the American population.

Several recent cases help illustrate the risks and challenges posed by data breaches. During the 2014 holiday shopping season, hackers stole at least 70 million records from Target.[20] Hackers obtained credit card information from 40 million consumers who shopped at Target between November 2014 and December 2014 by installing malware on Target's systems. The same hackers also stole up to 70 million additional customer records, including mailing and email addresses, phone numbers, and names.[21] In the months following the data breach, it was revealed that Target's security system—installed by the well-reputed computer security firm FireEye—detected the breach before any data had been stolen.[22] For somewhat unexplained reasons, Target's security officials declined to intervene—in fact, they had even turned off a FireEye feature that would have automatically deleted the malware from the system (again for unexplained reasons).[23] The result of this reportedly conventional and relatively unsophisticated malware attack was the loss of 70 million records, touching nearly one in three American consumers.[24] Target did not realize that it had been hacked until federal law enforcement officials notified them on December 12, 2014, by which time it was too late.[25]

In July 2015, the White House revealed that the records of 21.5 million people were stolen as a result of a data breach of the Office of

19. *Id*.; *see also* 2015 COST OF DATA BREACH STUDY, *supra* note 9, at 9.

20. Harris & Perlroth, *supra* note 1.

21. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014, 9:31 AM), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p3.

22. *Id*.

23. *Id*.

24. *Id*.

25. *Id*.

Personnel Management (OPM).[26] "Every person given a [federal] government background check for the last 15 years was probably affected," according to OPM.[27] Hackers were able to steal names, social security numbers, biometric fingerprint data, travel information, addresses, and other sensitive personnel information as part of the OPM data breach.[28] As in the Target case, there were warning signs over a period of years indicating that OPM's computer systems were antiquated and at serious risk of intrusion, yet no action was taken to secure the vast amount of personal data until it was too late.[29] The hack has since been blamed on elements associated with the Chinese government.[30] The U.S. government has provided victims with credit and identity theft monitoring for three years,[31] but this likely provides little comfort to national security experts concerned about the potential intelligence ramifications of government employees' sensitive personnel files in the hands of the Chinese government. The OPM case shows that the negative effects of data breaches go far beyond identity theft and monetary loss.[32]

Anthem, one of the largest health insurers in the United States, suffered a data breach in 2015 that resulted in the exposure of 80 million patients' records, including "names, social security numbers, birthdays, addresses, emails and employment information."[33] There was no evidence that sensitive medical records were stolen as part of the breach, but the loss of protected personal information was substantial. Investigators suspect that Chinese state-sponsored hackers were behind the Anthem breach as well.[34] As in the OPM case, Anthem has provided victims with credit monitoring and identity theft protection.[35]

Consumers face threats to their personal privacy wholly separate from the types of unauthorized data breaches described above. Most

---

26. Davis, *supra* note 6.

27. *Id.*

28. *Id*.

29. *Id*.

30. *Id*.

31. *Id*.; *see also* Michelle Singletary, *What to Do If You Are Affected by the OPM Data Breach*, WASH. POST (Dec. 11, 2015), https://www.washingtonpost.com/business/get-there/what-to-do-if-you-are-affected-by-the-opm-data-breach/2015/12/09/534455e0-9dd0-11e5-a3c5-c77f2cc5a43c_story.html?utm_term=.0a96cd4ab495.

32. Davis, *supra* note 6.

33. Abelson & Goldstein, *supra* note 4.

34. Michael Riley & Jordan Robertson, *Chinese State-Sponsored Hackers Suspected in Anthem Attack*, BLOOMBERG (Feb. 5, 2015, 5:40 PM), http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack.

35. *See supra* note 4 and accompanying text.

notably, consumers face risks that their personal privacy will be violated by unauthorized corporate access, misuse, or misappropriation of their data.[36] These claims of corporate misconduct can be grouped under a separate umbrella of "data misuse" issues. Data breaches relate to the *unauthorized* access to personal information by a third party. Data misuse or misappropriation, by contrast, involves the *authorized*—at least at some level—access to information by the party that holds that information for unauthorized commercial or other purposes.

Statistics on the scope of this problem are hard to come by, given the less public nature of the problem and the less tangible and immediate nature of the harm. In many cases, corporations sell or transfer consumer data to a third party without clear authorization from the consumer. One prominent example was the ChoicePoint debacle of 2005.[37] In that case, ChoicePoint, a prominent data trader, admitted to selling personal information of 163,000 California residents—which they possessed legally—to identity thieves.[38] At least 800 consumers had their identities stolen because of this incident.[39] This case raised difficult data privacy dilemmas: ChoicePoint existed to sell personal information to legitimate businesses, but instead, they provided this information to a ring of identity thieves who had registered fake companies.[40] The Federal Trade Commission's (FTC) enforcement action resulted in a $15 million settlement, which was the largest civil penalty in the FTC's history at that time.[41]

In addition to improper sales to a third party, some data misuse cases focus on a corporation's use of consumer data for its own purposes—generally to provide targeted ads or products to consumers. In 2012, it was revealed that Google had placed tracking cookies on Safari users' computers to collect data on their web browsing preferences in order to provide targeted advertisements.[42] Google then

36. Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 143, 150 (2006).

37. *Id*. at 154.

38. *Id*. at 154–55.

39. Bob Sullivan, *ChoicePoint to Pay $15 Million over Data Breach*, NBC NEWS (Jan. 26, 2006), http://www.nbcnews.com/id/11030692/ns/technology_and_science-security/t/choicepoint-pay-million-over-data-breach/.

40. *Id*.

41. *Id*.

42. *See* Claire Cain Miller, *F.T.C. Fines Google $22.5 Million for Safari Privacy Violations*, N.Y. TIMES (Aug. 9, 2012), http://bits.blogs.nytimes.com/2012/08/09/f-t-c-fines-google-22-5-million-for-safari-privacy-violations/. Some brief technical background: Safari is a popular web browser, used by millions of consumers to surf the Internet. Cookies are small files created and used by companies like Google to track the habits of Internet users. When a user visits a Google

used this information to better target ads to users, in turn making their ad products more valuable to potential ad buyers.[43] Presumably in response to consumer pressure, Safari, an Apple browser, created a tool to limit both the creation of cookies and the ability of cookies to track web browsing habits.[44] In violation of a previous FTC settlement and its public pronouncements, however, Google proceeded to override the Safari tool and continued to use cookies to track Safari users.[45] The result was extended litigation that eventually resulted in a $22.5 million FTC settlement.[46]

A similar case was brought against Facebook for its use of members' images in targeted advertisements known as "Sponsored Stories."[47] Unlike the case against Google, this was not a regulatory action brought on unfair competition grounds, but rather a class action brought on Right of Publicity grounds. The principal claim in this case, *Fraley v. Facebook, Inc.*[48]—which is discussed further in the next section—was that Facebook misappropriated the plaintiffs' images in paid advertisements without consent, and in so doing, unwillingly drafted them as unpaid and unknowing spokespersons for Facebook products.[49] After the court denied Facebook's motion to dismiss on newsworthiness grounds, the parties settled for $20 million.[50]

Despite the successes just mentioned, the continuing problems of data breaches, data misuse, and the consequent failure of current laws to adequately deal with the problems is widely acknowledged. Notwithstanding the widespread recognition of the problems, there is little consensus on the appropriate legal mechanisms to prevent or punish data breaches or provide compensation to those harmed by such breaches. This Article surveys one approach to dealing with these problems: The pathways available through tort law.

But tort, of course, is not the only strategy for addressing the data breach concerns. Current legal approaches to dealing with data breaches can be divided into three main categories. First, regulatory strategies aimed at setting standards of data protection through state

page, for example, it might create a cookie that can then follow the user around the web to track web browsing habits.

43. *Id*.

44. United States v. Google, Inc., No. CV-12-04177 SI, 2012 WL 5833994, at *1 (N.D. Cal. Nov. 16, 2012).

45. *Id*.

46. *Id*. at *2; *see also* Miller, *supra* note 42.

47. 830 F. Supp. 2d 785, 790 (N.D. Cal. 2011).

48. *Id*.

49. *Id*. at 814.

50. *Id*. at 815; *see also* Jesse Koehler, Note, Fraley v. Facebook*: The Right of Publicity in Online Social Networks*, 28 BERKELEY TECH. L.J. 963, 964 (2013).

and federal laws, and enforced either through the courts or federal administrative agencies. Second, information disclosure laws that require entities suffering data breaches to reveal to victims that their information has been lost or stolen, with the general hope that the market will favor companies with fewer breaches and thus provide competitive incentives for companies to protect data.[51] And finally, ex post tort liability that allows victims to sue for damages, with the twofold goal of compensating victims and shifting the incentives of companies holding private data toward better data protection practices.

Before turning to tort (the third of these approaches), I will provide an overview in Part II of the regulatory enforcement and information disclosure strategies for addressing the problem of data breach. And following my assessment of tort remedies in Part III, I will offer some concluding thoughts, in a final Part, including a brief reprise on the potential for more proactive federal regulatory action under the mandate of the FTC.

II. Regulatory Enforcement and Information Disclosure Laws

A. Regulatory Enforcement: Preventing and Responding to Data Breaches

Regulatory enforcement at the federal level typically takes one of two forms. First, federal agencies use enforcement actions or rulemaking to influence the data security practices of corporations within the federal agency's mandate. The enforcement activities of the FTC, the Securities and Exchange Commission (SEC), the Federal Communications Commission (FCC), and the Consumer Financial Protection Bureau (CFPB) illustrate this approach. The second is the imposition of criminal sanctions and other penalties for the access, disclosure, or theft of personal information.

The FTC prosecutes data breaches as "unfair and deceptive trade practices" under section 5 of the Federal Trade Commission Act[52]—a strategy that has elements of both ex ante and ex post regulation.[53] The FTC does not have the power to directly fine companies for un-

51. This taxonomy of legal approaches to data breaches comes from Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 Berkeley Tech. L.J. 1061, 1067–68 (2009).

52. Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012).

53. For a comprehensive article examining the FTC's authority in this realm, see Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 Admin L. Rev. 127 (2008).

fair practices, but its enforcement actions "typically result in consent decrees that prohibit the company from future misconduct and require audits for up to 20 years."[54] The FTC can then fine businesses if they violate a consent decree.[55] As I will discuss further in Part IV, in 2015, the Third Circuit affirmed that the FTC has the power to regulate cybersecurity policies through section 5, thus putting the agency's enforcement of data security laws on solid legal ground.[56] The FTC also protects consumer privacy by regulating financial institutions under the Gramm-Leach-Bliley Act.[57] Under this Act, the FTC requires financial institutions to maintain safeguards over their customers' data and disclose to customers any release of that information to third parties.[58]

The FCC has also stepped up its enforcement in response to data breaches over the past five years. In 2015, the FCC reached a $25 million settlement with AT&T based on AT&T's unauthorized access to personal customer information.[59] The FCC bases its enforcement authority on its interpretation of privacy provisions in section 222 of the Communications Act and "unjust and unreasonable practices" under section 201(b) of the Act.[60] Through its actions, the FCC has made clear that it expects Internet providers to "take 'every reasonable precaution' to protect their customers' data."[61]

The SEC and the CFPB have also stepped up enforcement of data security practices, within their mandates, to prevent and respond to breaches—the SEC targeting publicly traded companies and the CFPB targeting financial companies. In fact, the CFPB brought its first enforcement action under the Dodd-Frank Act for unfair or deceptive practices on March 2, 2016, against Dwolla Inc., a digital payment company.[62] Unlike the FTC, the CFPB has the statutory

54. Todd H. Greene et al., *A Crash Course in Data-Security Regulation and Litigation*, ACC DOCKET, Sept. 1, 2015, at 92, 94.

55. *FCC Continues Aggressive Action on Data Breaches*, COOLEY (Apr. 9, 2015), https://www.cooley.com/news/insight/2015/fcc-continues-aggressive-action-on-data-breaches.

56. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

57. *See* Scott, *supra* note 53, at 173.

58. *Id*. at 173–74.

59. *FCC Continues Aggressive Action*, *supra* note 55.

60. Privacy of Customer Information, 47 U.S.C. § 222 (2012); Service and Charges, 47 U.S.C. § 201(b) (2012).

61. *FCC Continues Aggressive Action*, *supra* note 55; *see also* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TULANE J. TECH. & INTELL. PROP. 45, 54 (2015).

62. *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices*, CONSUMER FIN. PROT. BUREAU (Mar. 2, 2016), http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

authority to directly fine companies that violate Dodd-Frank's provisions governing unfair business practices, including those related to data security.[63]

The U.S. Department of Health and Human Services (HHS) enforces various federal laws, including the Health Insurance Portability and Accountability Act (HIPAA),[64] and issues regulations regarding the privacy and security of personal health records. HHS has brought enforcement actions to ensure compliance with these requirements.[65] As will be noted below, HHS also mandates certain data breach notification rules pursuant to HIPAA.

Given the lack of comprehensive federal regulation, however, state law has come to play an important role in preventing and responding to data breaches. State privacy laws of California and Massachusetts are illustrative of the more privacy-protective schemes. Four laws form the backbone of California's strategy. First, the Shine the Light Law requires companies to disclose to consumers the details of any third parties with whom they have shared the consumer's personal information.[66] Second, the California Online Privacy Protection Act of 2003 requires operators of commercial websites that collect personal information to devise a privacy policy and make that policy conspicuously available to site users,[67] and the company's privacy policy must explain the types of personal information collected by the website, how users can request changes to the collected information, and how users will learn about changes to the policy, among other requirements.[68] Third, the recently expanded Data Security Law[69] requires all companies that maintain customer information to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[70] Fourth, California has a widely-criticized but nevertheless im-

63. Yuka Hayashi, *CFPB Fines Fintech Firm Dwolla over Data-Security Practices*, WALL ST. J. (Mar. 2, 2016, 5:05 PM), http://www.wsj.com/articles/cfpb-fines-fintech-firm-dwolla-over-data-security-practices-1456956326.

64. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C and 42 U.S.C.).

65. *See Data Breach Results in $4.8 Million HIPAA Settlements*, DEP'T. OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Aug. 9, 2016).

66. CAL. CIV. CODE §§ 1798.83–1798.84 (West, Westlaw current through 2016).

67. CAL. BUS. & PROF. CODE §§ 22575–22579 (West, Westlaw current through 2016).

68. *Id.*

69. CAL. CIV. CODE § 1798.81.5.

70. *Id.*

portant data breach notification law.[71] Outside of these four core statutes, California also has a multitude of specific statutory provisions setting protection standards for certain types of data and certain categories of businesses.[72] Companies that violate these laws may be subject to suit by the California Attorney General.[73] In all, this scheme is typical of the state schemes most protective of privacy.

Massachusetts is one of the few states with even more restrictive laws than California. Like California, it requires companies to implement reasonable security measures and disclose breaches to affected parties; however, it goes one step further: It requires companies to devise a business "information security program" and defines specific security elements for each program based on the size and type of business.[74] These elements include the encryption of personal information under certain circumstances and various administrative, technical, and physical safeguards.[75] This law is one of the few that is preventative, rather than merely reactive, and it requires specific data security measures of companies managing personal information within the state.[76]

B. Information Disclosure

Data breach notification laws are a regulatory strategy that deserves separate consideration. The federal government has various data breach notification regulations, including, for example, HIPAA's Breach Notification Rule.[77] The FTC also has similar rules that it applies to certain types of corporations. Most importantly, forty-seven states have passed data breach notification laws.[78] California requires companies to notify victims of a data breach "in the most expedient time possible and without unreasonable delay."[79] Many other states use similar language, though several mandate a specific time frame,

71. *Id*. § 1798.29.

72. For a list of all of California's privacy laws, see *Privacy Laws*, CAL. DEP'T JUST. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/privacy-laws (last visited Aug. 9, 2016).

73. Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CAL. 229, 241 (2015).

74. Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2016).

75. *Id*.; *see also* Greene et al., *supra* note 54, at 102.

76. Most states also maintain consumer protection laws that can be applied to data breaches under certain circumstances, but these laws are mainly about ex post liability rather than ex ante regulation.

77. 45 C.F.R. §§ 164.400–164.414 (2016); *see also Breach Notification Rule*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Aug. 9, 2016).

78. Wooten, *supra* note 73, at 237 & n.57.

79. CAL. CIV. CODE §§ 1798.29(a), 1798.82(a) (West, Westlaw current through 2016).

for example, a 30-day period within which notification must be completed.[80] As amended in 2014, California's notification statute also requires that companies subject to data breaches provide free credit monitoring to victims for at least one year.[81]

While data breach notification laws serve as a type of ex post regulation, they also have a broader purpose: promoting a competitive and transparent market for business services involving personal data. The hope is that data notification laws help publicize which companies are protecting individuals' data and which companies are failing to protect individuals' data, leading consumers to patronize the data-protecting companies, and in turn putting competitive pressure on companies with the worst data security to turn things around.[82] Of course, this assumes that consumers make decisions about where to shop or store their information based on a company's history of data breaches—not an outlandish notion, but certainly a contestable one.

C. Shortcomings with Current Approaches

The current legal regime governing data breaches suffers from three main problems: (1) uncompensated victims; (2) inadequate incentives for companies and governments to invest in data security; and (3) uncertainty for corporations with respect to their regulatory burdens and litigation risk. Any proposal to fix the legal regime surrounding data breaches must address each of these three flaws if it is to succeed.

Given the massive increase in data breaches over the past decade, it is clear that the current patchwork of regulatory strategies has failed to prevent data breaches across a wide sector of entities, whether financial, medical, governmental, or educational. The more important question is why have these regulatory efforts failed? As the earlier discussion indicates, there simply has not been any systematic effort to address the data breach problem from a regulatory perspective. First, there is no comprehensive federal regulatory scheme governing data breaches. Instead, one finds different agencies attempting to regulate data breach within their narrow jurisdictions with little coordination and certainly no standardization. The FTC is the only body that truly stretches across industries in its ability to regulate, but it faces other challenges in its mission; in particular, the FTC regulates data breaches solely as "unfair and deceptive business practices," rather than as simply insufficient measures relative to general industry data

80. Tschider, *supra* note 61, at 70 & n.118.
81. CAL. CIV. CODE § 1798.82(d)(2)(G).
82. Romanosky & Acquisti, *supra* note 51, at 1074–75.

security standards or aspirational "best practices."[83] Second, administrative agencies tend to regulate data breaches only through individual enforcement actions and without the issuance of clear rules and standards. Such individual enforcement diminishes the efficacy of regulation more broadly. In addition, individual enforcement leads to uncertainty among businesses regarding the appropriate standards for data security and whether they will in fact be subject to an enforcement action in any given situation. Third, agencies are often forced to stretch their statutory mandates to reach the type of conduct at issue in data breach cases. These limited mandates prevent broader regulation of data security, and they may even focus on the less relevant portions of industry conduct leading to a data breach. Of course, even if the regulatory systems were more robust, they would largely elide the concern for compensating victims of data breaches when they nonetheless occur.

Given that current strategies for data protection tend to be inadequate in addressing the underlying harms of the breach itself, tort law, in its many guises, warrants examination to determine its potential role in the data breach field. Tort theories are especially inviting in this realm (for exploration at least), as they have been applied to protect against certain dignitary and privacy harms that stem from the disclosure of personal information. Furthermore, successful application of tort principles would mean that consumers would have wider opportunities to pursue a legal course of action, hence incentivizing firms to take better care of their data and avoid suboptimal practices.

III. Tort Law and Data Security

This Part analyzes the forms of responsibility recognized in privacy and negligence law that might apply to protecting privacy interests harmed by corporate failure to secure personal data.

A. The Privacy Torts

On the surface, common law torts devoted to protection of privacy would seem a natural fit for securing a remedy to victims of corporate data breach. One need only view the doctrinal headings of the principal related privacy torts to generate positive expectations: public disclosure of private facts, intrusion upon seclusion, and appropriation of name or likeness.[84] Beneath the surface, however, the promise of re-

83. *About the FTC*, Fed. Trade Comm'n, https://www.ftc.gov/about-ftc (last visited Jan. 21, 2017).

84. *See* Restatement (Second) of Torts §§ 652B, 652C, 652D (Am. Law Inst. 1977).

medial relief is quickly called into question. Let me briefly explore, in turn, each of these privacy torts as remedial strategies.[85]

1. Public Disclosure of Private Facts

The cornerstone of this tort can be sketched out from consideration of two leading opinions: *Sidis v. F-R Publishing Corp.*[86] and *Haynes v. Alfred A. Knopf, Inc.*[87] In *Sidis*, a child prodigy who had attained notoriety for his mathematical skills became an eccentric recluse in later life, far-removed from the world of public exposure—that is, until the New Yorker Magazine ran a "where is he now" column recounting his idiosyncratic interests and mannerisms.[88] His suit for public exposure of private facts was dismissed by the Second Circuit Court of Appeals on the ground that there was a newsworthy interest in how the life of a much-heralded boy genius unfolded.[89]

Haynes involved a more scholarly venture. The plaintiff and his ex-wife were the subject of a narrative as part of a far wider historical examination in *The Promised Land: The Great Black Migration and How It Changed America*,[90] a study of the mass movement from the South to northern cities like Chicago during World War II and the post-war era.[91] The plaintiff was depicted by his ex-wife as a man who drank heavily, neglected his children, could not keep a job, was unfaithful, and eventually left her for another woman—a real ne'er-do-well.[92] Mortified by this exposure of his earlier life, Haynes, who took great pride in his later turnabout that led to a life of respectability, claimed invasion of privacy—again for public exposure of private facts.[93] Once again, the claim was denied—this time by the Seventh Circuit Court of Appeals—on newsworthiness grounds.[94]

Distinct as these two settings are, they both fall prey to the roadblock that has undercut the promise of the public disclosure of private facts tort—the newsworthiness defense—harking back to Warren and

85. For another approach to the tort issues discussed in this section, see Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805 (2010).

86. 113 F.2d 806 (2d Cir.1940).

87. 8 F.3d 1222 (7th Cir. 1993).

88. *Sidis*, 113 F.2d at 807.

89. *Id*. at 809–11.

90. *See generally* NICHOLAS LEMANN, THE PROMISED LAND: THE GREAT BLACK MIGRATION AND HOW IT CHANGED AMERICA (1991).

91. *Haynes*, 8 F.3d at 1224.

92. *Id*. at 1224–30.

93. *Id*. at 1229.

94. *Id*. at 1233–35.

Brandeis's classic article, *The Right to Privacy*.[95] The defense is set out as an element of the tort in William Prosser's authoritative Restatement Section 652D, requiring that the "matter publicized . . . is not of legitimate concern to the public."[96]

At this initial crossroad, the lack of fit of the public disclosure tort as a tool for protection against unwarranted personal data disclosures becomes immediately apparent. Corporate entities maintaining data files are simply not defendants analogous to the mass media sources targeted in virtually all of the public disclosure case law. In sharp contrast, corporate defendants have failed to adequately *secure* the victim's privacy, rather than engaging in *publication* of the private information. Indeed, publication of the information is precisely what the corporate defendants, have sought, however inadequately, to avoid.

2. Intrusion upon Seclusion

A leading case in the intrusion tort case law is *Nader v. General Motors Corp.*,[97] in which the New York Court of Appeals approvingly stated that the plaintiff, who had been subjected to General Motors' efforts to discredit him as a critic of auto safety, had a colorable claim for the securing of private information about his financial affairs.[98]

Here, the self-evident problem is one of the misplaced defendant. The tort is inapt for claims against corporate defendants in data breach cases because the focal point of the tort is on improper access to the victim's private information. That would be quite appropriate, of course, in a tort action against the hacker who gains access to the data; however, the claim against the corporate defendant is for failure to *protect against* access, not the improper eliciting of private information.

3. Appropriation of Name or Likeness

A major exception to the misguided path of privacy law involves claims that the corporate defendant has sold or otherwise provided private information to third-party commercial advertisers (or appropriated the information for its own commercial use).[99] Note that this

95. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

96. RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

97. 255 N.E.2d 765 (N.Y.1970).

98. *Id*. at 765–71.

99. The appropriation tort is grounded in RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977).

claim does not address harms like identity theft arising from inadequate security of personal data. But it is fertile ground for privacy tort claims of informational trafficking.

A leading example, is *Fraley v. Facebook, Inc.*,[100] where the court recognized that the defendants had a privacy right vested in California's "right to publicity" statute,[101] which—like the tort of commercial appropriation—establishes liability when the defendant makes use of "another's name, voice, signature, photograph, or likeness for advertising or selling or soliciting purposes."[102] The plaintiffs alleged that the defendants used their personal information, including names and photos obtained from their Facebook accounts, in paid advertisements without the plaintiffs' consent.[103] Although the case was eventually settled, it demonstrates a way in which plaintiffs who are victims of data breaches might arguably bring a privacy action to protect their interests. The limitation of the tort is evident, however—it is reliant on the plaintiff's ability to show loss of economic opportunity and profits that the defendant gained instead through its inappropriate dissemination of private data.[104] In *Fraley*, the court noted that the plaintiff's claim could go forward because they were able to allege injuries that were not just hypothetical or potential, but were instead "concrete and particularized" with respect to each individual plaintiff.[105]

This distinction weighed heavily in subsequent cases such as *Rojas-Lozano v. Google, Inc.*,[106] in which the court granted a motion to dismiss because the plaintiffs were unable to show that their private data was used in a manner for which a reasonable consumer would have expected compensation.[107] The plaintiff brought charges of unfair or deceptive practices and unjust enrichment against Google for profiting off of users' "free labor" in its "reCAPTCHA" program during Gmail sign-ups.[108] The reCAPTCHA program, which users were told served to distinguish between human users and automated programs,

100. 830 F. Supp. 2d 785 (N.D. Cal. 2011).

101. *Id*. at 796.

102. *Id*. at 796–97; *see* CAL. CIV. CODE § 3344 (West, Westlaw current through 2016).

103. *Fraley*, 830 F. Supp. 2d at 790.

104. Ironically, this tort in fact traces its origins to a non-commercial setting. In *Roberson v. Rochester Folding Box Co.*, defendant, a flour manufacturer, reproduced a likeness of the plaintiff, an attractive young woman, on its advertising posters. 64 N.E. 442 (N.Y. 1902). Plaintiff sued (unsuccessfully) for the humiliation and emotional distress from this invasion of her privacy. *Id*. at 443.

105. *Fraley*, 830 F. Supp. 2d at 797.

106. 159 F. Supp. 3d 1101 (N.D. Cal. 2016).

107. *Id.* at 1106–08, 1113.

108. *Id.* at 1107–08.

displayed two words: one that was used for security purposes, and one that Google's character recognition technology used to assist in digitalization of books.[109] Essentially, Google made use of its users' human input as a part of its transcription service to generate revenue. The court rejected the plaintiff's attempt to analogize to *Fraley*, as the plaintiff failed to show that "the few seconds it takes to type a second word is something for which a reasonable consumer would expect to receive compensation."[110]

Thus, while plaintiffs have a significantly greater chance of at least surviving a motion to dismiss when invoking the privacy tort of commercial misappropriation, their claims would require them to be able to show that use of their personal data generated some economic profit to which they were entitled.[111] Once again, note, however, that this data security issue is quite distinct from a defendant's failure to adequately secure plaintiff's private information from outside meddling.

B. Conversion and Trespass to Chattels: Old Wine in New Bottles

Putting aside commercial appropriation, the discussion above suggests that traditional privacy torts are generally inadequate to address harms to individual privacy stemming from a corporate data breach. However, torts outside of the standard privacy claims have been applied in attempts to protect privacy interests in the digital data context.

1. Conversion

Conversion, which traditionally protected ownership rights over physical property, has been extended to protect owner rights over digital information as well. Conversion imposes liability upon the intentional assertion of control over another's property so as to interfere with the property owner's right to control it,[112] and some courts have held that this protection extends to computer records and data. In *Thyroff v. Nationwide Mutual Insurance Co.*,[113] the New York Court of Appeals recognized conversion when the defendant prevented the plaintiff from accessing his electronic records stored on the defen-

109. *Id.* at 1106.

110. *Id.* at 1115.

111. *See* Robinson v. HSBC Bank USA, 732 F. Supp. 2d 976, 987, 990 (N.D. Cal. 2010) (dismissing claim against bank for unauthorized use of photos of plaintiff's residence for advertising purposes on grounds of no economic loss/no standing to sue).

112. RESTATEMENT (SECOND) OF TORTS § 222A (AM. LAW INST. 1965).

113. 864 N.E.2d 1272 (N.Y. 2007).

dant's system, noting that it made little difference whether the information was on physical paper or was intangible as computer data.[114] By preventing Thyroff from exercising his ownership over his own records, the defendants had effectively converted his property.[115] It should be noted that the *Thyroff* conception has not been adopted by every jurisdiction; some courts have maintained that conversion applies only to tangible property.[116]

Assuming conversion of intangible property is recognized, a plaintiff in a corporate breach case could argue that their information is property covered by the conversion tort. This is especially so in cases involving a breach of credit card or financial information, in which there is a clear connection between the digital data and the plaintiff's underlying property right. The more difficult task, however, is that plaintiffs would have to show the corporation engaged in behavior that interfered with the plaintiff's control or right of dominion over the information. For example, this could be the period of time in which the plaintiff could not access accounts or freely utilize finances due to increased need to monitor for potential unauthorized charges and fraudulent behaviors—let alone, outright exercise of identity theft.

Clearly, this is a perfect set-up for an action against the hacker. But once again the corporate defendant is one step removed from the harm, as harms produced by the conversion are clearly the result of the hacker's actions. This gap looms large in efforts to rely on conversion, which is traditionally an *intentional* tort. Of course, if it is shown that the corporation or an employee within the corporation had some role to play in the data breach, then the plaintiff's claim would stand on firm ground.

2. Trespass to Chattels

Like conversion, trespass to chattels has traditionally dealt with physical property, but it has since been broadened to cover portions of the digital domain (e.g., computer systems).[117] In these claims, the basis for liability frequently rests on the claim that the defendant had in some way damaged or impaired the property's "condition, quality,

114. *See id*. at 1273, 1278.

115. *Id*.

116. *See, e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 527 F. Supp. 2d 209, 211–13 (D. Mass. 2007) (citing other cases indicating Massachusetts common law does not recognize conversion of intangible property), *aff'd in part*, *rev'd in part*, 564 F.3d 489 (1st Cir. 2009).

117. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004) (allowing a preliminary injunction against the defendant's "search robots" as they may interfere with the plaintiff's computer system).

or value."[118] A leading case is *Intel Corp. v. Hamidi*,[119] in which the court specified that trespass to chattels need not be tied to physical damage—rather, it is applicable in instances where there is a depreciation in "quality" or "value" of the plaintiff's property, including instances where there is "intermeddling with or use of or damages to the personal property."[120] However, the court in *Hamidi* rejected the claim, as the plaintiff failed to show that the defendant, in using plaintiff's computer system to send mass-emails criticizing plaintiff's employment practices, caused any disruption in the system's functioning.[121]

In *Sotelo v. DirectRevenue, LLC*,[122] however, the court found a trespass to chattels and rejected a required showing of substantial interference with ownership.[123] There, the court held that a bombardment of pop-up advertisements supported a finding of trespass to chattels, as the injury was "the cumulative harm caused by the volume and frequency of the advertisements"—which caused damages in the form of "wasted time, computer security breaches, lost productivity, and additional burdens on the computer's memory and display capabilities."[124]

But the problem with trespass to chattels is, once again, the necessary "intent" element. One formulation of the trespass to chattels tort requires that there be intentional interference, not necessarily to violate the plaintiff's rights but at least an intent to commit the acts that lead to such violation.[125] Even if the plaintiff could show some evidence of intent on the part of the corporation—a virtually insurmountable task—there would need to be a demonstration of harm done to the "quality or value" of the victim's data, or rights associated with that data. It would be a stretch to meet this requirement by showing a need for credit-monitoring or short-term restrictions on use of personal data.[126]

---

118. RESTATEMENT (SECOND) OF TORTS § 218 (AM. LAW INST. 1965).

119. 71 P.3d 296 (Cal. 2003).

120. *Id*. at 327–28 (citing its holding in Zaslow v. Kroenert, 176 P.2d 1, 7 (1946)).

121. *Id*. at 308.

122. 384 F. Supp. 2d 1219 (N.D. Ill. 2005).

123. *Id*. at 1230 (citing CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997)).

124. *Id.* at 1233.

125. RESTATEMENT (SECOND) OF TORTS § 217 cmts. b, c (AM. LAW INST. 1965).

126. At the other end of the continuum from intentional tort liability would be a claim for strict liability for "abnormally dangerous activities." *Id*. § 520. But that theory seems to be of no avail in the data breach circumstances. The widely-followed *Restatement (Second) of Torts* provision, defining abnormally dangerous activities, listed six factors for consideration, focusing on high degree of risk of harm, but most importantly for present purposes, requiring "inability to

C. Negligence Pathways: Theoretical Prospects

If one concedes that corporate data security lapses are just that—unreasonable failures to maintain adequate security—then the "fit" that seemed elusive in tracking the privacy torts and various intentional and strict liability options, seems at last to have a prospective home. The focal point becomes, as it should be, the intentional wrongdoing of a third party (the hacker/identity thief), and the question arises: Under what circumstances can an intermediary defendant be held for failing to protect against misconduct by a malevolent third party? Two profiles of responsibility for safeguarding against such third-party initiated harm seem most germane—negligent failure to provide adequate security, and negligent enabling responsibility.[127]

1. Negligent Failure to Provide Adequate Security

The first is the case law that has developed from the 1970s to the present on failure to adequately protect an innocent victim from physical violence. There is a particular valence to these cases, which set aside the long-standing reluctance of tort law to embrace third-party obligations, expressed in the nonfeasance theme of no duty of affirmative action. This limitation is surmounted in the contemporary setting by focusing on the *relational* obligations of the intermediate defendant, whether landlord to tenant (in the residential violence cases),[128] or storeowner to customer (in the business premises violence cases).[129]

It is important to note that this status linkage is a considerably less stringent nexus than a fiduciary relationship.[130] Neither occupation—landlord or store owner—is a status weighted with customary fiduciary responsibilities. They are status relationships on the same plane

---

eliminate the risk by the exercise of reasonable care." *Id.* The *Restatement (Third) of Torts* collapses the factors into two, but retains the requirement that reasonable care be unavailing to eliminate the risk. RESTATEMENT (THIRD) OF TORTS § 20 (AM. LAW INST. 2010). For a leading case, carefully parsing the *Restatement (Second) of Torts* factors and holding that a concededly dangerous activity—the shipping of a highly toxic chemical—nonetheless failed to meet the requirements because due care would have avoided the harm, see Ind. Harbor Belt R.R. Co. v. Am. Cyanamid Co., 916 F.2d 1174, 1181 (7th Cir. 1990). The inadequate data security cases almost certainly founder on the same prospective showing.

127. For earlier discussions, see Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 259–62 (2005); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553 (2005).

128. *See, e.g.*, Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970) (leading case for landlord obligations to tenant).

129. *See, e.g.*, Ann M. v. Pac. Plaza Shopping Ctr., 863 P.2d 207 (Cal. 1993).

130. The latter requirement has been a limiting factor in the development of a robust breach of confidence tort in the United States.

with corporate defendants in data security breach cases, where the corporate entity has implicitly, if not explicitly, represented that it will safeguard a customer's private personal or financial information.

Then, the question becomes whether the distinction between security against physical violence and against financial/emotional harm should defeat recognition of an analogous claim for tort protection. In *Randi W. v. Muroc Joint Unified School District*,[131] a negligent misrepresentation case involving misleading letters of reference that set the stage for child sexual abuse, the California Supreme Court clearly thought that the distinction should be recognized.[132] Depending on the factual circumstances, a negligent misrepresentation theory might play out in a corporate data breach scenario, except that the tort claim as recognized in *Restatement (Second) of Torts*, Section 331, mirrors the *Randi W.* holding in limiting liability to physical harms.[133]

2. Negligent Enabling Conduct

A second prospective doctrinal handle in the case law is the concept of an enabling tort.[134] This is a close cousin to the negligent breach of security claim. In both scenarios, a defendant, through substandard precautionary conduct, has, in essence, set the stage for malevolence leading to victimization of an innocent party. There is less than total overlap, however. The enabling tort is not dependent on a status relationship between the intermediary defendant and the victim of third-party misconduct. Consider by way of illustration, *Weirum v. RKO General, Inc.*,[135] in which a radio disk jockey encouraged reckless driving by offering a prize for tracking him down on the highway;[136] or the key in the ignition cases in which the stage is set for theft, reckless driving, and third-party injury[137]—both illustrative of enabling torts, but neither resting on a status-based nexus between enabler and vic-

131. 929 P.2d 582 (Cal. 1997).

132. *Id*. at 591–92.

133. *Compare* RESTATEMENT (SECOND) OF TORTS § 331 (AM. LAW INST. 1977), *with Randi W.*, 929 P.2d at 582. There is a third-party negligent misrepresentation scenario in which stand-alone economic loss is well-recognized: The negligent provision of professional services (most frequently, a negligently-conducted audit that leads to third-party financial losses). *See, e.g.*, Nycal Corp. v. KPMG Peat Marwick LLP, 688 N.E.2d 1368, 1372 (Mass. 1998); RESTATEMENT (SECOND) OF TORTS § 552 (AM. LAW INST. 1977). However, it requires a considerable stretch to develop a bridge from negligent provision of professional services causing third-party injury to negligence in safeguarding the *immediate* security of information providers against outside malevolence.

134. For discussion, see Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 449 (1999).

135. 529 P.2d 36 (Cal. 1975).

136. *Id*. at 37–38.

137. *See, e.g.*, Palma v. U.S. Indus. Fasteners, Inc., 681 P.2d 893, 896 (Cal. 1984).

tim. Note, however, that this is a distinction without a difference for the corporate data security cases, in which the status relationship is invariably present in the defendant's breach of plaintiff's informational privacy.

D. Negligence Pathways: Damages

Now we come to the crux of the matter: Whether there is a viable claim for tort damages in these corporate data breach scenarios. This requires a closer look at the harm experienced by victims in the context of tort remedies. Consider, initially, claims arising out of the data breach, standing alone. Personal and financial information of a concededly private character has fallen prey to a hack, but there is no indication that the information has been put to illicit use. In these circumstances, the financial consequences to the victim most likely would be limited to credit monitoring (as a safeguard), and transactional costs in re-establishing new personal identifying information. From a tort perspective, these costs would be characterized as tangible, stand-alone economic loss.[138] The financial outlays would be relatively trivial so long as the focus remains on the harms to *individual* victims of the breach, rather than the *collective* harms.

In fact, the out-of-pocket expenditures associated with this anticipatory-risk scenario seem secondarily consequential. The more salient aspect of a hacker's access to a victim's supposedly secure personal data is arguably the affront to one's privacy and accompanying anxiety and from the keen awareness that one's personal information is in the hands of a malefactor—with a risk that it will be used for illicit purposes at some point. Whether this harm is viewed in tandem with the above-mentioned financial consequences, or as stand-alone emotional distress, the undermining of personal security and equanimity is undeniable.

Once again, however, from an individual victim perspective—setting aside for now the aggregate harm from a mass security breach—the tort-related ramifications seem problematic. Much of the breach-related distress (aggravation, anxiety) occurs in the "window" between notice of the breach and fix-related economic outlays. Beyond this distress, the lurking concern that the identity theft will be brought to fruition bears some similarity to the cancerphobia claims in recent

138. For discussion of stand-alone economic loss, see generally Robert L. Rabin, *Respecting Boundaries and the Economic Loss Rule in Tort*, 48 ARIZ. L. REV. 857 (2006). For discussion of the economic loss rule in the context of claims among issuer banks, acquirer banks, and merchants in the data security cases, see generally Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339 (2017).

long-latency toxic exposure cases.[139] But those claims—in the absence of a threshold underlying disease—have not been viewed favorably in the courts, for the most part.[140] Moreover, there is a substantial categorical distinction between fear and anxiety associated with the risk of contracting cancer and similar distress over misuse of personal identifying characteristics. Without meaning to trivialize the latter, my own view is that the dominant social concern—at least from a tort perspective—over the unrealized risk of malevolent use of private identifying information is collective rather than individual.

To what extent is this limiting perspective altered when the victim's claim is based on a malefactor's transactional use of the stolen information—in other words, identity threat that is brought to fruition—rather than simply the risk of such use? The answer turns on the recourse available to the victim to retrieve misplaced withdrawals against financial accounts. In the typical case, the losses would eventually be borne by the hacker's defrauded *corporate* victim rather than the innocent victim of the identity theft.[141] This, of course, has major economic consequences for the system of commerce—as briefly spelled out in the introductory section of this Article. But beyond the transactional costs of establishing eligibility for reimbursement (and re-establishment of frozen sources of credit), these are not consequences likely to animate individual tort claims for economic loss.

To a certain extent, the emotional distress claims associated with a fully realized identity theft track the discussion of anticipatory harm discussed above—anxiety, aggravation, and a sense of outrage. But there is arguably a distinctive dignitary loss associated with the fully realized identity theft; that is, a sense of personal transgression and violation intrinsic to the abuse of one's equanimity.

In some respects, this aspect of the wrong resembles the one privacy tort that I have not discussed above: the so-called false light claim, where the harm arises from being represented as someone other than one's true self.[142] If the analogue seems compelling, of course, the

---

139. On toxic exposure claims, see, for example, Bill Charles Wells, *The Grin Without a Cat: Claims for Damages from Toxic Exposure Without Present Injury*, 18 WM. & MARY J. ENVTL. L. 285, 289 (1994).

140. *See, e.g.*, Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424 (1997).

141. If the bank makes payment against the victim's account on the credit charge and then reimburses the victim, presumably, the bank would have a right of subrogation against the corporate vendor. If the identity theft victim refuses payment in the first instance, then the corporate vendor would simply bear the loss directly. For discussion, see Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203, 219–23 (2008).

142. *See* RESTATEMENT (SECOND) OF TORTS § 652E (AM. LAW INST. 1977).

dignitary claim would best be brought against the hacker (along with a bevy of other tort claims, ranging from conversion to intentional infliction of emotional distress). Nonetheless, the dignitary aspect of the emotional distress claim, in the context of a fully realized identity theft, does seem to be a direct consequence of the harm inflicted by the failure of the corporate entity to reasonably discharge its security responsibility. There does seem to be sufficient grounding here, in tandem with the more modest financial costs, to make out a colorable claim for relief.[143]

While this pathway to tort redress is not a trivial consideration, it hardly seems likely to serve as a strong incentive in generating an industry-wide framework of more adequate data security measures. In that regard, as the discussion to this point has inferred, an aggregative mechanism—collective tort action—would seem to be required. Paradoxically perhaps, the individual dignitary claim for realized identity theft is probably least likely to survive aggregate treatment in view of the class action requirement that common questions of law or fact predominate over questions affecting individual class members.[144] This is so, precisely because the dignitary harm seems so clearly a case-by-case inquiry.

By contrast, the stand-alone financial losses, particularly among those arising in fully realized identity thefts, may be more amenable to aggregate treatment. Predictably, however, in view of the somewhat attenuated character of the aggregation claim, there is sharp disagreement on whether class treatment is sustainable.[145]

---

143. There is a caveat, however. If this dignitary harm claim has its foundation in the tort of negligent infliction of emotional distress, there is a threshold duty limitation that may be difficult to surmount. Negligent infliction of emotional distress claims, in most jurisdictions, require that the victim be in a zone of physical danger. *See, e.g.*, Betsy J. Grey, *The Future of Emotional Harm*, 83 FORDHAM L. REV. 2605, 2615 (2015).

144. FED. R. CIV. P. 23(b)(3).

145. While the courts are split on class certification in the context of data breaches, several trends are apparent. First, class certification is generally granted only in a narrow set of circumstances. For example, courts tend to grant class certification where the plaintiffs' cause of action falls under a federal statute like the Fair Credit Reporting Act. *See*, *e.g.*, Engel v. Scully & Scully, Inc., 279 F.R.D. 117, 126 (S.D.N.Y. 2011); Stillmock v. Weis Mkts., Inc., 2010 WL 2621041, at *7 (4th Cir. July 1, 2010). This makes sense because the injuries in such cases tend to be identical across class members. The other common case where a trial court certifies a plaintiff class is where the parties reach a settlement agreement. *See, e.g.*, *In re* LinkedIn User Privacy Litig., 309 F.R.D. 573, 581 (N.D. Cal. 2015) (certifying settlement class for settlement up to $1.25 million for leaked password information); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., No. 11md2258 AJB (MDD), 2014 WL 7800046, at *2 (S.D. Cal. July 10, 2014). Sony settled with the class of plaintiffs for $15 million for the leak of personal account information. *See* Michael Lipkin, *Sony Strikes $15M Deal to Exit Data-Breach MDL*, LAW360 (June 23, 2014), https://www.law360.com/articles/548191/sony-strikes-15m-deal-to-exit-data-breach-mdl.

IV. Beyond Tort: A Concluding Thought

In the final analysis, my view is that the most promising pathway for achieving the collective goal of enhancing corporate data security via tort-type remedies lies *outside* the tort arena, but shares the safety incentives objective that animates the search for more effective corporate data security practices: A growing recognition that substandard practices might be re-cast as unfair competitive activity through federal regulatory enforcement.[146] In a recent case, *Federal Trade Commission v. Wyndham Worldwide Corp.*,[147] the Third Circuit Court of Appeals upheld the FTC's finding that a variety of security system shortcomings by the defendant hotel chain (absence of firewalls, insecure passwords, lax data storage provisions) constituted "unfair trade practices" under the agency's section 5 authority.[148]

Wyndham was the initial instance of a regulated party challenging in court the FTC's section 5 enforcement authority in an information privacy case.[149] Indeed, every FTC enforcement action since 2002, when the Commission began regulating information privacy, has resulted in settlement (including *Wyndham*).[150] One might reasonably conclude that this ruling will embolden the FTC in its quest to use section 5 to do the regulatory work that is beyond the capacity of the

---

In the vast majority of normal data breach cases, courts deny class certification on predominance grounds—namely, that common questions of liability, causation, and damages do not predominate over individualized determinations. *See, e.g.*, *In re* Google, Inc. Gmail Litig., No. 13-MD-02430-LHK, 2014 WL 1102660, at *19–21 (N.D. Cal. Mar. 18, 2014) (denying class certification because issues of implied or express consent, central to liability determination, did not predominate across the class); *In re* Hannaford Bros Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 28–29, 33 (D. Me. 2013) (denying class certification on predominance grounds because plaintiffs may have mitigated damages in very different ways). This is an unsurprising result. The particular features of data breach harms make class certification quite difficult. Only in the rare case will a class be able to show that common injuries predominate, as the range of injuries is often quite wide. The same is true of issues of causation—what caused the harms at issue; and mitigation—how much did each class member mitigate?

In a different context, one court certified a class of small financial institutions suing Target for its data breach and the effects the breach had on the class businesses—namely, reissuing cards and refunding fraudulent charges. *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 490 (D. Minn. 2015). *But see In re* TJX Cos. Retail Sec. Breach Litig., 246 F.R.D. 389, 401 (D. Mass. 2007) (denying class certification in similar circumstances). *See generally*, Sharkey, *supra* note 138.

146. For recent discussion, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum L. Rev. 583, 598–99 (2014).

147. 799 F.3d 236 (3d Cir. 2015).

148. *Id*. at 258–59.

149. J. Howard Beales III & Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 Geo. Wash. L. Rev. 2157, 2211 (2015).

150. *Id*.; *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, Fed. Trade Comm'n (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

tort system and other limited-mandate federal agencies with respect to data privacy.[151]

Ultimately, how proactive federal agencies will be in pursuing this remedial strategy remains an open question. Nonetheless, a strategy that focuses on systemic failures to give sufficient regard to our collective concern about maintaining security of private information seems preferable to the tort approach of remedying individual claims of harm, singly or collectively.

151. The FTC in its own administrative complaints and guidance reports has indicated that section 5 unfairness authority could potentially reach lapses in data security. *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 22 (2016) (noting that unfair practice could include "failure to reasonably secure consumers' data where that failure is likely to cause substantial injury"); *see, e.g.*, *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467 (2005) (finding respondent's failure to take reasonable measures to secure information, including the lack of encryption of files in transit and creating unnecessary risk by storing data longer than needed for business purposes, qualified as an unfair practice); *In re* ASUSTeK Comput., Inc., No. 142-3156, 2016 WL 807981, at *20 (F.T.C. Feb. 22, 2016) (holding that respondent's failure to take reasonable steps to secure its software caused or is likely to cause substantial injury and constituted an unfair practice). The FTC's unfairness authority is subject to limitations however. For example, in determining whether there was a substantial injury, the FTC has in the past largely focused on actual injuries to consumers as opposed to those that are "trivial, speculative, [or] emotional." Solove & Hartzog, *supra* note 146, at 639.