Florida Law Review

Volume 69 | Issue 3 Article 3

May 2017

Privacy, Mass Intrusion and the Modern Data Breach

Jon L. Mills

Kelsey Harclerode

PRIVACY, MASS INTRUSION, AND THE MODERN DATA BREACH

Jon L. Mills[*] *& Kelsey Harclerode*[**]

Abstract

Massive data breaches have practically become a daily occurrence. These breaches reveal intrusive private information about individuals, as well as priceless corporate secrets. Ashley Madison's breach ruined lives and resulted in suicides. The HSBC breach, accomplished by one of their own, revealed valuable commercial information about the bank *and* personal information about HSBC customers. The employee responsible for the breach has since been convicted of aggravated personal espionage, while third-party news outlets have been free to republish the hacked information.

Some information disclosed in data breaches can serve a public purpose. The Snowden disclosures, for example, revealed sensitive government information and were also crucial to public policy debate, a significant amount of disclosed information is destructive to individuals and companies alike, and often has little, if any, public value.

The conflict between publicly important disclosures and disturbing private intrusions creates a direct confrontation between freedom of expression and privacy. A full analysis of this confrontation requires assessment of the specific circumstances of breach—from the vulnerabilities present beforehand to the aftermath when the media, companies, and individuals all must cope with the information exposed.

This analysis begins by evaluating the importance of information in modern society. Big data is now an inescapable part of our culture. A data breach may contain intimate details about medical conditions or national security secrets. The disclosure of either has its own kind of devastating effect. Examples of the impact of a mass data breach include the hacking of Target Corporation, Yahoo! Inc., Home Depot, Inc., Sony Corporation, Anthem Inc., HSBC Private Bank (Suisse), SA, and AshleyMadison.com. A dissection of these breaches reveals a common theme—the ineffectual legal system, which provides little protection or remedy for any party involved. Several factors—including the anonymity of hackers, outdated legal remedies, and free speech protections for third-party publishers—together create an uncertain and uncharted legal landscape.

---

[*] Jon L. Mills, Dean Emeritus, Professor of Law, and Director of Center for Governmental Responsibility, University of Florida Fredric G. Levin College of Law.

[**] Kelsey Harclerode, J.D. 2016, Research Assistant at University of Florida Levin College of Law Center for Governmental Responsibility.

The authors would like to thank Brandon Butterworth, Matthew Christ, Jill Guidera Brown, Marie Moyle, and Emily Snider for their research assistance in the preparation of this Article.

After evaluating the available statutory and common law remedies, this Article posits that reinvigorated private causes of action can be a starting point for developing stronger legal remedies for those damaged in a breach. The right facts and legal arguments can create new remedies out of existing legal doctrines. Further, public values on protecting privacy are in flux. More protective policies in the European Union demonstrate that privacy and free expression can coexist. Some EU policies may provide examples of legislative options. Corporate entities and individuals are at risk and are suffering real harm in a world with daily data breaches and ineffective laws. The need for new perspectives is urgent.

INTRODUCTION

We live in an increasingly intrusive world. Even when we share our data with trustworthy entities, our privacy is still at risk due to the enhanced possibility of data hacks and breaches. Modern data breaches exist at the intersection of technology, modern culture, and human frailty. The rate of change is rapid and not easily predictable. Policy makers from almost every sector and level of government are trying to keep up with improving technology and more skilled hackers. Beyond general tensions between rapidly developing technology and slow-moving laws, data breaches present a direct confrontation between two of society's most fundamental of rights: the freedom of expression and the right to privacy.

The man behind the largest data breach in the financial sector's history, Hervé Falciani, is hailed as a whistleblower by some and regarded as a thief by others. His tale of international intrigue highlights the drama and massive scope of the modern data breach.

Falciani, a computer analyst for HSBC Private Bank Suisse, obtained and leaked upwards of 30,000 company files that contained information regarding $120 billion in assets from more than 100,000 clients across 203 countries.[1] The leak exposed client lists, irregularities in financial patterns, as well as the private financial information of thousands of customers.[2] After fleeing Switzerland, Falciani shared his information with French officials and the media. A French newspaper passed it along to the International Consortium of Investigative Journalists (ICIJ) to assist in organizing and disseminating the data.[3] Meanwhile, Falciani was arrested in Geneva, fled to France, and was ultimately detained in Spain.[4] He now lives as a fugitive in France.[5] Though his leak allowed several countries to recover billions of dollars in back taxes, Falciani reportedly has not received any payment for his disclosures.[6] Still, the Swiss government believes Falciani was unjustly enriched by his actions and a Swiss court agreed.[7] Falciani was convicted of aggravated industrial espionage and sentenced to five years in jail.[8] While Falciani endured international legal repercussions for spearheading this leak, the third-party media sources—mediated by ICIJ—have been free to republish the leaked material without legal consequence, including information about private individuals.[9]

When publicly important information is revealed, often private information that wounds innocent individuals and corporations is exposed as well. The harm done to innocent parties wrapped up in public disclosures highlights the need to balance free speech with individual privacy rights. The HSBC breach represents just one of the thousands of

1. David Leigh et al., *HSBC Files Show How Swiss Bank Helped Clients Dodge Taxes and Hide Millions*, GUARDIAN (Feb. 8, 2015, 4:00 PM), http://www.theguardian.com/business/2015/feb/08/hsbc-files-expose-swiss-bank-clients-dodge-taxes-hide-millions; *HSBC Bank "Helped Clients Dodge Millions in Tax*," BBC (Feb. 10, 2015), http://www.bbc.com/news/business-31248913.

2. Leigh et al., *supra* note 1.

3. *Id.*

4. *Profile: HSBC Whistleblower Herve Falciani*, BBC (Feb. 9, 2015), http://www.bbc.com/news/world-europe-31296007.

5. Patrick Radden Keefe, *The Bank Robber*, NEW YORKER (May 30, 2016), http://www.newyorker.com/magazine/2016/05/30/herve-falcianis-great-swiss-bank-heist.

6. Bill Whitaker, *The Swiss Leaks*, CBS NEWS (Feb. 8, 2015), http://www.cbsnews.com/news/hsbc-swiss-leaks-investigation-60-minutes.

7. Juliette Garside, *HSBC Whistleblower Given Five Years' Jail over Biggest Leak in Banking History*, GUARDIAN (Nov. 27, 2015, 12:47 PM), http://www.theguardian.com/news/2015/nov/27/hsbc-whistleblower-jailed-five-years-herve-falciani.

8. *Id.*

9. Leigh et al., *supra* note 1.

massive data breaches that have become everyday headlines.[10] Despite an elevated frequency of modern data breaches, the law has simply not caught up.

Data breaches present themselves to a corporate general counsel as a tornado of legal issues. The loss of data does not result in one or two academic doctrinal problems that can be attacked like a law school final exam. The issues can include: trademark law, privacy law, First Amendment law, insurance law, tort law, negligence, contract law, securities law, violations of data security laws of other countries, labor law, federal agency data security violations, criminal law, shareholder liability, attorney–client privilege, and board liability. This list is not exhaustive, and it is impossible to predict the exact combination of legal issues that will arise after a particular breach. What is known is that these issues must be addressed immediately. A company may face a class action lawsuit, a Federal Trade Commission (FTC) enforcement action, a State Attorney General investigation, or all of the above. To ensure success, all potential post-breach issues must be addressed as quickly as possible. There is a reason general counsel lose sleep over data breaches.

While this law is evolving and unpredictable, this Article seeks to provide a primer on the modern data breach. It would be thoughtless, however, to contend that this Article provides a complete primer on the issue. In just the time between the *Florida Law Review* accepting this Article and the final edits, our country experienced dramatic transformations at the federal level, including at the executive branch and two of the most central agencies entrusted with establishing data protection standards, *and* Equifax revealed that a data breach exposed the information of 145.5 million Americans. The latter occurred in the final weeks of editing. Both of the events reveal the true challenge in protecting against and responding to a data breach during an era of technological upheaval: the law may never be able to catch up.

---

10. *See, e.g.*, Zack Whittaker, *2017's Biggest Hacks, Leaks, and Data Breaches – So Far*, ZD NET (Sept. 20, 2017), http://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017/; *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html; Peter Elkind, *Inside the Hack of the Century*, FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1/; Andy Greenberg, *Hack Brief: Yahoo Breach Hits Half a Billion Users*, WIRED (Sept. 22, 2016, 12:15 PM), https://www.wired.com/2016/09/hack-brief-yahoo-looks-set-confirm-big-old-data-breach/; Dan Munro, *Data Breaches in Healthcare Totaled over 112 Million Records in 2015*, FORBES (Dec. 31, 2015, 9:11 PM), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#67efbf4b7b07; Robin Sidel, *Target to Settle Claims over Data Breach*, WALL ST. J. (Aug. 18, 2015, 5:10 PM), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013; *see also infra* Section I.B.

This Article will explore the legal and social conflicts inherent in publicly important disclosures and private intrusions. Part I provides an overview of the importance of information as it relates to the modern data breach. Part II reviews the most common patterns among these intrusions. Part III analyzes the federal and state standards for data security and how these standards shape the options for the breached companies and exposed individuals. Part IV examines the private causes of action available after a breach occurs. Part V compares the data security law in the United States with that of the European Union with an emphasis on the transition to the General Data Protection Regulation (GDPR) in May 2018. Finally, Part VI offers suggestions for how corporations and individuals can best respond to the current states of data security law.

I. DATA BREACH IN THE INFORMATION AGE

Chief Justice John Roberts recently wrote, "[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house."[11] The prospect of a hacker cracking your cell phone's code to retrieve information about your communications, medical records, GPS locations, contacts, stored financial records, photos, appointments, or Google search history is downright frightening. Exposing digital data and metadata may provide a fuller and more intimate and intrusive invasion of privacy than a walk through your bedroom. In light of this new reality, smart phones must receive the same constitutional protections that the drafters of the Fourth Amendment afforded to the sanctity of the private home.

High-profile government data breaches have acted as a catalyst for discourse on data security. In 2013, the Edward Snowden disclosures prompted national and international scrutiny of the National Security Agency (NSA)'s data collection practices.[12] Recognizing the leak's dramatic effect on public dialogue about government intrusion does not prevent an equally important discussion about the disclosure's intrusiveness to individuals. Accordingly, the debate over whether Snowden should be regarded as a "whistle blower" or a traitor is still ongoing.[13]

In 2016, a group of Russian hackers used a spear phishing attack to breach the email account of John Podesta, the chairman of Hillary

11. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

12. Snowden's legacy continues with another NSA data breach reportedly conducted by a contractor of NSA consulting company, Booz Allen Hamilton. Jo Becker et al., *N.S.A. Contractor Arrested in Possible New Theft of Secrets*, N.Y. TIMES (Oct. 5, 2016), http://www.nytimes.com/2016/10/06/us/nsa-leak-booz-allen-hamilton.html.

13. *See* AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE (Ronald Goldfarb ed., 2015).

Clinton's 2016 presidential campaign.[14] This initial intrusion, the original publication of the emails on Wikileaks, and the subsequent republication of the emails on almost every news site imaginable played a substantial—but largely immeasurable—role in Donald Trump's defeat of Hillary Clinton in November 2016.[15] The Kremlin's involvement in the 2016 election and President Trump's knowledge of such involvement has since dominated coverage of his first seven months in office and will likely continue to plague his presidency.[16]

Politically motivated intrusions and leaks are not a new trend. In 1971, Daniel Ellsberg leaked portions of the Pentagon Papers to the press.[17] One year later in 1972, former President Richard Nixon's aides broke into and bugged the Democratic National Committee's headquarters at the Watergate Hotel.[18] These disclosures—new and old—demonstrate the dramatic impact that data security has on the individual and society at large.

When information is stolen or misappropriated, the result is frequently characterized as a "data breach."[19] Data can take on many different meanings. Sensitive data is generally afforded greater legal protection, and includes financial, educational, and medical records, as well as personally identifiable information (PII), business information, and location data.[20] Data can be most easily broken down into two types: "metadata" and "content." Metadata is the information about the content data.[21] For example, the body of an email is the content and the subject

14. *See* Lorenzo Franceschi-Bicchierai, *How Hackers Broke into John Podesta and Colin Powell's Gmail Accounts*, MOTHERBOARD (Oct. 20, 2016, 9:30 AM) https://motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts.

15. *See* Harry Enten, *How Much Did Wikileaks Hurt Hillary Clinton?*, FIVETHIRTYEIGHT (Dec. 23, 2016, 5:01 AM), https://fivethirtyeight.com/features/wikileaks-hillary-clinton/.

16. *See* Silvia Amaro, *Russia Scandal Could Dog Trump's Presidency for Years, Political Analyst Says*, CNBC (July 17, 2017, 5:55 AM), https://www.cnbc.com/2017/07/17/russia-scandal-could-dog-trumps-presidency-for-years-political-analyst-says.html.

17. *The New York Times* published three articles detailing Daniel Ellsberg's leak of the Pentagon Papers before the Nixon administration sought to enjoin *The New York Times* and *The Washington Post* from publishing information and analysis of the Pentagon Papers. *See* David W. Dunlap, *1971 Supreme Court Allows Publication of Pentagon Papers*, N.Y. TIMES (June 30, 2016), https://www.nytimes.com/2016/06/30/insider/1971-supreme-court-allows-publication-of-pentagon-papers.html.

18. *See* Carl Bernstein & Bob Woodward, *FBI Finds Nixon Aides Sabotaged Democrats*, WASH. POST (Oct. 10, 1972), https://www.washingtonpost.com/politics/fbi-finds-nixon-aides-sabotaged-democrats/2012/06/06/gJQAoHIJJV_story.html.

19. Margaret Rouse, *Data Breach*, TECHTARGET, http://searchsecurity.techtarget.com/definition/data-breach (last updated May 2010).

20. For a discussion of federal and state laws that protect sensitive information, see *infra* Part III.

21. *Metadata Definition*, LINUX INFO. PROJECT (Mar. 21, 2006),

line, origin, and destination of the email is metadata. Both forms are vulnerable to a breach,[22] and the information itself carries varying levels of intimacy, which may be intensified when aggregated. While the content of your medical records may seem more private than the corresponding metadata, uncovering a complete log of the appointment times of one's health visits (metadata) is no less of a Health Insurance Portability and Accountability Act (HIPAA) violation than the exposure of the reason for a person's health visit (content).

Despite the interconnectivity of data and the overarching implications of privacy in all aspects of life today, the United States primarily compartmentalizes the regulation of data security by each defined sector.[23] For example, the legal standards for protecting health data are different from the standards for protecting education data. Regardless of the sector, metadata is often less protected than content under current legal doctrine. Courts have traditionally held that while there is an expectation of privacy in the content of a telephone call, the metadata about that telephone call is not private.[24] The common analogy in support of this view is that the return address and address on an envelope are not considered private while the contents of the envelope are.

This analysis undervalues metadata. Collected in the aggregate or over a broad span of time, metadata can reveal as much about a person as content.[25] Innovative technologies help entities collect massive amounts of metadata nearly constantly, while sophisticated analytic tools allow detailed evaluations.[26] One well known example of metadata collection and analysis is the NSA's bulk data collection and analysis program, which has undergone significant legal scrutiny following the Snowden

---

http://www.linfo.org/metadata.html.

22. *How to Extract Metadata from Websites Using FOCA for Windows*, NULL BYTE (May 28, 2016), http://null-byte.wonderhowto.com/how-to/hack-like-pro-extract-metadata-from-websites-using-foca-for-windows-0155076/.

23. There are more than fifty privacy related federal laws. *See, e.g.*, Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (2012); Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–05 (2012); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012); The Common Rule, 45 C.F.R. § 46.101 (2010); Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. §§ 160, 164 (2010).

24. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that metadata pertaining to phone numbers dialed was not protected under the Fourth Amendment because it was available to the phone company).

25. Joe Coscarelli, *Metadata Can Be More Revealing Than Your Actual Conversations*, N.Y. MAG. (June 7, 2013, 1:03 PM), http://nymag.com/daily/intelligencer/2013/06/metadata-whats-in-your-phone-records.html.

26. *See* Sara Schwartz, *9 Ways You're Being Spied on Every Day*, HUFFINGTON POST (Apr. 3, 2014, 12:28 PM), http://www.huffingtonpost.com/2014/04/03/government-surveillance_n_5084623.html.

disclosures.[27] Judge Richard J. Leon, in a ruling that the U.S. District Court for the District of Columbia ultimately reversed for a lack of standing, aptly commented, "Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[28] The legal system's slow progression towards recognizing the importance of metadata is but one of the many challenges within privacy law.[29]

A. *Corporate Data Breaches*

As part of their business model, modern corporations collect, store, use, create, and disseminate information constantly—and are thus made vulnerable to a third party stealing or misappropriating that information. Corporate data can be as routine as an employee's weekly work schedule, or as unique as the formula for Coca Cola. In 2016, documented incidents of data breaches reached an all-time record high of 1,093, leaving more than 36 million records exposed.[30] Based on data through June 2017, one estimate suggests that this figure will rise by 37% by the end of 2017.[31] Consistent with these numbers, 64% of American adults report having experienced their personal data compromised in a breach.[32] A corporation's public reputation and economic value may be profoundly damaged in a breach, as well as the reputations, finances, and personal lives of the individuals associated with the breach. When users of the

27. *See* Jack Goldsmith, *Reflections on NSA Oversight, and a Prediction That NSA Authorities (and Oversight, and Transparency) Will Expand*, LAWFARE (Aug. 9, 2013, 7:52 AM), https://www.lawfareblog.com/reflections-nsa-oversight-and-prediction-nsa-authorities-and-oversight-and-transparency-will-expand; *see also* Kelsey Harclerode, *How USA Freedom Impacts Ongoing NSA Litigation*, ELECTRONIC FRONTIER FOUND. (June 23, 2015), https://www.eff.org/deeplinks/2015/06/how-usa-freedom-impacts-ongoing-nsa-litigation.

28. Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

29. The ability for long-term surveillance and the subsequent collection of data to eventually reveal significant insight about one person when put together is often referred to as the "mosaic theory." In *United States v. Jones*, two concurring opinions signed or joined by five of the Supreme Court justices supported the notion that long-term surveillance triggers Fourth Amendment protection. 565 U.S. 400, 413–17 (2012) (Sotomayor, J., concurring); *Id.* at 429–31 (Alito, J., concurring); *see also* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (using the phrase "mosaic theory" to describe the fact that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble").

30. IDENTITY THEFT RES. CTR., DATA BREACH REPORTS: 2016 END OF YEAR REPORT 2 (2017), http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf.

31. *At Mid-Year, U.S. Data Breaches Increase at Record Pace*, IDENTITY THEFT RESOURCE CTR. (July 18, 2017), http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release.

32. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

cheating-enabling website Ashley Madison were exposed through a leak, many marriages were dissolved, public figures ridiculed, and, tragically, multiple people committed suicide.[33] Clearly, the real-life implications of a data breach can be severe, and the harms can extend beyond the immediate consequences of the thief's initial exposure.

B. *Examples of Corporate Data Breaches*

The following cases across different industries demonstrate the importance of data security, the need for concrete remedies for individuals harmed in a data breach, and the general security patterns that emerge throughout the life cycle of data management.

1. Target

Because Target failed to identify the lax security of a subcontractor, the company became the victim of a sophisticated hacking attack that left 40 million customers' debit and credit cards exposed and an additional 70 million customers' nonfinancial personal information stolen.[34] In the aftermath, Target's CEO resigned, the company settled a massive consumer class action lawsuit for $18.5 million,[35] and the company lost approximately $148 million due to a drastic decline in consumer trust.[36] Target also agreed to pay $39.4 million to the banks and credit unions that sued Target for the costs incurred to reimburse fraudulent charges and issue new credit and debit cards to Target's consumers.[37]

2. Yahoo!

In September of 2016, Yahoo, the internet search engine, mail provider, and content platform, revealed that the company had

33. Sara Malm, *Two Suicides Are Linked to Ashley Madison Leak: Texas Police Chief Takes His Own Life Just Days After His Email Is Leaked in Cheating Website Hack*, DAILY MAIL (Aug. 24, 2015, 5:08 PM), http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html; Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN MONEY (Sept. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/.

34. Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

35. *Id*.

36. Samantha Sharf, *Target Shares Tumble as Retailer Reveals Cost of Data Breach*, FORBES (Aug. 5, 2014, 9:16 AM), http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach.

37. Jonathan Stempel & Nandita Bose, *Target in $39.4 Million Settlement with Banks Over Data Breach*, REUTERS (Dec. 2, 2015, 9:16 PM), https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203.

experienced a massive breach two years prior in which 500 million users' PII, encrypted passwords, and in some cases security questions were hacked by a "state-sponsored actor."[38] Just three months later, the company disclosed a separate, and even greater, hack that compromised the accounts of more than 1 billion users.[39] As a result of the double breaches, Yahoo lost profits in its pending acquisition deal with Verizon. In March of 2017, the U.S. Justice Department indicted two Russian spies and two criminal hackers on charges of hacking, wire fraud, trade secret theft and economic espionage in connection to the earlier Yahoo breach.[40] The Justice Department's indictment of foreign cybercriminals is consistent with U.S. government's recent strategy of issuing economic sanctions against foreign governments in the aftermath of cyber attacks, as seen against North Korea in the Sony case,[41] and Russian officials after interference in the 2016 U.S. presidential election.[42]

3. Home Depot

In 2014, hackers deployed malware that infected the Home Depot payment systems, and 56 million customers' credit cards were exposed.[43] It reportedly took five months for the company to become aware of the attack.[44] Following the breach, Home Depot faced a daunting class action lawsuit that ultimately led to a $19.5 million settlement.[45]

4. Sony Pictures and Entertainment

In November 2014, Sony, the global entertainment company, experienced a sweeping data breach that revealed a massive amount of intellectual property and sensitive personal information.[46] In the weeks

38. Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

39. Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

40. Ellen Nakashima, *Justice Department Charges Russian Spies and Criminal Hackers in Yahoo Intrusion*, WASH. POST (Mar. 15, 2017), https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.4169dbd11053.

41. *See* discussion *infra* Subsection I.B.4.

42. *See* Nakashima, *supra* note 40.

43. Melvin Blackman, *Home Depot: 56 Million Cards Exposed in Breach*, CNN (Sept. 18, 2014, 5:56 PM), http://money.cnn.com/2014/09/18/technology/security/home-depot-hack/.

44. *Id.*

45. Jonathan Stempel, *Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016, 2:10 PM), http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z.

46. *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

following the public disclosure of the breach on November 24, the hackers released 38 million files in eight individual batches.[47] These files included salacious content, such as emails between executives and celebrities.[48] The leaked intellectual property included unreleased movies and unfinished manuscripts.[49] The estimated twenty-five gigabytes of sensitive and/or confidential employee data released included passwords, private keys, personal health information, social security numbers, home addresses, bank account information, workers compensation details, performance reviews, retirement plan information, and criminal background checks.[50] Sparking international intrigue and igniting debates concerning the intersection of national security and the First Amendment, many believe that North Korea perpetrated the breach to deter the release of *The Interview*, a comedic film that featured an assassination of North Korea's leader.[51] Following the breach, Sony fired several executives and also agreed to pay $2–4.5 million to settle a class action lawsuit brought by employees whose personal records were exposed in the breach.[52]

5. Anthem Health Insurance

The healthcare sector has been the target of several massive hacks, a trend that is predicted to continue due to the high value of personal medical information.[53] In 2015, questionable internal storage encryption led to the theft of nearly 80 million personal records from Anthem, a large medical insurance company.[54] The hackers targeted PII like social security numbers, email addresses, and birthdays.[55] The fifty plus class actions suits filed against Anthem also raised concerns over potential

47. *See, e.g.*, Elkind, *supra* note 10.

48. *See id.*

49. *See id.*

50. *See id.*

51. David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.

52. Jody Godoy, *Sony to Pay up to $4.5M to Settle Employee's Breach Suit*, LAW360 (Oct. 20, 2015, 4:00 PM), http://www.law360.com/articles/716417/sony-to-pay-up-to-4-5m-to-settle-employees-breach-suit.

53. *2017 Data Breach Industry Forecast*, EXPERIAN (2017), http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf.

54. Bruce Japsen, *Hackers Stole Data on 80 Million Anthem Customers. Why Wasn't It Encrypted?*, FORBES (Feb. 6, 2015, 8:45 AM), http://www.forbes.com/sites/brucejapsen/2015/02/06/anthem-didnt-encrypt-personal-data-and-privacy-laws-dont-require-it/.

55. *Id.*

HIPAA violations since the breach included medical IDs.[56] In 2017, Anthem settled the consumer claims for $115 million.[57]

6. HSBC Finance Corporation

This hack of a global bank by an employee revealed intimate financial information about thousands of the bank's international clients, some of whom were notable business leaders and public figures.[58] Not only did this hack bring HSBC data security practices under scrutiny, but several of the individual customers are now under criminal investigation for information brought to light in the disclosure.[59]

7. Ashley Madison

An anonymous hacker group—self-named The Impact Team—hacked into the online cheating website and threatened to release the stolen information if the owners did not permanently shut down the site.[60] When the website owners did not meet their demands, the hackers uploaded around thirty gigabytes of stolen data onto the dark web.[61] This data dump exposed the personal account information of the site's users, as well as maps of the company's internal servers, financial data, and employee salary information.[62] Thus far, two suicides have been linked to the hack,[63] the CEO has resigned,[64] and exposed users have filed a $576 million class action suit against the owners of Ashley Madison.[65]

---

56. Joseph Conn, *Legal Liabilities in Recent Data Breach Extend Far Beyond Anthem*, MOD. HEALTHCARE (Feb. 23, 2015), http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem.

57. Pamela A. Maclean, *Anthem Agrees to $115 Million Settlement Over Data Breach*, BLOOMBERG (June 23, 2017, 5:45 PM), https://www.bloomberg.com/news/articles/2017-06-23/anthem-reaches-115-mln-settlement-in-massive-data-breach-case.

58. *See* David Leigh et al., *HSBC Files: Why the Public Should Know of Swiss Bank's Pattern of Misconduct*, GUARDIAN (Feb. 8, 2015, 4:00 PM), https://www.theguardian.com/business/2015/feb/08/hsbc-files-public-right-to-know-swiss-operation-leaked-data.

59. *Id.*

60. Brian Krebs, *Online Cheating Site AshleyMadison Hacked*, KREBS ON SECURITY (July 15, 2015), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

61. Kim Zetter, *Ashley Madison Hackers Release an Even Bigger Batch of Data*, WIRED (Aug. 20, 2015, 3:01 PM), http://www.wired.com/2015/08/ashley-madison-hackers-release-even-bigger-batch-data/.

62. Krebs, *supra* note 60.

63. Chris Baraniuk, *Ashley Madison: 'Suicides' over Website Hack*, BBC NEWS (Aug. 24, 2015), http://www.bbc.com/news/technology-34044506.

64. Kim Zetter, *Ashley Madison CEO Resigns in Wake of Hack, News of Affairs*, WIRED (Aug. 28, 2015, 11:35 AM), http://www.wired.com/2015/08/ashley-madison-ceo-resigns-wake-hack-news-affairs/.

65. *Ashley Madison Faces Huge Class-Action Lawsuit*, BBC NEWS (Aug. 23, 2015), http://www.bbc.com/news/business-34032760.

However, those exposed have faced several hurdles during the litigation process. The Missouri federal district judge presiding over the multi-district litigation ordered the class representatives to be publicly identified[66] and prohibited the plaintiffs from referencing stolen documents in their consolidated complaint.[67] Despite these limitations, in 2017, Ashley Madison reached a settlement deal with consumers totaling $11.2 million, in addition to the company's $1.6 million fine from the FTC.[68] Affected consumers can claim up to $2,000 to cover costs of identity theft.

While each of these data breaches have different facts, the common element was devastation to both individuals and to the breached entity. In many instances, the business is left just as exposed as the individuals. What remains constant is that neither have adequate recourse.

C. *Data Breach Victims: Where Are the Remedies?*

The overarching theme of these data breaches is the ineffectiveness of the legal system to redress wrongs in a timely or complete fashion. Both the hacked businesses and victimized individuals are left frustrated and wondering—where are the remedies? Breaches are akin to thefts of valuable information or personal property, and yet victims lack a clear pathway to legal redress. Hackers are most often anonymous or difficult to hold accountable. Even more frustrating is the inability to stop the republication of the hacked personal information. After the hacker's work is done, the damage is furthered by bloggers, the media, and others, who copy, republish, and comment on the stolen data.[69] In fact, hackers generally view broad publication of the data by the media after the breach as an integral component of their plan to harm the target of the breach. Principals of free speech and free press protect the republication of hacked data, leaving little opportunity for a data subject to seek relief once stolen data has been made available to the media.[70]

---

66. Brandon Lowrey, *Ashley Madison Class Reps Can't Hide Names in Hack MDL*, LAW360 (Apr. 6, 2016, 10:52 PM), http://www.law360.com/articles/781507/ashley-madison-class-reps-can-t-hide-names-in-hack-mdl.

67. Steven Trader, *Ashley Madison Users Blocked from Citing Leaked Docs*, LAW360 (May 2, 2016, 3:26 PM), http://www.law360.com/articles/791195/ashley-madison-users-blocked-from-citing-leaked-docs.

68. David Kravets, *Lawyers Score Big in Settlement for Ashley Madison Cheating Site Data Breach*, ARS TECHNICA (July 17, 2017, 1:15 PM), https://arstechnica.com/tech-policy/2017/07/sssshhh-claim-your-19-from-ashley-madison-class-action-settlement/.

69. *The Legality of Publishing Hacked E-mails*, COLUM. JOURNALISM REV., http://www.cjr.org/the_observatory/the_legality_of_publishing_hac.php (last visited Jan. 19, 2017).

70. WikiLeaks published data that revealed a person's sexual status, and also identified underage victims of sexual assault. This sensitive information was later widely republished by

Legal remedies for commonplace wrongs such as a home invasion or physical theft of personal property are by comparison adequate and predictable. Consider the theft of a laptop versus the theft of information *inside* the laptop. If that laptop is found even after it has been sold or exchanged, the owner gets the tangible laptop back. If the information on the laptop is opened and disclosed, that personal data may be irretrievable and damage may continue to be inflicted regardless of a retrieval. Whether it is a jewel thief or a data thief, the law should have a defined toolbox to protect societal values and ownership interests. The broad categories of legal remedies include criminal penalties, civil damages, or injunctions to prevent harm. Yet despite multiple legal approaches available, remedies for data breach victims are not reliably effective. For both individuals and corporations, the remedies for data breaches seem both limited and limitless.

II. EVALUATING A BREACH

The first steps in evaluating the post-breach legal remedies and options are evaluations of A) who is responsible for the unauthorized disclosure, and B) how did the breach occur. The answers to these deceptively simple questions dictate the immediate response and define options for moving forward.

A. *Who Is the Intruder?*

Not all online intruders hide behind their computer screens. Some publicly celebrate their breach. There are four basic categories of potential intruders: the whistleblower, the insider, the hacker, and the republisher.

1. The Whistleblower

A whistleblower obtains and discloses data to expose some degree of misconduct.[71] Under the Whistleblower Protection Act, federal employees are generally protected if they reasonably believed that the disclosure would reveal "any violation of any law, rule, or regulation"[72] or "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[73] There

third parties. Raphael Satter & Maggie Michael, *Private Lives Are Exposed as WikiLeaks Spills Its Secrets*, ASSOCIATED PRESS (Aug. 23, 2016, 5:09 PM), http://bigstory.ap.org/article/b70da83fd111496dbdf015acbb7987fb/private-lives-are-exposed-wikileaks-spills-its-secrets.

71. *What Is a Whistleblower?*, GOV'T ACCOUNTABILITY PROJECT, https://www.whistleblower.org/whatwhistleblower (last visited Jan. 19, 2017).

72. 5 U.S.C. § 2302(b)(8)(A)(i) (2012).

73. *Id.* § 2302(b)(8)(A)(ii).

are additional restrictions on what types of information can be disclosed to the press or public.[74] Daniel Ellsberg and Edward Snowden are both lauded as whistleblowers.[75] Congress has further extended protection to corporate whistleblowers who reasonably believe that their disclosure reveals corporate fraud or other violations of federal or state financial regulations.[76]

2. The Insider

"Insider" data breaches can be committed by a well-intentioned whistleblower or by an employee who uses internal data with the intent to harm the company or for any other unauthorized purpose. One example is a Walgreen pharmacist's disclosure of prescription records to her husband with the motivation to harm a woman she suspected had shared a sexually transmitted disease with her husband.[77] The result was a $1.4 million verdict against Walgreens for negligent supervision.[78] Insider breaches can be inadvertent or negligent. In fact, internal actors were responsible for 25% of breaches in 2016, and 14% of all 2016 breaches were due to employee error.[79] The image of the highly trained hacker or hackers sitting in a dimly lit room with multiple screens is not always accurate. Often the breach is simply caused by an angry employee or a negligent subcontractor, however, sometimes it can be an act of a malicious and sophisticated hacker.

3. The Hacker

There are a wide variety of techniques to hack databases—some technical and some based on human frailty. Intrusions committed by

74. *Id.* § 2302(b)(8)(A)-(B); *see generally* Nick Schwellenbach, *Survivor's Guide to Being a Successful Whistleblower in the Federal Government*, JUST SECURITY (Feb. 22, 2017), https://www.justsecurity.org/37994/survivors-guide-successful-whistleblower-federal-government/.

75. Ellsberg and Snowden's background and acts are often pitted against one another. *See, e.g.*, Malcolm Gladwell, *Daniel Ellsberg, Edward Snowden, and the Modern Whistle-Blower*, NEW YORKER (Dec. 19, 2016), https://www.newyorker.com/magazine/2016/12/19/daniel-ellsberg-edward-snowden-and-the-modern-whistle-blower.

76. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1376 (to be codified in various sections of the U.S. Code); Sarbanes Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 11, 15, 28, and 29 U.S.C.).

77. Andrew Scurria, *Walgreen Pharmacy Customer Scores $1.4M Privacy Verdict*, LAW360 (July 29, 2013, 7:08 PM), http://www.law360.com/articles/460788/walgreen-pharmacy-customer-scores-1-4m-privacy-verdict.

78. *Id.*

79. *See* VERIZON, 2017 DATA BREACH INVESTIGATIONS REPORT 2 (2017), https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf.

criminal hackers include point-of-sale hacks, web-app attacks, physical theft, crimeware, spear phishing, brute-force attacks on encryption, card skimmers, and cyber espionage.[80] The tools of this trade may include exhaustive preparation and extensive knowledge of the dark web. There are also hackers that focus on human frailty. The story of the hacker that gains access because an employee downloaded malware that the hacker baited the employee into downloading is well known.[81] The criminal hacker makes victims out of unsuspecting consumers and the company as well. Criminal hacks comprised the majority (62%) of data disclosures in 2016.[82] This criminal hacker is unambiguously motivated to harm a target, expose a truth, benefit herself personally, or in the case of corporate espionage, benefit or harm a competitor.[83]

4. The Republisher

A republisher is a type of intruder that is often overlooked despite their ability to inflict substantial damage with one simple post. A republisher is an entity, such as a curious individual on social media, a blog, or a major media outlet, that publicly shares leaked data after a breach.[84] Hackers may count on republishers to disseminate stolen data once leaked, or may even provide information directly to media outlets with the expectation that the media will publish the data. By reaching a broad audience, a republisher may cause as much—or more—damage than the hacker who initially stole the information.[85] There is little legal authority

80. VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 16, 20, 27, 32, 35, 43 (2014), http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

81. Peter Schablik & Scott M. Higgins, *The People Factor in Cyber Breach*, FAST COMPANY (Oct. 14, 2016, 9:00 AM), https://www.fastcompany.com/3064490/growth-notes/the-people-factor-in-cyber-breach.

82. *See* VERIZON, *supra* note 79, at 2.

83. Not all hackers are nefariously motivated. Security researchers, often labeled as white hat hackers, will intrude systems to expose vulnerabilities. Unfortunately, the line between "criminal hackers" and "white hat hackers" is ambiguous, which puts white hat hackers at risk of criminal culpability. For example, in August 2017, the FBI arrested Marcus Hutchins on suspicion that the security researcher developed and/or sold the malware strain Kronos. Hutchins is known for stopping the spread of the WannaCry ransomware and is seen as a white hat hacker by most in the security community. *See, e.g.*, Brian Krebs, *Who Is Marcus Hutchins*, KREBS ON SECURITY (Sept. 5, 2017, 6:50 AM), https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/.

84. Jon Mills et al., *Ashley Madison—Intrusion and the Family*, UF L. FAC. BLOGS, https://facultyblogs.law.ufl.edu/ashleymadisonintrusionandthefamily/ (last visited Jan. 19, 2017).

85. While "revenge porn" is commonly not treated as a data breach, the republication of nonconsensual intimate media is a frustrating example of the horrendous amount of damage that can occur after an initial data intrusion. *See generally* Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. (forthcoming Sept. 2017) (detailing the harms of revenge porn and discussing the trend of states criminalizing the unauthorized disclosure of sexually explicit images of adults). For example, in 2014, Ryan Collins used phishing

to prevent or punish the third-party publication—particularly in the United States. The legal issue becomes balancing intrusion against free speech principles.[86] Often, the republisher who copies and redistributes the hacked information may be protected by free speech principles. Relevant factors that may determine the outcome of legal challenges to republishers include: How was the information obtained? Did the republisher have a role in hacking or stealing the information, or were they an innocent third party? Is the disclosure of the content illegal, overly intrusive, or without justification? Was the subject of the publication newsworthy? Generally, content of the disclosure may not be considered, except in some limited constitutionally accepted restraints on speech relating to national security,[87] obscenity, defamation, fraud, incitement, and speech integral to criminal conduct.[88] However, these cases are few and far between. Usually courts have allowed publication of dangerous, intrusive, and even illegally obtained information by third parties. [89]

B. *How Did the Intrusion Occur?*

The method of intrusion is also relevant to the legal analysis and legal liability. Data stolen *despite* an advanced security system differs significantly from data stolen *because of* a weak security system. In the wake of the Target hack, there were several reports regarding the company's flawed security standards.[90] Failure to meet technical or any

techniques to hack into the iCloud and Google accounts of several celebrities and then disseminated private, mostly nude images and videos of the celebrities. After several weeks of the media being shared privately, the photos and videos were posted on several online forums—including 4chan and Reddit. In the span of one day, a subreddit titled "the Fappening" amassed over 100,000 subscribers. The willingness of both individuals and websites to non-consensually republish the intimate media prolonged the celebrities' victimization and amount of harm suffered. *See generally* Adrienne Massanari, *#GamerGate and The Fappening: How Reddit's Algorithm, Governance, and Culture Support Toxic Technocultures*, 19 NEW MEDIA & SOC'Y 329 (2015); *Lancaster County Man Sentenced to 18 Months in Federal Prison for Hacking Apple and Google E-Mail Accounts Belonging to More than 100 People, Including Many Celebrities*, U.S. ATTORNEY'S OFFICE, MIDDLE DIST. OF PA., DEP'T OF JUSTICE (Oct. 27, 2016), https://www.justice.gov/usao-mdpa/pr/lancaster-county-man-sentenced-18-months-federal-prison-hacking-apple-and-google-e-mail.

86. *See, e.g.*,. Bartnicki v. Vopper, 532 U.S. 514 (2001); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

87. *See* Near v. Minnesota, 283 U.S. 697, 716 (1931).

88. United States v. Stevens, 559 U.S. 460, 468–69 (2010).

89. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (holding the government could not use the national security exception to enjoin newspapers from publishing government documents).

90. Jaikumar Vijayan, *Target Breach Happened Because of a Basic Network Segmentation Error*, COMPUTERWORLD (Feb. 6, 2014, 6:28 AM), http://www.computerworld.com/article/

other reasonable security measures can spell liability. The class action lawsuit filed against Target specifically complained of rampant disregard of industry standard violations and negligence after the company ignored reports of the vulnerabilities of their point of sale system.[91] Target's negligent adherence to ineffective security protocols potentially exposed it to more liability than if the company had simply followed industry standards and heeded expert advice.[92] The subsequent *FTC v. Wyndham Worldwide Corp*.[93] decision reinforces the fact that negligence in maintaining cyber security incurs legal liability.[94] In addition to penalizing Wyndham, that case confirmed the FTC's right to hold companies to a standard of care for customer data.[95]

However, some intrusions are seemingly unavoidable. A company could abide by all security standards and still be hacked by a sophisticated group of cyber-criminals. This gap between cyber defense regulations and sophisticated attacks is largely due to the rapid development of technology. Abiding by regulations and standards created ten, five, or even two years ago does not necessarily prepare a company for the evolution of a modern cyber-criminal attack.[96] Experts now advise companies to accept that that data breaches are virtually inevitable and focus on how to respond, as well as how to secure their most valuable data through encryption, controlling access, and authorization.[97]

This is especially true as these attacks become even more unpredictable. Cybercriminals have begun deploying ransomware attacks on soft targets, such as hospitals and law firms. After hacking into the system by exploiting software vulnerabilities, the criminals gain access

---

2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html; *see also* Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG: BUSINESSWEEK (Mar. 17, 2014, 10:31 AM), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

91. Class Action Complaint at 12–13, Trustmark Nat. Bank v. Target Co., No. 1:14CV02069, 2014 WL 1229602 (N.D. Ill. Mar. 24, 2014).

92. Joel Schectman, *Banks Heap Suits on Target over Breach*, WALL ST. J. (Feb. 7, 2014, 3:06 PM), http://blogs.wsj.com/riskandcompliance/2014/02/07/banks-heap-suits-on-target-over-data-breach/.

93. 799 F.3d 236 (3d Cir. 2015).

94. *Id.* at 246; *see infra* pp. 796–97.

95. *Wyndham*, 799 F.3d at 246.

96. *See* Joe Dysart, *'Ransomware' Software Attacks Stymie Law Firms*, A.B.A (June 1, 2015, 2:30 AM), http://www.abajournal.com/magazine/article/ransomware_software_attacks_stymie_law_firms; Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

97. *See* GEMALTO & SAFENET, 2014 YEAR OF MEGA BREACHES & IDENTITY THEFT 11 (2014), http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

to PII and other confidential information and then threaten to expose the information if the ransom is not paid. For example, the 2017 WannaCry and Petya attacks used leaked NSA exploits to cripple networks across the globe. Notably, the Petya attack successfully targeted DLA Piper, an international law firm that touted its cybersecurity prowess.[98] In addition to reputational harm, the attack left the firm without phone and internal document access for at least one day and without email access for nearly a week.[99]

As discussed, data breaches do not end with the intrusion, and often republication by third parties cause the most harm.[100] Though the First Amendment protects most republishers, in *Bartnicki v. Vopper*[101] the U.S. Supreme Court set forth a three-part balancing test that weighs the conduct of the defendant, the public importance of the disclosure, and the nature of the disclosure.[102] This balancing test determines the chance of success in limiting the dissemination and has become the essential rubric for determining the legality of such disclosures.[103]

Therefore, the *Bartnicki* analysis is important in examining publication of data breaches. In *Bartnicki*, the Court found that broadcasting a stolen audio recording was protected by the First Amendment because of the public importance of the recording, and because the defendant himself did not conduct the initial breach even though he knew it was obtained illegally.[104] However, the Court indicated it would consider punishing disclosure if the disclosing party engaged in illegal activity to obtain the information.[105]

The logic of *Bartnicki* supports balancing privacy and publicly important information, sometimes with opposing outcomes. In *Dahlstrom v. Sun Times Media, LLC*,[106] the U.S. Court of Appeals for the Seventh Circuit used the *Bartnicki* three-part test to determine that publication of illegally obtained information was wrongful.[107] The court

98. *See* Sam Reisman, *Days After Hack, DLA Piper Restores Email Service*, LAW360 (June 30, 2017 6:35 PM), https://www.law360.com/articles/940448/days-after-hack-dla-piper-restores-email-service.

99. *Id.*

100. *See supra* Section I.C.

101. 532 U.S. 514 (2001).

102. *See id.* at 525, 527, 534.

103. *See* Eric B. Easton, *Ten Years After:* Bartnicki v. Vopper *as a Laboratory for First Amendment Advocacy and Analysis*, 50 U. LOUISVILLE L. REV. 287, 330 (2011).

104. *See Bartnicki*, 532 U.S. at 529–30, 533–34.

105. The Court, citing to New York v. Ferber, 458 U.S. 747 (1982), identifies the dissemination of child pornography as an example of a "rare occasion[] in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another." *Bartnicki*, 532 U.S. at 528–30.

106. 777 F.3d 937 (7th Cir. 2015), *cert. denied*, 136 S. Ct. 689 (2015).

107. *Id.* at 953.

reasoned that publisher misconduct, combined with the determination that the information was not of great public interest, meant that disclosure was not protected by the First Amendment.[108] The court also recognized that the statute in question, the Driver's Privacy Protection Act (DPPA), limited disclosure of data based on the categorization and the source of the data.[109] Importantly, because the statutory limitation was not based on *content*, the review of the statute's constitutionality did not face strict scrutiny.[110] The particular data in question were records of police officers that disclosed personal information from DPPA records.[111] The issue is therefore a hybrid because the restriction is based on both the source (DPPA) and content (personal information), which the *Sun-Times* argued amounted to prior restraint.

The protective order issued by the lower court was also more justifiable because the same information about the officers derived from other sources was permitted to be published, thus reducing the public interest factor of the illegally obtained information.[112] This evaluation is very fact-specific, as are many cases in the privacy-disclosure area.[113] However, this case provides further logic supporting a restriction on disclosure of information that was legally obtained and personal in nature. This same logic may be used to support restrictions on disclosures or publications of sensitive information obtained from a breach. In other words, only a statute restricting disclosure of certain types of sensitive personal information obtained from an unlawful data breach could be constitutional.

Under the *Bartnicki* analysis, if a republisher has no knowledge that the data she seeks to publish was obtained illegally, the right of republication will almost always prevail.[114] This means that bloggers who "innocently" posts stolen material may be protected under the *Bartnicki* standard. Likewise, the *Bartnicki* standard would protect whistleblowers who reveal publicly valuable information such as government or corporate misconduct, while those who reveal private matters unrelated to public affairs are afforded little protection under the Whistleblower Protection Act. Announced in 2001, the *Bartnicki* standard predates many of the technical intrusions society now expects.[115] However, the ability to balance the impact of intrusion against the nature of the disclosure is still

108. *Id.* at 954.
109. *See id.* at 946–49.
110. *Id.* at 949.
111. *Id.* at 941.
112. *Id.* at 953–54.
113. *Id.* at 954
114. *See* Easton, *supra* note 103, at 333.
115. Bartnicki v. Vopper, 532 U.S. 514, 514 (2001).

relevant.[116] The *Bartnicki* standard can provide a bridge to a remedy against harmful republication of leaked or hacked data, particularly in cases where the breach does not contain information of public concern, or where the data was obtained illegally.

III. THE LAWS, REGULATIONS, AND STANDARDS FOR DATA SECURITY

Any entity in possession of personally-identifiable data has certain duties to protect that data. These standards of care are continually evolving based on rapid developments in technology and shifting legal and regulatory standards. If a data breach does occur, there are some firmly established obligations for companies to abide by, but there are many unknown risks. The type of data and position of the data subject determine many of these regulations. One thing is certain—the breached entity must be ready to take immediate responsive action to the breach, or else be exposed to multiple dangers, including legal liability.[117] This Section will explore various federal, state, and international data protection laws, as well as provide examples that show how companies have responded to modern data breaches.

A. *Federal Trade Commission—The Common Law of Privacy*

The principal federal watchdog on privacy issues is now the Federal Trade Commission (FTC). The FTC has a statutory duty to protect consumers, and this federal agency has interpreted this role to allow it to promulgate rules on data collection and protection as well as to punish violators of its standards.[118] Accordingly, the FTC is now the source of

116. Consider the 2016 breaches involving the Democratic National Convention and the NSA. While the exact sources of these two breaches remains unknown, both breaches resulted from hacking and included the publication of highly intrusive information—including donor PII from the DNC breach and the NSA's own hacking tools from the NSA breach. News agencies will have to continue to determine the best way to report on these kinds of breaches, which will have to include decisions regarding how much actual content from the breach to publish. *See generally* Dan Goodin, *Group Claims to Hack NSA-Tied Hackers, Posts Exploits as Proof*, ARS TECHNICA (Aug. 15, 2016, 8:50 PM), http://arstechnica.com/security/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/ (describing the effects of an anonymous group's hack without detailing the specific information the group made public); Dan Spinelli et al., *Identity Thieves Target Dems' Big Donors After DNC Hack*, POLITICO (Aug. 18, 2016, 5:03 AM), http://www.politico.com/story/2016/08/democratic-donors-identity-theft-cyberhack-227140 (detailing the extent of anonymous hacks of donor information without revealing what specific information was made public).

117. Generally, all breached entities must be immediately prepared to respond to potential lawsuits from their consumers, financial institutions, insurers, shareholders, employees, and the government. *See* Melissa Maleske, *The 6 Lawsuits All GCs Face After a Data Breach*, LAW360 (Dec. 9, 2015. 2:17 PM), http://www.law360.com/articles/735838/the-6-lawsuits-all-gcs-face-after-a-data-breach.

118. FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S

most rules and standards for data collection and security.[119] The FTC's seemingly simple authority under Section V of the Federal Trade Commission Act to prevent "unfair or deceptive acts or practices in or affecting commerce"[120] has spawned an entire network of privacy and cybersecurity law as interpreted by the FTC.[121] Despite a relatively small number of professional staff, the FTC has become the most prominent federal agency in privacy policy. The FTC has regulatory authority to protect consumer privacy through the Fair Credit Reporting Act[122] and the Gramm–Leach Bliley Act.[123] Additionally, the FTC regulates data management practices of websites targeted towards children as set forth in the Children's Online Privacy Protection Act.[124]

The FTC drafts enforcement actions and publications that establish industry standards for privacy and security. A company that breaks these standards is immediately put within the crosshairs of Section 5,[125] which grants authority to the FTC to file an action against organizations that engage in "unfair or deceptive . . . practices."[126] The FTC investigates and cites hundreds of companies for violations of regulatory standards. In addition, the FTC will punish companies that fail to comply with their own privacy policies—even if their actions square with FTC standards.[127] That sanction is imposed because misrepresentations of privacy or security policies is a violation of fairness standards even when the policies comply with technical standards. Data security violations can include: allowing data to be exposed by inadequate encryption or flawed security software, failure to test a security system, failure to implement

---

INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY 2 (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

119. 15 U.S.C. § 45 (2012).

120. *Id.* § 45(a)(1).

121. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY ch. 6–11 (2016) (surveying the FTC's authorities on specific issues such as online privacy, information security and international privacy efforts).

122. Pub. L. No. 91-508, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C. § 1681 (2012)).

123. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. §§ 6801–09); *see* FED. TRADE COMM'N, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT 1, 4 (2002), https://www.ftc.gov/system/files/documents/plain-language/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act.pdf.

124. Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified as amended at 15 U.S.C. §§ 6501–06); *see* HOOFNAGLE, *supra* note 121, at 198–99.

125. ch. 311, § 5, 38 Stat. 717, 719–20 (1914) (codified as amended at 15 U.S.C. § 45).

126. 15 U.S.C. § 45(a)(1).

127. *See, e.g.*, *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMMISSION (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

security procedures, failure to assess procedures, failure to implement industry standards, failure to minimize data collection, failure to train employees, failure to monitor recipients, such as contractors or third parties, and inadequate password protocols.[128]

Dependent on the rapid development of technology, the manner in which companies collect and use data is unpredictable. Accordingly, in an effort to uphold their mission to protect consumers, the FTC has built their regulatory regime upon the principle of adaptability. FTC enforcement actions are not always spurred by actual breaches. The FTC can also find violations of their suggested practices (as provided in *Start with Security: A Guide for Business*), such as inadequate mode of collection, storage, usage of data, or failure to notify consumers about these inadequacies.[129] These suggested practices are further reinforced through the FTC's blog series, *Stick with Security: Insights into FTC Investigations*.[130] The FTC may also punish a company that violates its own terms of service under the deceptive practices theory, even if the data management practice would otherwise be considered adequate.[131] Some industry representatives have commented that companies may be better situated by not making any representations about privacy other than those absolutely required.[132]

These punishments are initiated by FTC staff and are either a product of their own investigations or a result of consumer complaints. These actions usually end in settlements—213 occurred as of August 2017[133]—although some violations have occasionally gone to trial.[134] Settlements are usually in the form of a consent decree, and the company agrees to stop the disputed act. If a consent decree is violated, the FTC may fine the corporate data custodian up to $60,654 for each violation.[135] The fine can reach exceedingly high amounts if a company violates a consent

128. *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 3–8, 10, 12–14 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

129. *Id.*

130. *Stick with Security: Insights into FTC Investigations*, FED. TRADE COMMISSION (JULY 21, 2017, 10:57 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.

131. *See* FED. TRADE COMM'N, *supra* note 128.

132. *Id.*

133. FED. TRADE COMM'N, LEGAL RESOURCES 1 (2017), https://www.ftc.gov/tips-advice/business-center/legal-resources?title=&type=case&field_consumer_protection_topics_tid=245&field_industry_tid=All&field_date_value%5Bmin%5D%5Bdate%5D=&field_date_value%5Bmax%5D%5Bdate%5D=August+24%2C+2017&sort_by=field_date_value.

134. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

135. *FTC Publishes Inflation-Adjusted Civil Penalty Amounts*, FED. TRADE COMMISSION, (Jan. 12, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts.

decree or court order through the continued failure to protect consumer data. For example, the FTC levied a $100 million fine against LifeLock Inc. after the FTC determined that the company violated a 2010 federal court order requiring the company to secure consumers' personal information and prohibiting deceptive advertising.[136]

As a federal agency, the composition and focus of the FTC is often subject to political changes, including federal elections. Commissioners serve seven-year terms, and if there is a vacancy, the President of the United States nominates an individual to fill the position and the nominee must then be confirmed by the United States Senate.[137] While no more than three of the five Commissioners can be of the same political party, the President selects one Commissioner to act as Chairman.[138] Predictably, the Chairman's focus can significantly alter the FTC's direction. For example, the appointment of Maureen Ohlhausen as Chairwoman by President Trump in January 2017 is expected to cause the Commission to reprioritize the proof of tangible harm during FTC investigations, which ultimately may cause a reprioritization of corporate data security responsibilities.[139]

Despite this malleability, the effects of the FTC's standards are far-reaching. There is no private cause of action under Section 5 for consumers, but the FTC orders create data management standards that directly benefit consumers and affect standards for liability.[140] Many states have adopted unfair and deceptive trade practices laws modeled after Section 5, and common law negligence causes of actions have developed based off of these state statutes.[141] By setting these standards, the FTC draws the line between effective data protection and violations of fair consumer practices. A breach that occurs because the company fails to comply with the FTC's standards exposes a company to liability for consequences of the breach. Two recent orders against Wyndham Hotel Corporation and LabMD, Inc. illustrate and confirm the FTC's regulatory reach for protecting consumer privacy.

---

136. *See LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order*, FED. TRADE COMMISSION (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

137. *See* FED. TRADE COMM'N, COMMISSIONERS, CHAIRWOMEN AND CHAIRMEN OF THE FEDERAL TRADE COMMISSION (Dec. 2016), https://www.ftc.gov/system/files/attachments/commissioners/ftc_commissioners_history_-_december_2016.pdf.

138. *Id.*

139. *See* Allison Grande, *New FTC Chair to Shift Data Security Focus to Actual Harm*, LAW 360 (Jan. 26, 2017, 9:28 PM), https://www.law360.com/articles/885212/new-ftc-chair-to-shift-data-security-focus-to-actual-harm.

140. *See infra* note 147 and accompanying text.

141. *See* FLA. STAT. § 501.204(1) (2016).

1. *FTC v. Wyndham Worldwide Corp.*

The U.S. Court of Appeals for the Third Circuit in *FTC v. Wyndham Worldwide Corp.*[142] reinforced the FTC's central role in data security. After a data breach, the Wyndham Worldwide Corporation argued that the FTC did not have the statutory authority to penalize it for security failures and that it did not have constitutional notice of potential liability. In other words, since the FTC had no explicit statutory authority to set security standards, Wyndham could not have fair notice of FTC standards. This challenge went to the core of the FTC's authority to regulate privacy. Yet, the court rejected those arguments, concluding that the FTC had authority to regulate data security practices under the unfairness prong of the FTC Act, the company's practices did not fall outside the plain meaning of unfair, and that previous FTC adjudications and interpretive guidance provided the company with fair notice.[143]

In addition to misstating their own privacy policy in an unfair way, Wyndham's substantial list of security transgressions included allowing payment card information to be available in readable text and failing to monitor for malware.[144] The Third Circuit agreed with the FTC that Wyndham had engaged in cybersecurity practices that "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[145] More notably, the court agreed that the FTC—as the focal point of cybersecurity policy to protect consumers—has the authority to interpret statutes, including 15 U.S.C. 45(a).[146] This opinion marked a major victory for FTC authority. Consequently, corporations like Wyndham are put on notice of cybersecurity standards from FTC consent orders as well as other administrative guidance.[147] In the wake of this decision, corporations must regularly assess their own security practices, track security rulings and law changes, and be aware that an FTC violation could subject the company to future negligence charges. For example, if a company does not encrypt sensitive information stored on its computer network,[148] this failure could constitute a breach of an applicable security standard in a negligence action. In sum, then-FTC chairperson Edith Ramirez identified the Wyndham case as one of importance for the future of data security:

142. 799 F.3d 236 (3d Cir. 2015).
143. *Id.* at 244–55.
144. *Id.* at 258.
145. *Id.* at 240.
146. *Id.* at 253–55, 259.
147. *Id.* at 257.
148. *See* FED. TRADE COMM'N, *supra* note 128, at 6.

"[T]he court rulings in the case have affirmed the vital role the FTC plays in this important area."[149]

2. LabMD, Inc.

Another example of the FTC's moves for privacy preeminence involves a three-year investigation of the clinical laboratory, LabMD. In 2012, the billing information for over 9,000 LabMD consumers was found on a peer-to-peer file sharing network, which led to the direct exposure of several hundred consumers' records to identity thieves.[150] On July 29, 2016, the FTC issued a Final Order that reversed an administrative law judge's dismissal of the FTC's enforcement action with the main point of contention being whether an actual injury occurred.[151] In the reversal, the FTC specifically reasoned that the federal commission did not have to abide by federal standing requirements, thus promulgating that a cognizable injury is not required for an FTC action.[152] Further, the FTC justified their continued action against the now-defunct LabMD because the company technically still maintained consumer information and may use this information in the future.[153] The issues of whether there is a tangible injury is a major threshold for federal jurisdiction. The issue is critical because negligent security practices may not result in actual injury. For example, the FTC may discover bad practices before there is a breach. If this decision survives appeal, then not only will consumer harm be redefined in injury requirements, but breached companies will be forced to deal with an FTC that can enforce its standards without needing to demonstrate harm.

B. *Federal Communications Commission—Common Carrier Regulation*

As with the FTC, the Federal Communications Commission (FCC) has steadily expanded its regulatory reach. Although, the 2017 shift of leadership has already diverted this growth. The FCC regulates telecommunication companies, cable and satellite television providers,

149. *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, FED. TRADE COMMISSION (Dec. 9, 2015, 12:00 PM), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

150. *LabMD, Inc., in the Matter of*, FED. TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter (last updated Sept. 29, 2016).

151. Final Order at 1, LabMD, Inc., No. 9357 (F.T.C. July 29, 2016).

152. Opinion of the Commission at 20 n.63, LabMD Inc., No. 9357 (F.T.C. July 29, 2016).

153. *Id.* at 36.

and, now, internet service providers (ISPs).[154] The federal agency is empowered primarily by Sections 201(b),[155] 222,[156] and 551[157] of the Communications Act and utilizes the "just and reasonable" language in its authorizing legislation in similar way to how the FTC leverages its power with the "unfair and deceptive acts" language in Section 5. Similar to how health entities have a duty to secure protected health information (PHI), telecommunication carriers have a specific duty to protect the unique form of data that they collect about their consumers. This data is called Customer Proprietary Network Information (CPNI) and includes a wide range of information including the date of a call or the destination number of each call.[158]

In addition to providing guidance as how to best protect CPNI, the FCC has initiated actions against telecommunication companies to enforce data management standards. In October 2014, the FCC found two breached telecommunications companies—TerraCom Inc. and YourTel—in violation of § 201 and § 222 for the companies' use of unsecure internet-based (cloud) storage of customer data.[159] While initially planning to fine the companies $10 million,[160] the ultimate fine totaled only $3.5 million.[161] In another example, the FCC levied a civil penalty of $25 million for AT&T's failure to take "every reasonable precaution" to protect customer data after two AT&T employees sold customer information to a third party and exposed the data of 51,422 AT&T customers.[162] Only a few months later, the FCC assessed a

154. *See* Report and Order on Remand at 3, 10, 14, 17, 22, 82–83, Protecting & Promoting the Open Internet, GN Docket No. 14-28 (F.C.C. Mar. 12, 2015).

155. 47 U.S.C. § 201(b) (2012) ("All charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable.").

156. *Id.* § 222 (proscribing a duty on telecommunications carriers to "protect the confidentiality of proprietary information" of their customers and defining CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier").

157. *Id*. § 551 (defining notice requirement for cable operators and prohibiting cable operators from "us[ing] the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned").

158. *Id.* § 222.

159. Press Release, Fed. Commc'n Comm'n, FCC Plans $10 Million Fine for Carriers That Breached Consumer Privacy (Oct. 24, 2014), http://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy.

160. *Id.*

161. Press Release, Fed. Commc'n Comm'n, TerraCom and YourTel to Pay $3.5 Million to Resolve Consumer Privacy & Lifeline Investigations (July 9, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-334286A1.pdf.

162. Order ¶ 1, AT&T Servs., Inc., DA 15-399 (F.C.C. Apr. 8, 2015).

$595,000 penalty on Cox Communications in the FCC's first ever enforcement action on a cable company.[163] An FCC investigation into a third-party hack of Cox's system revealed that the company failed to adequately protect CPNI and PII.[164] Although the FCC primarily focused on Cox's failure to protect customer information, the FCC also chastised the company's violation of FCC notification standards.[165] While AT&T and Cox simply failed to notify the FCC of the breaches within the mandated seven-day period, TerraCom and YourTel only notified the FCC after a news reporter discovered the breach.[166]

This reinvigorated level of enforcement became particularly important when the Ninth Circuit—in an opinion that the court has since ordered to be reheard—held that common carriers are exempt from FTC Section V actions.[167] As a result of this perceived gap, the FCC began exploring new ways to exert their authority even beyond the enforcement actions discussed above.

In 2015, the FCC and FTC signed a *Memorandum of Understanding*, which clarified that the FTC can target and fine common carriers for any of their non-common carrier activities, such as any Fair Credit Reporting Act violations.[168] In 2016, the FCC publicized their Notice of Proposed Rulemaking (NPRM) that seeks to increase privacy protections for customers of broadband and other telecommunications services.[169] Two of the most controversial components of the NPRM included (1) tighter restrictions for the protection of customer data[170] and (2) extensive data breach notification requirements including mandated adoptions of risk management procedures and the obligation to notify affected customers no later than ten days after the breach.[171] While the NPRM received extensive support from digital liberties organizations,[172] State Attorneys

163. Order ¶ 4, Cox Commc'ns, Inc., DA 15-1241 (F.C.C. Nov. 5, 2015).

164. *Id.* ¶ 1.

165. *Id.* ¶ 2.

166. *See* Press Release, Fed. Commc'n Comm'n, *supra* note 161.

167. *See* FTC v. AT&T Mobility LLC, No. 15-16585, 2016 WL 4501685, at *4 (9th Cir. Aug. 29, 2016), *reh'g en banc granted sub nom.*, Fed. Trade Commn. v. AT&T Mobility LLC, 864 F.3d 995 (9th Cir. 2017).

168. FCC-FTC, FCC-FTC CONSUMER PROTECTION MEMORANDUM OF UNDERSTANDING 2 (2015), https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

169. Notice of Proposed Rulemaking, Protecting the Privacy of Customers of Broadband & Other Telecomm. Servs., WC Docket No. 16-106 (F.C.C Apr. 1, 2016).

170. *Id.* ¶¶ 60–66.

171. *Id.* ¶¶ 174, 234.

172. Letter from Access Humboldt et al. to Tom Wheeler, Chairman, FCC (Sept. 7, 2016), https://www.aclu.org/letter/coalition-letter-urging-fcc-reject-calls-weaken-broadband-privacy-rule.

General[173] and the telecommunications industry[174] staunchly opposed the NPRM as unnecessarily draconian. The negative reaction to the NPRM led then-FCC Chairman Thomas Wheeler to release an updated version of the proposed rule. The update included sensitivity distinction to comport with the existing FTC privacy framework, but very little change to the data breach requirements.[175] While the FCC initially adopted the broadband privacy rules in October 2016,[176] current FCC Chairman Ajit Pai successfully led the effort to stay the enforcement of the rules in March 2017.[177] To formalize this stay, Congress voted to reverse the privacy rules and President Trump signed an official repeal of the rules in April 2017.[178]

Chairman Pai's leadership signals the FCC's likely reduced role in the establishment and enforcement of privacy and data security regulation.[179] Despite this course reversal, it is in the best interest of any company that falls within the common carrier designation to follow both FCC and FTC guidelines, which includes staying up to date on any FCC consent decrees and FTC Section 5 enforcements.[180]

---

173. Kurt Orzeck, *FCC Should Drop ISP Privacy Plan, 16 State AGs Say*, LAW360 (Sept. 19, 2016, 9:00 PM), http://www.law360.com/articles/840974/fcc-should-drop-isp-privacy-plan-16-state-ags-say.

174. Allison Grande, *Internet Group Fights Bid for Uniform FCC Privacy Rules*, LAW360 (Sept. 21, 2016, 9:58 PM), http://www.law360.com/corporate/articles/843055/internet-group-fights-bid-for-uniform-fcc-privacy-rules.

175. FED. COMMC'N COMM'N, FACT SHEET: CHAIRMAN WHEELER'S PROPOSAL TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION 2 (2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/DOC-341633A1.pdf.

176. *FCC Adopts Broadband Consumer Privacy Rules*, FED. COMM. COMMISSION (Oct. 27, 2016), https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

177. *FCC Moves to Ensure Consumers Have Uniform Online Privacy Protection*, FED. COMM. COMMISSION (Mar. 1, 2017), https://www.fcc.gov/document/fcc-moves-ensure-consumers-have-uniform-online-privacy-protection.

178. Pub. L. No. 115-22; 131 Stat. 88 (2017).

179. *See* Cecilia Kang, *F.C.C., in Potential Sign of the Future, Halts New Data Security Rules*, N.Y. TIMES (Mar. 1, 2017), https://www.nytimes.com/2017/03/01/technology/fcc-data-security-rules.html?mcubz=0.

180. Companies should also stay up to date with any data security guidance released by the National Institute of Standards and Technology (NIST), the Securities and Exchange Commission (SEC), and the Consumer Financial Protection Bureau (CFPB). In 2017, NIST issued a draft update to their 2014 Cybersecurity Framework that sets forth a highly detailed and technical approach for private organizations to better manage cybersecurity risk. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: DRAFT VERSION 1.1 (Jan. 10, 2017), https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf. In 2011, the SEC issued non-binding guidance for publicly traded companies that suffer a significant cybertheft or are vulnerable to such an attack. For example, the SEC encourages these companies to disclose a cybersecurity incident if it renders an investment in the company risky or if the incident materially affects its products, services, customer relationships, or competitive conditions. *See* DIV. OF CORP. FIN. SEC. & EXCH.

C. *Federal Standards in Other Sectors and Requirements for Notification*

In addition to the FTC's broad jurisdiction and FCC regulation of communications, private and public-sector enterprises have additional specific regulatory requirements. Those requirements may be extremely industry specific—such as healthcare data protections set forth in HIPAA. However, there are also more general statutory requirements, such as the breach notification standards that apply across industries, though even these notification standards may differ[181] depending on the specific industry.[182] These statutory duties are codified in several different statutes and federal rules rather than in one comprehensive law. Irrespective of the particular federal legal obligation in a sector, any entity that suffers a breach would be well advised to promptly notify those exposed.

1. Healthcare Data

Among the various possible private sector breaches, one of the most sensitive is disclosure of healthcare data. HIPAA sets forth the regulatory framework to protect health information. In the event of a data breach, entities in the health sector[183] are required to notify affected individuals by first-class mail or email. The health care provider must also notify the media if the breach affects more than 500 individuals.[184] Further, if a

---

COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2, at 2, 4 (2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. In March 2016, the CFPB initiated their first data security enforcement action against a payment card company that deceived consumers about its data security practices. Citing the increased frequency of data breaches, the CFPB criticized the company's failure to address known security flaws including poor employee practices. *See* Press Release, Consumer Fin. Prot. Bureau, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

181. A 2010 Congressional Research Service Report provides a comprehensive discussion of the patchwork of federal data breach notification standards. *See* GINA STEVENS, CONG. RES. SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 4 (2010).

182. In 2015, Congress considered several data breach bills that would create a more standardized data breach response across the sectors. The Center for Democracy and Technology analyzes four of the more prominent data breach bills in this 2015 report. *See generally* CTR. FOR DEMOCRACY & TECH., COMPARISON OF FOUR DATA BREACH BILLS CURRENTLY BEFORE CONGRESS (114TH SESSION) 1 (2015), https://cdt.org/files/2015/09/2015-09-09-Federal-DBN-Bills-Comparison-Chart_2.pdf.

183. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 11-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

184. 45 C.F.R. §§ 164.400–.414 (2017).

"business associate" entrusted with patient information is breached, the associate must notify covered entities without unreasonable delay within sixty days of the breach.[185] These protections are of a particular importance now as the healthcare industry has come under continual assault from various hackers including the deployment of ransomware to blackmail the provider.[186]

2. Education Data

Though education data has heightened privacy protections, the education sector does not have breach notification requirements, nor are they the subject of rigorous regulation by the FTC or FCC. In fact, the 2008 amendment to the Family Educational Rights and Privacy Act (FERPA) specifically detailed how:

> The [U.S.] Department [of Education] does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA requires only that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student's education record.[187]

The amendment advises that student notification may be triggered if the breach involves a social security number or other information that would increase the likelihood of identity theft.[188] The Department of Education recommends that an institution should notify the Family Policy Compliance Office (FPCO) if a breach does occur.[189] Regardless of notification, the FPCO has the authority to conduct its own investigation of the breach.[190] If reintroduced in a future session, the proposed Student Privacy Protection Act would amend the current standards by requiring parental notification if a student's data is accessed.[191] As student data is increasingly stored using cloud computing,[192] and education technology

185. *Id.* § 164.410(b).

186. *See* discussion *infra* pp. 788–89.

187. PRIVACY TECH. ASSISTANCE CTR., DATA BREACH RESPONSE CHECKLIST 3 (2012), http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf.

188. *Id.*

189. *Id.* at 9.

190. 34 C.F.R. § 99.64(b) (2017).

191. Student Privacy Protection Act, S. 1341, 114th Cong. (2015).

192. *See* Family Educational Rights and Privacy, Final Rule, 76 Fed. Reg. 75603, 75612 (Dec. 2, 2011); *see generally* PRIVACY TECH. ASSISTANCE CTR., FREQUENTLY ASKED QUESTIONS–CLOUD COMPUTING 1, 4 (2012), http://ptac.ed.gov/sites/default/files/cloud-computing.pdf.

platforms become mainstream teaching tools,[193] FERPA protection of education data will need to be further updated to anticipate security challenges unique to sensitive digital data.

3. Financial Data

In the financial sector, Title V of the Gramm–Leach–Bliley Act (GLBA)[194] requires financial institutions to notify individuals as soon as possible if the institution determines that misuse of PII has occurred or is reasonably possible. Due to the lack of enforcement mechanisms in the GLBA, the FTC will intervene to initiate compliance if an institution violates the data security or privacy standards.[195] Beyond notification standards, the SEC has established a series of cybersecurity "requests" for corporate boards.[196] SEC requests range from establishing a corporate culture of data security to having procedures in place in case of a data breach.[197] In a similar vein, the Financial Industry Regulatory Authority also released its 2015 Cybersecurity Report on Best Practices, which provides an extensive data security guide for broker-dealers.[198]

4. Data Managed By Government and Government Contractors

In 2015, hackers compromised the data of 4 million federal employees in the massive Office of Personnel Management breach.[199] In the event of a breach, the federal government must adhere to standards set by Office of Management and Budget Memorandum M-07-16.[200] For

193. *See* Press Release, U.S. Dep't of Educ., Department of Education Launches the Educational Quality Through Innovative Partnerships (EQUIP) Experiment to Provide Low-Income Students with Access to New Models of Education and Training (Oct. 14, 2015), http://www.ed.gov/news/press-releases/fact-sheet-department-education-launches-educational-quality-through-innovative-partnerships-equip-experiment-provide-low-income-students-access-new-models-education-and-training; *see also* FLA. STAT. § 1004.0961 (2016) (beginning in the 2015–2016 school year, Florida students can earn academic credit for online courses).

194. Pub. L. No. 106-102, 113 Stat. 1338, 1437 (1999) (codified as amended at 15 U.S.C. §§ 6801–09 (2012)).

195. 16 C.F.R. § 314 (2017).

196. OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE 2 (2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

197. *Id.*

198. *See* FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 1 (2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

199. Spencer Ackerman, *US Government Responds to Latest Hack: Give Us More Power over Data Collection*, GUARDIAN (June 5, 2015, 3:06 PM), https://www.theguardian.com/technology/2015/jun/05/us-government-opm-hack-data-collection-powers.

200. Memorandum from Deputy Dir. for Mgmt. of the Office of Mgmt. & Budget to the Heads of Exec. Dep'ts & Agencies (May 22, 2007), https://www.whitehouse.gov/sites/

instance, a federal agency must internally disclose a breach of PII within one hour of becoming aware of the breach.[201] However, external notification is not as immediate and must be done only without "unreasonable delay."[202]

Another specific set of sector regulations apply to government contractors who handle Controlled Unclassified Information (CUI) and other federal information. Edward Snowden, for example, gained access to NSA data as an employee of Booz Allen Hamilton, a private sector contractor.[203] In 2015, the National Institute of Standards and Technology (NIST) issued updated guidelines for federal agencies working with contractors who handle CUI.[204] Because the guidelines do not impose strict requirements for the contractors to adopt, inconsistencies between different contractors are likely to develop. In May 2016, the Department of Defense, General Services Administration, and the National Aeronautics and Space Administration released a Final Rule to be added to the Federal Acquisition Regulation regarding the basic safeguarding of contractor information systems.[205] The rule is applied with other federal requirements, but also maps out the basic cyber security practices to be adopted by all contractors that "process[], store[], or transmit[] [f]ederal contract information."[206] These practices include: authenticating or verifying the identities of users, processes, and devices before allowing access to an information system; sanitizing or destroying information system media containing federal personnel contract information before disposal, release, or reuse; and performing periodic malicious code scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.[207]

---

whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

201. *Id.*

202. *Id.*

203. Julian Borger, *Booz Allen Hamilton: Edward Snowden's US Contracting Firm*, GUARDIAN (June 9, 2013, 5:01 PM), https://www.theguardian.com/world/2013/jun/09/booz-allen-hamilton-edward-snowden.

204. These guidelines are not in and of themselves legally binding. However, failure to follow industry standards can be risky. *See* RON ROSS ET AL., NAT'L INST. OF STANDARDS & TECH., PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 12 (2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

205. Federal Acquisition Regulation for Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30,439, 30,439 (May 16, 2016) (to be codified at 48 C.F.R. pts. 4, 7, 12, and 52).

206. *Id.* at 30,445.

207. *Id.* at 30,446.

D. *State Standards for Breach Notification*

In addition to the complex federal standards, forty-eight states have enacted data breach notification laws. California was the first state to enact a law requiring notification to victims of a data breach.[208] The statute requires a data custodian to notify the original creator or "owner" of the data when data is disseminated to an unauthorized person.[209] Most other states have since adopted similar statutes that require prompt notification when a data breach occurs and authorize civil penalties when notification is delayed or not made.[210] However, if the data is encrypted, forty-seven states plus the District of Columbia, Guam, Puerto Rico, and Virgin Islands exempt the entities from these notification requirements.[211] Despite one in five breaches involving paper records,[212] several states require notification if the data breach concerns electronic records only.[213] Some states require notification immediately after a breach occurs, while others allow the data custodian to assess the potential risk of harm to the person before determining whether to issue notification.[214] Data custodians face consequences for failing to notify or for making an untimely notification that vary from a small fine issued by a state agency to a private right of action for damages.[215]

The multitude of statutes across the states create a patchwork of standards and enforcement.[216] Thirty-one states, plus Puerto Rico and the District of Columbia, have enacted legislation that broadens the general definition of personal information to reflect the changing technical landscape, including username and passwords, answers to security

208. *See* FCC-FTC, *supra* note 168, at 1.

209. GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 3 (2012).

210. *Id.*

211. *See* BAKER & HOSTETLER LLP, STATE DATA BREACH LAW SUMMARY 24–27 (2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

212. Melinda L. McLellan, *2015 BakerHostetler Incident Response Report Shows One in Five Breaches Involved Paper Records*, BAKERHOSTETLER (June 1, 2015), https://www.dataprivacymonitor.com/data-breaches/2015-bakerhostetler-incident-response-report-shows-one-in-five-breaches-involved-paper-records/.

213. *See Many State Data Breach Laws Don't Protect Paper Records*, BLOOMBERG BNA: TECH., TELECOM & INTERNET BLOG (Jan. 12, 2009), http://www.bna.com/state-data-breach-b12884907245/.

214. STEVENS, *supra* note 209, at 6.

215. Steptoe & Johnson, LLP has created an excellent catalog of the different types of penalties different state notification laws authorize. STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS 3 (2016), http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf.

216. *See* BAKER & HOSTETLER LLP, *supra* note 211, at 1.

questions, or biometric data as PII.[217] Alternatively, some states employ a catch-all definition as exemplified by New York's statute: "Personal information means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."[218]

Most state statutes do not enable civil action if the personal data was acquired in encrypted form.[219] However, a handful of state statutes provide that if encrypted data is obtained along with access to the encryption key, it renders the data as accessible as if it were unencrypted, and, accordingly, a civil action remedy is available.[220]

Many states give exclusive power to the attorney general to enforce data breach notice statutes,[221] but some states provide exemptions to this standard, carving out the power for individuals to pursue civil remedies. Fourteen, plus the District of Columbia, Puerto Rico, and the Virgin Islands, permit a civil cause of action for data breaches, while Texas and Tennessee address data breach damages under their respective consumer protection acts.[222] Even where a state provides an avenue for relief, demonstrating sufficient damages for a claim may be a challenge.[223] Most states impose time limits and restrictions on monetary damages, such as the District of Columbia statute, which expressly states that damages may not include dignitary damages such as pain and suffering.[224]

Emerging state standards may soon become industry standards and targets for other federal and state governments alike. For example, in the financial services industry, the New York Department of Financial Services (DFS) is setting a high bar with its highly detailed cybersecurity regime, which partially went into effect on March 1, 2017.[225] This regulation requires covered entities to implement an internal cybersecurity program and policy, requires third-party service providers to have a cybersecurity policy, hire a chief information security officer,

217. *Id.* at 2–9.

218. N.Y. GEN. BUS. LAW § 899-aa(1)(a) (McKinney 2016).

219. For example, Arkansas's statute notes how the statute only applies to "unencrypted data elements." BAKER & HOSTETLER LLP, *supra* note 211, at 24.

220. *See id.* at 24–27.

221. State Attorneys General (AGs) are further expanding the role in data breaches by using these notification laws to step in when the FTC fails to take action. For example, the New York AG entered into a settlement with Uber mandating the adoption of new authentication and encryption practices. Allison Grande, *Uber Privacy Pact Shows New Enforcement Role for State AGs*, LAW360 (Jan. 11, 2016, 10:47 PM), http://www.law360.com/articles/745180/uber-privacy-pact-shows-new-enforcement-role-for-state-ags.

222. *See* BAKER & HOSTETLER LLP, *supra* note 211, at 22–23.

223. *See generally* Elizabeth D. de Armond, *A Dearth of Remedies*, 113 PA. ST. L. REV. 1, 7–8 (2008) (discussing federal gaps and the states' role in protecting data privacy).

224. *See* BAKER & HOSTETLER LLP, *supra* note 211, at 23.

225. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

comply with access privileges and personnel/intelligence requirements, adopt an incident response plan, and bear the responsibility to provide notice of qualifying security to the DFS superintendent.[226] The existence of state requirements and standards presents a challenge to every multistate enterprise. For example, the litigation surrounding the Target breach included allegations of violations of certain state standards where civil actions were authorized, as well as federal standards. Interstate enterprises are well advised to be aware of state security and notification standards.

IV. PRIVATE CAUSES OF ACTION OR RESPONSES TO A DATA BREACH

Providing legal remedies for victims of breach presents novel challenges. Government actions are limited to penalizing companies or punishing hackers. Government sanctions against companies can be significant and harmful to these private entities, but harmed individuals have had limited success because of outdated or inadequate remedies. Based on the continued frequency of data breaches, government actions alone are neither an effective deterrent to hackers, nor an adequate remedy for harmed individuals.

For any given data breach, there may be multiple plaintiffs and also numerous defendants. The breached entity may seek recovery from others who are responsible for the data breach. For example, the harmed company may seek relief against the hacker, an individual causing the breach, a data custodian, a service provider, or a subcontractor. Other injured parties—other than the exposed individual—may seek recovery against the breached company. Common examples are banks or credit card companies who are legally accountable to customers whose credit card data was stolen and used.[227] Most often, the individual must join a class action option, which reflects the relatively small nature of the losses, but also presents multiple approaches to seeking compensation. Even though the common law remedies have yet to be highly effective, there are, *hypothetically*, a plethora of options available.

A. *Negligence*

A plaintiff in a data breach class action premised on negligence will allege that the company, as the data custodian, had a duty to exercise reasonable care in protecting the plaintiff's PII, the company breached

226. *Id.*

227. Banks and credit card companies will compensate customers for fraudulent charges, but seek reimbursement—with varying degrees of success—from retail companies for expenses incurred through a data breach. Julie Creswell, *As Online Data Theft Escalates, Banks Look to Retailers to Bear the Losses*, N.Y. TIMES (Sept. 28, 2015), http://www.nytimes.com/2015/09/29/business/as-online-data-theft-escalates-banks-look-to-retailers-to-bear-the-losses.html.

that same duty, and that this breach caused the resulting damages, for example, allowing or inducing the data breach.[228] Typical claims brought against a data custodian premised on negligence may be negligent or unreasonable data security practices, failing to fix compromised security systems, failing to test a network security system, or breaching a general duty to keep consumer's data safe.[229] In these negligence actions, the standard of care is a central issue during litigation.[230]

These actions may allege that the data custodian "enables cybercrime, unreasonable data security practices, or fail[s] to fix known security vulnerabilities that compromise confidential information."[231] Another approach to establish liability is grounded in statutory standards for data custodians, "such as vendor liability under Article 2 of the Uniform Commercial Code (UCC) or the application of professional malpractice law to software programmers."[232] Still other plaintiffs have pled liability on grounds of a breach of fiduciary duty, alleging that the plaintiff relied on the company holding the data, which was in a position of trust and confidence to use the data to the plaintiff's benefit.[233]

Regardless of the particular negligence theory a data breach victim utilizes in a suit against the data custodian, the greatest hurdle data breach victims face when suing in negligence is the economic loss rule.[234] This time-honored legal doctrine precludes recovery in tort for economic losses where the economic loss does not stem from a causally related personal injury or tangible property damage.[235] However outdated, courts

228. *See* Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010).

229. *See In re* Sony Gaming Networks & Customer Data Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (explaining that plaintiffs in a data breach class action alleged that Sony violated a duty to consumers to provide reasonable network security and "allege[d] [that] this duty included, among other things, the duty to design, implement, maintain, and test Sony's security system in order to ensure Plaintiff's Personal Information was adequately secured and protected"); William Dalsen, Comment, *Civil Remedies for Invasions of Privacy: A Perspective on Software Vendors and Intrusion upon Seclusion*, 2009 WIS. L. REV. 1059, 1063 (2009).

230. *See In re Sony*, 996 F. Supp. 2d at 972.

231. Dalsen, *supra* note 229, at 1063.

232. *Id.*

233. *See, e.g.*, Daly v. Metro. Life Ins., 782 N.Y.S.2d 530, 535 (N.Y. Sup. Ct. 2004).

234. In 2016, the U.S. Supreme Court chose not to redefine the economic loss rule to allow recovery under a federal cause of action despite the nonexistence of concrete harm. Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("Article III standing requires a concrete injury even in the context of a statutory violation.")

235. For a thorough discussion on the different common law and state-specific statutory exceptions to the economic loss doctrine in a consumer data breach class action, see *In re Sony*, 996 F. Supp. 2d at 966–73; *cf.* Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S 237, 268 n.139 (2007) (noting that plaintiffs have not been successful in "side-stepping" the economic loss rule in data breach cases premised on negligence).

are reluctant to recognize data as legal property.[236] Further, if the victim suffers no financial harm—for example, when a credit card loss is covered by the card company—there is no "economic loss." As a result, data breach victims suing under negligence are frequently unsuccessful in surviving motions to dismiss.[237]

The economic loss rule does not always operate as a total bar to negligence claims. Compensatory damages have been successfully sought against corporate data custodians under theories that held the custodians to a standard to exercise reasonable care of the data regardless of direct economic loss.[238] In some states, noneconomic damages have been permitted in a data breach negligence cause of action. For example, in the recent Target data breach class action, negligence claims survived Target's initial motion to dismiss under Georgia, D.C., Idaho, and New Hampshire law.[239] However, in 2016, the Third Circuit ruled that the economic loss doctrine barred a plaintiff from claiming negligence after a data breach.[240]

Plaintiffs also face justiciability issues such as standing and ripeness when suing in negligence or any other common law action. Many data breach victims can only allege the mere threat of identity theft or other speculative damages rather than particularized damages, such as a dollar amount lost by someone utilizing their personal profile. In other words, it is difficult to assign value to the harm caused in a data breach where the victim has suffered no particular loss. In light of the recent U.S. Supreme Court decision in *Clapper v. Amnesty International USA*,[241] which reemphasized the need for a threatened injury to be "certainly impending" to meet standing requirements,[242] more recent cases have followed the traditional stringent approach to standing.[243] For example, in 2015, a New Jersey federal court denied standing to plaintiffs who had

236. *See* Douglas H. Meal & David T. Cohen, *Private Data Security Breach Litigation in the United States*, ASPATORE, https://webcache.googleusercontent.com/search?q=cache:a4I5Jit356YJ:https://www.ropesgray.com/~/media/Files/articles/2014/February/Meal%2520Chapter.ashx+&cd=1&hl=en&ct=clnk&gl=us (last visited Mar. 10, 2017).

237. *Id.*

238. *See In re Sony*, 996 F. Supp. 2d at 966–73.

239. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1314 (D. Minn. 2014). However, the development of the economic loss rule in Alaska, California, Illinois, Iowa, and Massachusetts required the court's dismissal of certain negligence claims brought by plaintiffs from these states. *Id.*

240. Longenecker-Wells v. Benecard Servs. Inc., No. 15-3538, 2016 WL 4474701, at *1–2 (3d Cir. Aug. 25, 2016).

241. 113 S. Ct. 1138 (2013).

242. *Id.* at 1147.

243. *See, e.g.*, Galaria v. Nationwide Mut. Ins., 998 F. Supp. 2d 646, 655–56 (S.D. Ohio 2014), *rev'd and remanded*, Nos. 15-3386/3387, 2016 WL 4728027, at *1 (6th Cir. Sept. 12, 2016).

their PII and PHI stolen as part of a breach that affected 800,000 patients, and also denied standing to the one plaintiff in the consolidated class action that actually suffered from identity theft after the breach.[244] Nevertheless, some courts have found that the credible threat of harm resulting from a data breach is enough to satisfy standing requirements.[245] The issue of individual remedy or recovery as a victim of a data breach with no defined loss remains uncertain territory.

B. *Fair Credit Report Act Claims*

To invoke subject matter jurisdiction in federal courts, data breach plaintiffs have also attempted to bring a Federal Credit Reporting Act (FCRA)[246] claim against a hacked company. A FCRA claim targets the company's improper transfer of data to unauthorized third parties. Pursuing this statutory violation is an effort to overcome the barrier of the economic loss rule discussed primarily. A May 2016 U.S. Supreme Court decision not only provided an example of this strategy, but also reenergized plaintiffs involved in class action lawsuits that traditionally struggle to establish actual harm.

In *Spokeo, Inc. v. Robins*,[247] Robins argued that Spokeo, a people search website, violated FCRA by publishing inaccurate information about him online.[248] Robins's argument focused on how the inaccurate information negatively affected his search for a job.[249] The U.S. Court of Appeals for the Ninth Circuit agreed with Robins that the statutory violation, as alleged, constituted actual harm sufficient to establish standing.[250] The U.S. Supreme Court did not completely agree. In a 6–2 decision, Justice Samuel Alito, writing for the majority, explained that the allegation of an injury-of-fact requires the injury to be concrete and

244. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., No. 13-7418 (CCC), 2015 WL 1472483, at *4–9 (D.N.J. Mar. 31, 2015) (dismissing the consolidated class action of plaintiffs whose PII and PHI were stolen after two employees' encrypted laptops were stolen).

245. *See* Meal & Cohen, *supra* note 236 (citing, *inter alia*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding plaintiffs had standing because they alleged a credible threat of real and immediate harm of stolen personal information after a laptop was stolen); Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) (finding standing because risk of identity theft from stolen laptop was "real, and not merely speculative"); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634, 640 (7th Cir. 2007) (finding standing because "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions," but dismissing because the cost of credit monitoring is not a compensable damage).

246. Pub. L. No. 91-508, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681 (2012)).

247. 136 S. Ct. 1540 (2016).

248. *Id.* at 1546.

249. *Id.* at 1554 (Ginsburg, J., dissenting).

250. *Id.* at 1544–45 (majority opinion).

particularized.[251] Because the Ninth Circuit failed to fully analyze both of these requirements, the case would need to be reheard by the Ninth Circuit.[252] Fortunately for Robins and other data breach plaintiffs, the Court's ruling is not a complete bar to FCRA or other statutory claims. The Court also recognized that the *risk of harm* could constitute an injury-of-fact. Justice Alito wrote:

> Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any additional harm beyond the one Congress has identified.[253]

Unfortunately, this decision also does not completely clarify this murky issue. Without a clear path, plaintiffs continue to pursue creative litigation strategies based on the hope afforded by the Supreme Court.[254] After rehearing the *Spokeo* case, the Ninth Circuit provided plaintiff and defense counsel alike with little certainty in regard to when the violation of a federal statute gives rise to a concrete injury.[255] While a unanimous Ninth Circuit panel ruled that Robins had Article III standing because the statutory violation implicated his "concrete interests in truthful credit reporting," the court also recognized that "determining whether any given inaccuracy in a credit report would help or harm an individual (or perhaps both) is not always easily done."[256] Thus, courts still have significant discretion when analyzing whether a FCRA or other statutory violation gives rise to Article III standing, and plaintiffs will continue to have to test these limits.

C. *Privacy Torts*

Affected individuals may also turn to privacy torts to redress their injuries. There are four different traditional privacy torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) appropriation of name or likeness; and (4) publicity placing a person in false light.[257]

---

251. *Id.* at 1547–50.

252. *Id.* at 1550.

253. *Id.* at 1549.

254. *Compare* Galaria v. Nationwide Mut. Ins., Nos. 15-3386/3387, 2016 WL 4728027, at *3–6 (6th Cir. Sept. 12, 2016) (holding that the plaintiffs could continue their class action suits based on negligence, bailment, and FCRA violations without establishing that their customer data had been misused), *with* Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016) (holding that the plaintiff's Cable Communications Policy Act claim could not meet the *Spokeo* bar because the retention of consumer data did not cause the plaintiff any definite harm).

255. *See* Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

256. *Id.* at 1116–17.

257. JON L. MILLS, PRIVACY IN THE NEW MEDIA AGE 42–44 (2015).

Though the damages flowing from a data breach may concern all of these violations of privacy, the first two traditional torts are most applicable.

Intrusion upon seclusion protects an individual's "spatial" privacy, which can be violated without disclosure or publication of the individual's data because the commission of the tort is the intrusion itself.[258] The intrusion does not have to be physical[259] and may be a breach of a persons' "digital space."[260] In order to prevail under the intrusion upon seclusion tort, the data breach victim must satisfy the tort's three elements: (1) the intrusion was intentional; (2) the act intruded upon matters that the data breach victim reasonably expected would remain private; and (3) the intrusive act was highly offensive to the reasonable person.[261] Unlike a negligence cause of action, proof of damages is not an element of the intrusion upon seclusion tort. The economic loss rule also does not apply, so data breach victims may bring the action even when the damage is not purely economic. However, traditional justiciability requirements still apply to limit suits based on speculative injuries.

The third element of this privacy tort—whether the intrusive act was highly offensive to the reasonable person—is a shifting target and difficult to standardize. An intrusion that resulted in the dissemination of a person's health information protected by federal regulations such as HIPAA would likely offend a reasonable person. As would an intrusion that resulted in the dissemination of any sort of data protected by the patchwork of regulations previously discussed,[262] such as the unlawful disclosure of an individual's credit card information. However, dissemination of an aggregated set of individual data points that are readily available to the public—such as an address, telephone number, age, and name—may not be so objectively offensive in light of the fact that the information collected was public. The intentionality element of this privacy tort also presents a problem for the average data breach victim seeking to sue the data custodian rather than the hacker, simply because most data custodians never intend for a data breach to occur. Hackers would meet the intentionality standard, but are more difficult to sue because they are frequently anonymous and may not have any assets to collect with a judgment.[263]

---

258. *Id.* at 42.

259. *Id.*

260. *Id.* at 43.

261. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

262. *See supra* Part III.

263. Terry Bollea, who publicly is known by his wrestler-moniker Hulk Hogan, initiated a high-profile legal action—including invasion of privacy, publication of private facts, violation of the right of publicity, and intentional infliction of emotional distress—against Gawker after the

The tort of public disclosure of private facts requires the actual publication of facts that are so sensitive and personal that a reasonable person would object to their publication.[264] This action may only be brought by a natural person, not a corporation.[265] Unlike an intrusion upon seclusion claim, this tort does not require proof that the dissemination of the public facts was intentional.[266] Again, the data custodian who loses data due to a computer hacking did not actually "publish" the information. Usually if the information was published, the hacker or someone to whom the hacker disclosed the information published it.

For example, in *Randolph v. ING Life Insurance & Annuity Co.*,[267] the District of Columbia Court of Appeals determined that an insurance company did not "publish" personal information stolen from the company when a thief stole one of the insurance company's computers containing a trove of personal information.[268] Similarly, in *Galaria v. Nationwide Mutual Insurance Co.*,[269] a federal district court judge in Ohio held that the publicity requirement was not met when a data breach resulted in the theft of personal information by a hacker.[270] The class of plaintiffs in *Galaria* had given personally identifiable information to Nationwide Insurance in the course of purchasing insurance products and other services from Nationwide, but later found out that the information had been stolen when Nationwide's computer network was hacked.[271] Like most data breach scenarios, the hackers were never found, and the only plausible defendant for seeking a remedy for the invasion of privacy caused by the data breach was the data custodian, Nationwide Insurance, and it could not be held liable.

---

website posted excerpts of a sex tape featuring the former wrestler accompanied with a written report that detailed and commented on the sex tape. Bollea claimed he did not release the tape and Gawker maintained that they received the tape anonymously. Without the original leaker/intruder to go after, Bollea targeted, and eventually took down, the popular website. *Gawker Media, LLC v. Bollea*, 129 So. 3d 1196 (Fla. 2d Dist. Ct. App. 2014); *see also* Sydney Ember, *Gawker and Hulk Hogan Reach $31 Million Settlement*, N.Y. TIMES (Nov. 2, 2016), https://www.nytimes.com/2016/11/03/business/media/gawker-hulk-hogan-settlement.html.

264. MILLS, *supra* note 257, at 43.

265. *Id.* at 46.

266. *Id.* at 43.

267. 973 A.2d 702 (D.C. Cir. 2009).

268. *Id.* at 710.

269. 998 F. Supp. 2d 646 (S.D. Ohio 2014), *rev'd and remanded*, Nos. 15-3386/3387, 2016 WL 4728027, at *1 (6th Cir. Sept. 12, 2016).

270. *Id.* at 663.

271. *Id.* at 650.

D. *Unjust Enrichment*

Unjust enrichment is an equitable theory of law rooted in contract law principles.[272] The essential element of unjust enrichment is that the plaintiff actually conferred an unjust benefit on the defendant.[273] A data breach defendant that came into possession of the plaintiff's data without having received any remuneration from the plaintiff—in the form of the plaintiff purchasing something from the defendant, for example—will likely be immune from an unjust enrichment claim bought by the data breach victim. Data breach victims who have brought successful unjust enrichment causes of action against data custodians had each bought a product or service from the data custodian.[274] Thus, if the victim purchased a product, such as a video game or some clothes, liability may be possible.

Unjust enrichment may also be asserted by corporate employees against a corporate data custodian that opportunistically failed to protect employee data. In *Enslin v. Coca-Cola Co.*,[275] former employee Shane Enslin brought a class action against Coca-Cola following the theft of several company laptops that contained PII and the subsequent identity theft that Enslin endured.[276] The U.S. District Court for the Eastern District of Pennsylvania dismissed most of Enslin's claims, but allowed his unjust enrichment claim to move forward.[277] The court agreed that Enslin had fairly alleged the existence of an express or implied agreement that the company would protect the employee's PII as a result of the employee's acceptance of the employment contract.[278] Essentially, the company failed to implement adequate security measures to protect from the theft and benefited from employee labor while doing so.

E. *Violation of Trade Secrets*

During the recent rash of data breaches, an avalanche of commercial information were divulged, including private communications, strategies,

272. *See In re* Zappos.com, Inc., No. 3:12–cv–00325–RCJ–VPC, 2013 WL 4830497, at *4 (D. Nev. Sept. 9, 2013).

273. *Id.*

274. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) (accepting the plausibility of plaintiff's "would not have shopped" theory which alleged that Target should have not received plaintiffs' money when plaintiffs would not have spent money at Target if they had known about the breach); *see also* Meal & Cohen, *supra* note 236 (citing Bell v. Blizzard Entm't, Inc., No. 12-CV-09475 BRO (PJWx), slip op. at 7–8 (C.D. Cal. July 11, 2013) (where video game consumers alleged violations of the video game developer's privacy policy)).

275. 136 F. Supp. 3d 654 (E.D. Pa. 2015).

276. *Id*. at 658–60.

277. *Id.* at 669–80.

278. *Id.* at 674–75.

customer lists, movie scripts, marketing ideas, and other commercial secrets. Some of the disclosures were protectable intellectual property and others were just embarrassing private files. Determining whether the commercial information qualifies as protectable intellectual property turns on the distinct characteristics outlined by the Uniform Trade Secrets Act (UTSA). The criteria are: (1) the information is subject to reasonable measures to maintain its secrecy and (2) by remaining secret, the information confers a competitive advantage on its owner.[279] Examples of information protected under trade secret are the formula for Coca-Cola, proprietary customer lists, and copyrighted material such as an unreleased motion picture or script. While some items are clearly protectable intellectual property, the vulnerability for breach and the ability to share stolen information widely almost instantly creates a difficult setting to enforce trade secret laws.

In some instances, the existing law will protect against the redistribution of trade secrets. Under UTSA, anyone who steals valid trade secret property can be liable for the loss and resulting damages, and trade secret owners can seek injunctions to prevent disclosure.[280] In the right circumstances, even a republication of a trade secret exposed by a data breach may be a violation of UTSA. This protection from further republication would likely depend on the content of the trade secret and the extent of the republication.[281]

Despite the fact that the *Bartnicki* court specifically rejected a blanket First Amendment protection for the republication of trade secrets,[282] an innocent third party may be protected and allowed to publish a stolen trade secret if it deals with a matter of public concern. For example, in *CBS Inc. v. Davis*[283] the U.S. Supreme Court adopted the view that disclosure of a trade secret was protected speech if it was related to public health and safety.[284] The Court overturned a preliminary injunction that would have prevented CBS from broadcasting undercover footage of a meat packing facility, which included trade secrets, despite CBS's

279. UNIF. TRADE SECRETS ACT § 1(4)(i)–(ii) (UNIF. LAW COMM'N amended 1985).

280. *Id.* § 2(a).

281. In *Bartnicki*, the Court identified limits to First Amendment protection of republished material, particularly information of public importance. Bartnicki v. Vopper, 532 U.S. 514, 533 (2001). The Court suggested that republishing trade secrets may not qualify as protected speech, as they would fail the prong of *Bartnicki* requiring the information to be of public importance: "We need not decide whether that interest is strong enough to justify the application of § 2511(c) to disclosures of trade secrets or domestic gossip or other information of purely private concern." *Id.*

282. *Id.*

283. 510 U.S. 1315 (1994).

284. *Id.* at 1318.

"calculated misdeeds" in obtaining the footage.[285] This result should be no surprise. Under the *Bartnicki* balancing test,[286] even stolen information is provided with First Amendment republication protection if the information has significant public importance. It is unclear what the outcome would be if the stolen information was insignificant but just as intrusive. In that case, trade secret protection might apply.

When trade secrets are treated more as property than information, the plaintiff's chances to stop republication improve because the breach and publication are considered a theft or misappropriation of an identifiable asset rather than pure speech.[287] Simply put, property rights do not face the same test for publication as information under the First Amendment. The California Supreme Court tacitly accepted this argument in *DVD Copy Control Ass'n v. Bunner*[288] and ultimately held that an injunction prohibiting the online publication of a trade secret (a code for breaking DVD encryption technology) did *not* constitute an unlawful prior restraint.[289] However, as discussed, the argument to prohibit online publication is considerably weakened if the trade secret owner is seeking post-disclosure injunctive relief. Accordingly, although a trade secret posted on an obscure website may be protected from publication under UTSA, a loss of trade secret status will likely occur if it is widely distributed online. Likely due to these considerations, the California Court of Appeal for the Sixth District reversed the granting of the preliminary injunction in *Bunner* because the technology had since lost its trade secret status after continued online publication on several different popular websites.[290]

Policymakers should work to redefine misuse of trade secrets to include republication, and to reclassify stolen sensitive information as property or protectable information, unless there is a public interest for disclosure. Until policies change or court interpretations evolve, the epidemic of data breaches will continue to facilitate substantial harm to corporations as well as mass privacy intrusions on individuals.

---

285. *Id.* at 1315–18.

286. *See* discussion *supra* pp. 789–91.

287. *See* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 799–805 (2006).

288. 75 P.3d 1 (Cal. 2003).

289. *Id.* at 17–19. Once again demonstrating that matters of public concern will receive First Amendment publication protection, the court also distinguishes between the code at issue in the case and trade secrets involving matters of public concern. *Id.* at 15–16. The latter, a matter of public concern, implicates First Amendment protection and will prevent an injunction against an online post. *Id.*

290. DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 195–96 (Cal. Ct. App. 2004).

F. *Other Common Law Actions*

Replevin is an action at law designed to recover a specific piece of personal property.[291] A replevin action does not seek damages for the loss of the property, but rather the physical recovery of the property.[292] If this has applicability in a data breach scenario, a replevin action would seek the return of the data to the data breach victim. A replevin action may have some applicability to litigation seeking to stop dissemination of the stolen data by the media or others. However, due to the amorphous nature of "data," and the courts' reluctance to define data as any type of property, much less personal property,[293] replevin is generally not a useful action for the data breach victim, regardless of whether the victim is an individual or a corporation. Further, because stolen data is usually widely republished by third parties, replevin of the original data may provide little actual relief to the victim. A trespass to chattels remedy is similar to replevin, except damages are sought rather than the repossession of the stolen property.

Bailment is "the relationship that arises when personal property is delivered to another for some particular purpose with an express or implied contract to redeliver the property when the purpose has been fulfilled, or to otherwise deal with the property according to the bailor's instructions."[294] The classic example of a bailment claim is one made against a valet driver who refuses to deliver a patron's car.[295] Data breach plaintiffs have attempted to apply this old common law claim to modern, technologically complex data breach litigation scenarios.[296] Yet the transitory and quickly replicating nature of digital data may make it impossible to "return" it to the data breach plaintiff after a disclosure or further republication.[297] Further, as discussed, most courts have not recognized "data" as legal property.[298]

G. *Cyber Liability Insurance*

Due to the inadequate patchwork of legal remedies to fix the emerging web of problems surrounding data breach, some corporations use cyber liability insurance as an option to minimize seemingly inevitable

291. 66 AM. JUR. 2D *Replevin* § 1, Westlaw (database updated Nov. 2016).
292. *See id.*
293. Meal & Cohen, *supra* note 236, at 7.
294. *Id.* (citing Earhart v. Callan, 221 F.2d 160, 163 (9th Cir. 1955)).
295. *Id.*
296. *Id.*
297. *Id.*
298. *Id.*

damages.[299] Although such protections were traditionally used only in high-risk industries such as healthcare and finance, many companies in a wide range of industries are now purchasing cyber liability policies as part of their standard operating practices.[300] However, as with any insurance scheme, coverage can be denied, and data breach insurance is a complex area. Cyber liability insurance provides coverage for losses and crisis management support after a breach.[301] However, cyber liability insurance is not a standalone tactic for data security, but rather one tool in a company's cyber security toolbox.[302] Before attaining coverage, companies are often expected to have adequate risk management techniques already in place. If the company maintaining the data has been negligent, it is likely that insurance coverage will be denied after the breach, or be subject to higher premiums. However, if a company forgoes data breach insurance, it may not be able to simply rely on its preexisting commercial general liability policy.[303] This predicament results in increased costs and uncertain data security standards for the consumers.

Because the internet is global, the challenges for redressing data breaches are worldwide. A data breach on a company with a multinational reach will give rise to legal issues that cross borders.[304] The European Union and the United States are partners in many agreements and also are home to numerous corporations who do business in both jurisdictions. It is important to understand that these two jurisdictions, although they have much in common, have important differences in regulating privacy and data breaches.

299. In fact, there is a developing industry in cybersecurity insurance. *See* Mahendra Ramsinghani, *Can Startups Disrupt the $20 Billion Cyber Insurance Market?*, TECH CRUNCH (May 23, 2016), https://techcrunch.com/2016/05/23/can-startups-disrupt-the-20-billion-cyber-insurance-market/.

300. Steve Durbin, *Cybercrime: The Next Entrepreneurial Growth Business?*, WIRED, https://www.wired.com/insights/2014/10/cybercrime-growth-business/ (last visited Nov. 21, 2017).

301. JUDY SELBY & C. ZACHARY ROSENBERG, THOMSON REUTERS, CYBERINSURANCE: INSURING FOR DATA BREACH RISK 1 (2014), https://www.bakerlaw.com/files/uploads/News/Articles/LITIGATION/2014/Selby-Rosenberg-Dec-2014.pdf.

302. *See* Durbin, *supra* note 300.

303. *See* Zurich Am. Ins. v. Sony Corp., No. 651982/2011, 2014 WL 3253541, at *1 (N.Y. Sup. Ct. Feb. 24, 2014) (holding that Sony's insurance companies did not owe Sony coverage under their general liability policy after the 2014 PlayStation hacks); *see also* Young Ha, *N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation*, INS. J. (Mar. 17, 2014), http://www.insurancejournal.com/news/east/2014/03/17/323551.htm (noting that Sony's commercial general liability policy did not provide coverage for data breach incident).

304. *See* RONALD J. KROTOSZYNSKI, JR., PRIVACY REVISITED: A GLOBAL PERSPECTIVE ON THE RIGHT TO BE LEFT ALONE (2016).

V. COMPARING EUROPEAN UNION AND UNITED STATES POLICIES FOR DATA BREACHES AND PRIVACY

Because the transfer of digital information takes place on a global scale, it is important to consider distinctions in international and cross-border privacy law. As distinguished from the United States' treatment of privacy as a penumbral right, the European Union treats a person's right to privacy as fundamental. The right to privacy is explicitly enshrined in the European Union's premier human rights treaty, the European Convention on Human Rights (ECHR).[305] In the European Union, the right to privacy is afforded the same level of legal protection as the freedom of expression.[306] Accordingly, European courts must balance the right to privacy with the freedom of expression rather than substantially favoring the freedom of expression like courts in the United States.[307] The impact of this balance is noticeable in both European case law, which sets forth the "right to be forgotten," and legislative reform, including the incoming General Data Protection Regulation (GDPR) and EU-U.S. Privacy Shield.

A. *Privacy Law Within the European Union*

Arising from a more equal balancing between privacy and speech, Europeans treat the issue of prior restraint differently from the United States. Although European courts are hesitant to enjoin speech,[308] the line appears to be drawn with a less liberal interpretation than in the United States. In the case of *Mouvement Raëlien Suisse v. Switzerland*,[309] the Court upheld Swiss authorities' decision to ban a Raelian poster from display along public highways, weighing the harm of the controversial material over the speakers' religious freedom.[310] Previous cases in Europe have banned similar content, such as Nazi paraphernalia, under circumstances that would not justify banning the same content in the United States.[311]

---

305. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 1955 U.N.T.S. 222.

306. *Id.* art. 10.

307. *See* MILLS, *supra* note 257, at 66–68.

308. *See* Yildirim v. Turkey, 2012-VI Eur. Ct. H.R. 505, 542–43 (holding that the Turkish government could not block access to an academic website where plaintiff expressed controversial political views).

309. 2012-IV Eur. Ct. H.R. 373, 441–43, 447.

310. Since the Raelian movement stood in favor of principles like "human cloning, geniocracy, and sensual meditation" (often predicated on viewing the child as a privileged sexual object), the court held that there were sufficient public interest grounds to justify the government's refusal to allow the poster to be displayed along the highway. *Id.*

311. French web users were accessing online auction websites in the United States to purchase Nazi memorabilia. *See* Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme,

While the European Union may enforce some privacy components more strictly than the United States, the test to determine the legality of disclosure is strikingly similar to the test developed in *Bartnicki*. In *Axel Springer AG v. Germany*,[312] the European Court of Human Rights provided an analysis for determining whether a ban on the publication of an arrest and conviction of a well-known actor violated Article 10 of the ECHR. That Court evaluated (1) whether the event published was of general interest; (2) whether the person concerned was a public figure; and (3) how the information was obtained and whether it was reliable.[313] Similar to the *Bartnicki* holding, the Court found in favor of publication because the actor was well known and the information was only published after the prosecuting authorities' disclosure.[314] Again, freedom of expression triumphed over the right to privacy.

In a 2014 ruling, however, the Court of Justice of the European Union ruled that the fundamental right to personal privacy overrides, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in accessing information online.[315] Upholding the right to be forgotten, the Court ruled that Google must comply with EU data protection rules and remove a link for a digitized article that accurately detailed the foreclosure of the plaintiff's home.[316] Since 2014, Google has accepted more than 1 million URL removal requests (56.8% of all requests are approved).[317] The company reviews each request on a case by case basis following the Article 29 Working Party's guidelines[318] which require removal if the content is "inadequate, irrelevant or no longer relevant, or excessive . . . in the light of the time that has elapsed."[319] Google refused to apply a French order requesting

169 F. Supp. 2d 1181, 1192–93 (N.D. Cal. 2001), *rev'd*, 433 F.3d 1199 (9th Cir. 2006); *see also* MILLS, *supra* note 257, at 90–91 (analyzing the *Yahoo!, Inc.* decision during a conflict of laws discussion).

312. 2012 Eur. Ct. H.R. at 18, 27–30, http://hudoc.echr.coe.int/webservices/content/pdf/001-109034?TID=ihgdqbxnfi.

313. *Id.* at 27–30.

314. *Id.* at 30–33.

315. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014).

316. *Id.*

317. *Transparency Report: Search Removals Under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview (last visited Aug. 24, 2017).

318. ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON "GOOGLE SPAIN AND INC. V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12 (2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

319. *Google Spain SL*, 2014 EUR-Lex CELEX LEXIS.

worldwide removal of the contested data.[320] After years in the legal system, the European Court of Justice (ECJ) is set to hear the case, and the outcome will likely determine scope, potency, and longevity of the right to be forgotten—whether offending content must be taken down only in the requesting country, throughout the EU, or worldwide.[321] The evolution of European privacy law impacts not only member-nations within the EU, but also companies within the United States that engage in transatlantic business operations.

B. *Transatlantic Data Security Standards*

Major changes to European data regulatory structures were voted into place in 2016, and are set for implementation in May 2018. Data controllers and processors around the globe are currently reconsidering their data management practices and international data transfers to comply with the incoming GDPR[322] and EU-U.S. Privacy Shield.[323] Traditionally, the Data Protection Directive (the Directive) provided standards for all government and private entities that process EU employee or consumer data, as distinguished from the sector-specific approach in the United States.[324] The Directive also imposed strict requirements on non-EU countries that received personal data from EU citizens.[325] In the event of a data breach, the Directive imposed a duty on data processors[326] to notify the data controller,[327] and the controller to communicate the breach to the data subjects without delay.[328]

Until 2016, the European Commissions permitted U.S. companies to avoid some of these requirements as long as the companies abided by the Safe Harbor Principles.[329] After a push for stronger privacy protections

320. Julia Fioretti, *Google Refuses French Order to Apply 'Right to be Forgotten' Globally*, REUTERS (July 31, 2015, 5:01 AM), http://www.reuters.com/article/2015/07/31/us-google-france-idUSKCN0Q50VP20150731.

321. Alex Hern, *ECJ to Rule on Whether 'Right to Be Forgotten' Can Stretch Beyond EU*, GUARDIAN (July 20, 2017, 5:19 EDT), https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed.

322. *See* Commission Regulation 16/679, arts. 94, 99, 2016 O.J. (L 119) 1, 86, 87 (EU).

323. *See* U.S. DEP'T OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 6 (2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

324. *See* Council Directive 95/46, art. 2(d), 1995 O.J. (L 281) 31, 38 (EC).

325. *See id.* art. 25.

326. '"[P]rocessor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller . . . ." *Id.* art. 2(e).

327. The "data controller" is the party primarily responsible for compliance. *Id.* art. 2(d).

328. *Id.* arts. 12, 17.

329. The seven Safe Harbor privacy principles are notice, choice, transfer to third parties, access, security, data integrity, and enforcement. *See Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMMISSION (Dec. 2012),

by EU citizens and the courts,[330] the Directive was replaced by the GDPR and the EU-U.S. Privacy Shield replaced Safe Harbor. However, unlike the Directive, which allowed each member country to decide how to apply standards, the GDPR is law that applies uniformly to all EU countries and reaches foreign companies dealing in EU data.[331]

The GDPR will apply to any company worldwide that processes or controls personal data[332] of an EU resident in connection to (1) offering goods or services, or (2) monitoring behavior.[333] Before the GDPR comes into effect on May 25, 2018, companies will need to assess what kinds of structural changes will be necessary to ensure compliance, chiefly providing notice and consent to EU data subjects.[334] Most companies will need to appoint a Data Protection Officer (DPO), and many companies will also need to appoint a local representative to be located in the European Union.[335] If a data breach occurs, DPOs will be required to notify a data protection authority within seventy-two hours of the breach, ideally within twenty-four hours.[336] While there will be many issues related to jurisdiction, the GDPR permits EU residents to pursue legal action against any data processor or controller, including those located in

---

https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

330. *See* European Union Press Release No. 117/15, The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid ¶¶ 4, 11–12 (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (finding that American companies' mere compliance with the United States's Safe Harbor provisions is not, by itself, adequate protection in Europe and may still leave these companies exposed to liability).

331. The CJEU deemed Safe Harbor framework inadequate in the case because the cross-border transfer of personal data by Facebook did not provide a level of data protection essentially equivalent to that of the European Union. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 650; *see also* John Naughton, *Data-Hucksters Beware – Online Privacy Is Making a Comeback*, GUARDIAN (Aug. 20, 2017, 1:59 EDT), https://www.theguardian.com/commentisfree/2017/aug/20/data-hucksters-beware-online-privacy-eu-general-data-protection-regulation.

332. "Personal Data" is defined as any information relating to the subject. Commission Regulation 16/679, art. 4(1) 2016 O.J. (L 119) 1, 33 (EU).

333. *Id.* art. 3(2).

334. *Id.*

335. *Id.* arts. 27, 37.

336. *Id.* art. 33. In addition to data breach requirements under the GDPR, in 2016, the European Parliament passed the Network and Information Security (NIS) Directive, which imposes additional reporting requirements on companies following a breach. The NIS Directive targets entities that provide essential services, such as the energy, health, finance, and transportation sectors, and digital service providers. Council Directive 16/1148, arts. 4(4), 5(2), 2016 O.J. (L 194) 1, 13, 14 (EU). Similar to the GDPR, the NIS Directive applies to companies outside of the European Union *if* the company offers services within the European Union. *Id.* art. 18. If a company falls within one of the regulated sectors and is breached, the company is then required to notify the relevant authorities regardless of whether the breach exposed personal data. *Id.* arts. 14, 16.

the United States, alleged to be in violation of the GDPR.[337] Administrative fines for violations of the GDPR will operate in a two-tiered system, with the most egregious data breaches incurring fines of up to 4% of global annual turnover—up to €20 million.[338] Factors for determining the fine include, but are not limited to, the nature of infringement, intentionality or negligence, mitigating factors taken by the data controller, and nature of the personal data.[339]

The EU-U.S. Privacy Shield will protect personal data in transfers between EU residents and U.S. companies, while encouraging the flow of data between U.S. companies and the European Union.[340] The FTC will monitor U.S. companies subject to the Privacy Shield stateside.[341] The Privacy Shield protects personal data by imposing requirements on organizations for their data collection, management, and consumer transparency practices.[342] U.S. companies must provide notice to EU data subjects on data use and recourse available, provide choice of opt-out of data collection or opt-in for sharing sensitive data,[343] and must take reasonable and appropriate security measures to protect personal data from "loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data."[344] Consistent with principles of data minimization, companies must limit collection of personal data to what is relevant to the purpose.[345] Companies must also allow data subjects access to their own data and the ability to correct or amend it where reasonable, and must make available independent recourse mechanisms in the event of breach.[346] Additionally, companies must limit data use and transfers to third parties consistent with purpose provided in notice, and are accountable for third-party organizations receiving data transfers,

337. Commission Regulation 16/679, art. 79, at 80.

338. Kuan Hon, *GDPR: Potential Fines for Data Security Breaches More Severe for Data Controllers Than Processors*, REGISTER (May 12, 2016, 8:33 AM), http://www.theregister.co.uk/2016/05/12/gdpr_potential_fines_for_data_security_breaches_more_severe_for_data_controllers_than_processors_says_expert/.

339. Commission Regulation 16/679, art. 83, at 82.

340. *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 1, 10 (2016).

341. European Commission Press Release MEMO/16/434, EU-U.S. Privacy Shield: Frequently Asked Questions (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

342. *See id.*

343. Sensitive data is not specifically defined but generally includes personal data about medical history, health, race or ethnic origin, political, religious or philosophical beliefs, trade union membership, or sex life. Voss, *supra* note 340, at 9.

344. *See* U.S. DEP'T OF COMMERCE, *supra* note 323, at 6.

345. *See* Voss, *supra* note 340, at 13.

346. *See id.*

ensuring the third party takes steps to comply with the Privacy Shield.[347] U.S. companies can self-certify that they abide by EU data privacy standards, which track the seven principles established in the Directive.[348]

VI. RESPONSES TO DATA BREACHES AND THE FUTURE OF DATA BREACH LAW AND POLICY

The specific responses to a data breach must be rapid and organized. Of the two classes of victims affected—individuals and the corporate entities that hold these individuals' private information—the corporations have the principal duty to maintain security of individuals' information.

A. *The Corporation*

Corporations have the duty and the opportunity to reduce their exposure to harmful breaches and reduce the damage to the individuals whose information they hold. Any entity that possesses information—whether it be sensitive corporate information or the personal information of customers and/or employees—should, at a minimum, implement the following practices:

1. monitor the guidance and rules provided by the federal and state agencies regulating their industry, including the guidance promulgated within enforcement actions, presentations, and agency editorials or blog posts;
2. apply up-to-date technical standards, such as the NIST industry standards;
3. develop and adopt adequate data collection and security plans that are constantly reviewed against regulatory requirements and actions at both the state and federal level; and
4. repeatedly test all data collection and security plans.

Essentially, corporations must heed the FTC's advice by starting *and* sticking with security.[349] To build an even stronger program, corporations should conduct internal investigations that test their own policies. Supervisors can test their employees with benign spear phishing exercises in order to ensure that every employee is equipped to handle malicious attacks. Corporate counsel can draft monthly data security reminders and run tabletop exercises that simulate a breach experience. These

347. *See id.* at 15.

348. The Framework's seven privacy principles are notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse. *See* U.S. DEP'T OF COMMERCE, *supra* note 323, at 4–6.

349. *See supra* notes 128, 130 and accompanying text.

evaluations should occur as frequently as possible with a goal of constant improvement.

Once a breach occurs, the breached entity is in crisis mode but should have a plan to follow and follow quickly. The corporation or breached entity must assess the problem, issue internal notifications, freeze all evidence surrounding the breach, perform its legal obligations to affected individuals based on applicable law, and then pursue its legal remedies, some of which might require mounting defenses against the individuals its policies were designed to protect. Some of these responses may include offensive legal actions against negligent providers or others who caused the breach. As demonstrated by the graphic below, the legal landscape is treacherous.[350]

The landscape can become even more treacherous if the breach reaches valuable commercial information. The corporate entity must be ready to enjoin or, at the least, reduce publication in the media and online. The loss of trade secret status because of predictable republication in the current digital age seems to be a seriously harsh penalty if the corporation made all efforts to sustain confidentiality of the information. The legal and practical problem is that the republishers may be clueless and blameless, only repeating what they see posted online. However, the harm to the corporation is the same as if the data were stolen and distributed by corporate espionage.

But the corporation must make an effort to defend valuable trade secrets. If a trade secret has been widely republished at no fault of the

350. Pedro Allende, Data Security Law: Foundations, Workshop Presentation at the Privacy + Security Forum (Oct. 24, 2016) (on file with authors).

trade secret holder and has subsequently lost trade secret status under UTSA, in lieu of an injunction prohibiting all publication by any publisher, courts could instead order a targeted delisting of the trade secret from search engines. This type of search engine takedown is the method utilized by the European Union's right to be forgotten policy.[351] This policy reflects the logic used in "search engine optimization," which focuses on the primary sources used to research information or individuals—i.e., the principal search engines such as Google, Yahoo, or Bing.[352] While this proposal has less First Amendment concerns than an all-encompassing injunction on the publication of information, it still may not provide the relief that many trade secret holders seek.

Another proposed remedy to this situation is a takedown system akin to that of intellectual property takedowns under the Digital Millennium Copyright Act (DMCA). The DMCA[353] has worked to enable the removal of information located on ISPs through specific notice. The same type of process could work for trade secrets, and trade secret scholars have long advocated for an improved trade secret takedown process modeled after the DMCA.[354] One such suggestion would require ISPs to remove the publication of alleged misappropriated trade secrets from their site within a few hours after being notified of the infringing material.[355] Then, the original complainant would have a week to a file an official complaint with the court.[356] The takedown notice would be accompanied by a bond or fee to minimize potential frivolous complaints.[357] Some First Amendment concerns would be alleviated by an exception for established news organizations, which would exempt such sites from the accelerated takedown process altogether.[358] While such a process may limit the digital republication of valuable information, it does not necessarily escape the continuing criticisms lodged against the DMCA. Just as the DMCA suffers from the lack of a take-down-and-

351. *See supra* text accompanying notes 315–17.

352. *See What Is SEO / Search Engine Optimization?*, SEARCH ENGINE LAND, http://searchengineland.com/guide/what-is-seo (last visited Jan. 17, 2017).

353. 17 U.S.C. § 512(c)(3) (2012). Section 512 of the DMCA requires that the takedown request be in writing, be signed by the copyright owner or agent, identify the infringed work, identify the material that is infringing the work, include contact information for the copyright owner, have a statement of good faith and accuracy, and have a statement that the complaining party is authorized to proceed in the takedown request. *See id.*

354. *See* Elizabeth Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041, 1043 (2007).

355. *Id.* at 1061–62.

356. *See id.* at 1062.

357. *Id.* at 1063.

358. *Id.* at 1065–66, 1071–84.

stay-down approach,[359] a trade secret takedown process could become unmanageable if the online posting frenzy has already started. Further, the First Amendment concerns are not completely solved by the established media exception, especially considering that what constitutes media and public interest changes and expands every day.

Regardless, creating an effective trade secret takedown process is important because it directly relates to the impact of removing information from the internet—a critical problem that has yet to be overcome in current data breaches. Pragmatically, data breaches are going to deal with information that is somehow made available to unauthorized sources. It may be on the dark web, as in the Ashley Madison breach;[360] it may be in the hands of journalists, as in the HSBC breach;[361] or it may be published on a website, as in the Sony breach.[362] In all of these cases, a major issue facing companies is preventing further republication after an initial criminal breach, which commonly discloses important trade secrets as well as intrusive personal disclosures that affect individuals.

B. *The Individual*

Individuals, like corporations, face numerous hurdles when preparing for and responding to a data breach. Both also face massive consequences if a breach occurs, but the landscape for individuals is significantly less defined. The central difficulties that individuals must learn to navigate fall primarily into two categories:

1. Understanding and implementing the necessary steps to protect against harm caused by data breaches; and
2. Determining whether to pursue legal action.

For many practitioners, the most pressing issues for affected individuals revolve around the efficacy of legal action. However, realistically, most individuals are rightfully consumed with the task of protecting themselves before and immediately in the aftermath of the breach. Simply put, they cannot wait for the legal system to provide them

359. Copyright holders are limited in only targeting the takedown of infringing material posted by a particular user on a specific website. There is no blanket takedown process for copyrighted material posted by multiple users on multiple websites, thus creating an excruciating process comparable to the children's game Whack-A-Mole. *See* Stephen Carlisle, *DMCA "Takedown" Notices: Why "Takedown" Should Become "Take Down and Stay Down" and Why It's Good for Everyone*, NOVA SE. U. (July 23, 2014), http://copyright.nova.edu/dmca-takedown-notices/.

360. *See supra* Subsection I.B.6.

361. *See supra* Subsection I.B.5.

362. *See supra* Subsection I.B.3.

with adequate relief. Instead, individuals must adopt their own security measures to better protect themselves against identity theft and other post-breach consequences. While corporations and courts drag their feet, individuals can implement simple techniques, such as the use of complex and unique passwords, to better secure their digital activities. Shifting these responsibilities to the individual should not be the ultimate solution, but adopting stronger personal security measure is a practice, and it could mean the difference between a breach ruining a life or being a minor inconvenience.

Of course, individuals should also have the opportunity to pursue legal remedies by seeking relief in tort, breach of contract, or through statutory damages. Whether through statutory claims such as the FCRA claim in *Spokeo*[363] or a negligence complaint, it is critical that plaintiffs employ creative legal strategies in order to overcome the barriers to relief from the effects of data breaches. Although there have been notable successes for individuals in class action litigation like the *Target* action,[364] and in cases where negligence of the breached entity is clear, barriers such as standing and First Amendment protections for republication create major hurdles to an individual's relief.

In the long term, cutting-edge litigation and serious policy reform can provide more options for innocent victims of the mass privacy intrusions known as data breaches. Courts must begin to better value the potentially intrusive nature of personal data disclosures and more willing to view a wider range of remedies.

C. *The Future*

The current society collects and exposes massive amounts of data continually. These collections contain sensitive and personal information. Reflecting this trend, the Supreme Court recognized the intrusiveness of observing personal cell phone data in the Fourth Amendment context. The Court stated that the warrantless search of the data contained on a cell phone may be even more intrusive than the search of a home.[365] In his reasoning, Chief Justice John Roberts acknowledged the high value of protecting private digital information in the search and seizure and public safety realm.[366] Just as public safety concerns compete with privacy rights, the right to privacy competes with the First Amendment right to publish information. The modern data breach is facilitating a mass intrusion on corporate confidentiality and individual privacy.

363. *See supra* notes 264–71 and accompanying text.

364. *See* Stempel & Bose, *supra* note 37.

365. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014).

366. *See id.* at 2494–95.

Accordingly, the right of corporate trade secrets and individual's confidentiality must be protected in a reliable way. Further, individual dignity and privacy must prevail. The EU approach to balancing the harm to individual dignity against the value of public disclosure is workable and can be supported by the logic of *Bartnicki*.[367]

Just as the republication of commercially valuable data should not be automatically protected speech, neither should the breaches of individual privacy by third parties or republishers of breached information. Simply because an individual has revealed sensitive information to another does not mean the person abandoned all privacy interests.

In the Fourth Amendment context, Justice Sonia Sotomayor eloquently expressed the need for privacy rights when information has been disclosed to third parties. In a data breach context, the data given to a website, retailer, medical provider, or financial institution should not be freely distributed by third parties after a breach makes that information available. As Justice Sotomayor said, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[368]

Certainly, the mere disclosure to a third party for routine life tasks cannot be viewed as consent for the republication of information wrongfully obtained from a data breach from that third party. That is exactly the circumstance when a blogger or media outlet republishes private information posted on the web by a hacker.

Victims, whether corporate or individual, must also contend with the plaintiff's paradox or what others have termed the "Streisand Effect"[369]: litigation to vindicate privacy rights risks exposure to greater attention to the embarrassing slanderous, intimate, commercially sensitive, or invasive information.[370] Sometimes the costs of republicizing the events of the breach are worse than simply allowing it to disappear into the

367. *See supra* notes 101–03 and accompanying text.

368. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

369. *See* T.C., *What Is the Streisand Effect?*, ECONOMIST (Apr. 15, 2013, 11:50 PM), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect.

370. For example, see CTB v. News Grp. Newspapers Ltd. [2011] EWHC (QB) 1232 [2] (Eng.), regarding the "super injunction" sought by famous soccer player Ryan Giggs to prohibit the media from releasing not only information about his extramarital affair, but also his identity in seeking the injunction. Ultimately the injunction became useless because social media worldwide disclosed Giggs's identity.

perpetual clamor of the modern media.[371] So far, corporate suits to vindicate privacy in the form of property rights such as trade secrets have been successful.[372] Individuals who brought lawsuits to vindicate personal privacy have seen less success, but this precedent need not dictate the future; creative use of the privacy torts may be the most workable vehicle moving forward. Responding to and preventing damages from data breaches will require changes in policy and creative litigation strategies.

Policy advancements, particularly by the FTC, have made great leaps in protecting individual privacy and raising the standards for sensitive data protection. However, a significant hurdle left to clear is avoiding or mitigating harmful republication. The European Union has provided a useful model for reform in this arena by recognizing the importance of privacy as personal dignity. A logical extension of the *Bartnicki* framework in the United States leads to the inexorable conclusion that the republication of private facts cannot automatically be immune from liability. New legislation seeking to limit the republication of both valuable commercial information and individuals' private information could codify this *Bartnicki* extension and recognize the growing value of modern privacy. Either legislation or litigation must be able to thread the First Amendment needle to provide protection to corporations and individuals. Until law and policy changes, the epidemic of data breaches will continue to cause substantial harm to breached corporations and to create mass privacy intrusions on innocent individuals.

371. Individual victims seeking anonymity while pursuing post-breach remedies may be denied such privacy. *See* Emily Fiend, *Ashley Madison User Must Reveal Real Name in Breach Suit*, LAW360 (Dec. 14, 2015, 8:08 PM), http://www.law360.com/articles/737739/ashley-madison-user-must-reveal-real-name-in-breach-suit (describing how U.S. District Court Judge James M. Moody, Jr. required the anonymous Ashley Madison user leading the class action to reveal his name instead of filing under an alias).

372. *E.g.*, DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 13–19 (Cal. 2003).