Vanderbilt Journal of Entertainment & Technology Law

Volume 23 | Issue 3 Article 5

2021

Regulating Data Breaches: A Data Superfund Statute

Kyle McKibbin

Regulating Data Breaches: A Data Superfund Statute

ABSTRACT

Collecting and processing large amounts of personal data has become a fundamental feature of the modern economy. Personal data, combined with good data analytics, are valuable to businesses as they can provide highly detailed information about individual preferences and behaviors. This data collection can also be valuable to the consumer as it generates innovative products and digital platforms. The era of big data promises great rewards, but it is not without its costs. Data breaches, or the release of personal data into unwanted hands, are pervasive and increasingly massive in scale. Despite the personal privacy harm caused by data breaches, businesses can largely externalize the costs of these breaches to the public. While privacy harm is undoubtedly an important issue, the release of data generates arguably more significant social costs. This Note argues that policy makers should view the unwanted release of data as a form of pollution that dilutes critical public goods. As such, an effective regulatory solution to data breaches should mirror the current regulatory approaches to environmental pollution. Like the physical environment, the data environment is a complex and highly interconnected system; accordingly, there is unlikely to be a single best way to regulate it. Thus far, the United States has approached data regulation in a stepwise and targeted fashion, much like environmental regulation. This approach has some advantages, but there is a pressing need for more comprehensive regulation. Current proposals point to omnibus privacy laws like the European Union's General Data Protection Regulation and the California Consumer Privacy Act as a solution. However, these regulations are ultimately privacy focused and impose high costs on the data economy. To balance these concerns, this Note proposes that Congress enact federal legislation implementing a data protection statute modeled after the Comprehensive Environmental Response, Compensation, and Liability Act.

TABLE OF CONTENTS

In 2019, approximately 540 million Facebook user records were released to the public on Amazon's cloud computing service by two third-party Facebook app developers.[1] This included a wealth of personal data, such as account names, IDs, location check-ins, unprotected passwords, and general user activity.[2] This data breach[3] is

1. Jason Silverstein, *Hundreds of Millions of Facebook User Records Were Exposed on Amazon Cloud Server*, CBS NEWS (Apr. 4, 2019, 11:35 AM), https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/ [https://perma.cc/B5D7-Y4KE].

2. *See id.*

3. *See* Kevin Ferguson, *Data Breach*, SEARCHSECURITY: TECHTARGET, http://searchsecurity.techtarget.com/definition/data-breach [https://perma.cc/M3YC-BJXU] (last updated May

one of the largest of all time.[4] However, this was not the first time in recent years that Facebook—a company with personal data pertaining to over 2.3 billion active monthly users worldwide—had suffered a major data breach.[5] Even more concerning, Facebook is not alone. In 2019, major breaches also affected well-known entities such as Microsoft, Instagram, Adobe, DoorDash, and Fortnite.[6]

In an information-age economy increasingly driven by the collection of data,[7] these data breaches are not going away. Americans transmit their data through personal computers, mobile phones, and internet devices to private companies at an exponential rate.[8] By 2025, the proliferation of these devices means that each person with an internet-connected device will have at least one data interaction every eighteen seconds, or almost five thousand per day.[9] As institutions collect this increasingly large pool of consumer data, the risk of exposure will continue to grow.[10]

In light of these trends, this Note argues that current government intervention is insufficient to protect the public from data breaches affecting private firms. Part I begins with a discussion of current data collection practices and explains why personal and economic incentives fail to effectively police firm behavior. It further provides an overview of relevant privacy laws and the various regulatory regimes that serve to protect consumer data in the United States. Part II addresses the limitations and shortcomings of that regulatory regime, particularly with regard to newer legislation such as the California Consumer Privacy Act (CCPA) and the European Union's

---

2019) (defining data breach). When "sensitive, confidential or otherwise protected data" such as this are either accessed or disclosed by an unauthorized party, it is referred to as a data breach. *Id.*

4. Kenneth Kiesnoski, *5 of the Biggest Data Breaches Ever*, CNBC (July 30, 2019, 10:22 AM), https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html [https://perma.cc/CV4Y-ACSW].

5. Silverstein, *supra* note 1. In 2018, the information of 50 million users was exposed in an attack on Facebook's networks, and in 2016 it was revealed that Cambridge Analytica, a company working on the Trump campaign, gained access to information from more than 87 million users. *Id.*

6. Rob Sobers, *107 Must-Know Data Breach Statistics for 2020*, VARONIS, https://www.varonis.com/blog/data-breach-statistics/ [https://perma.cc/2QJZ-Z38Y] (last updated Sept. 24, 2020).

7. *See Data Is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [https://perma.cc/WLX7-XKZ2].

8. *See* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 1 (2019).

9. Joseph V. DeMarco & Brian A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J.F. 1016, 1020 (2019).

10. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 1–2.

General Data Protection Regulation (GDPR). Part III explores the similarity between data breaches and environmental pollution. It argues that the environmental laws that regulate the release of hazardous substances can serve as an effective model for regulating data pollution. Specifically, this Note recommends that Congress implement a federal statute modeled after the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), also known as the Superfund Statute. Such a liability-focused regime, along with certain prescriptive requirements, would incentivize better data protection at a minimal cost.

I. BACKGROUND

A. Current Data Practices

1. Data Collection

Companies derive significant economic benefits from aggregating personal data and selling it to third parties.[11] Data brokers, an important subsection of firms that collect and sell data, demonstrate how profitable this practice can be. These firms collect a wide range of data, such as "bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions."[12] Once collected and aggregated, brokers sell this data to businesses for a variety of purposes, such as sending targeted advertisements or verifying identities to mitigate risk.[13] The nine firms mentioned in the report alone collect data on billions of individuals, including one firm that had over three thousand data segments for nearly every US consumer.[14] Indeed, in an industry that includes between 2,500 and 4,000 data brokers, these nine brokers generated $426 million in annual revenue.[15]

A data broker's objective in gathering all of this data is to create an easily accessible compendium of consumer information that provides

---

11. *See* Patrick Myers, *Protecting Personal Information: Achieving a Balance Between User Privacy and Behavioral Targeting*, 49 U. MICH. J.L. REFORM 717, 723 (2016).

12. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/5W56-YA5N].

13. *Id.* at ii–iii.

14. *Id.* at 8–9.

15. *Id.* at 23; Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016, 2:30 PM), http://www.newsweek.com/secretive-world-selling-data-about-you-464789 [https://perma.cc/H9K3-YRUW].

powerful insight into consumer preferences.[16] Data are collected from a variety of sources including government databases, social media, and commercial sources.[17] Each source may provide only a few data elements about a consumer, but, once combined, even information that is seemingly anonymous can be used to create a shockingly comprehensive profile of an individual.[18] With this information, a firm could match an individual's browser history with her profile to "identify" the consumer and target her with advertisements for products that she might be more likely to purchase.[19] Taken a step further, these individual behaviors can then be grouped together and used to identify generalizable patterns of behavior.[20] The result is a powerful tool with vast potential in the commercial realm[21] and beyond.[22]

2. The Consumer Privacy Paradox

Although society stands to benefit from data collection, consumers do not know the scope or quantity of personal data that firms collect[23] and are concerned about how firms use their data.[24] For instance, data collection practices in the data broker industry make it nearly impossible for consumers to control the spread of personal data.[25] Unlike large, identifiable companies like Facebook, these brokers are shrouded in obscurity and avoid name recognition.[26] Data are often not collected directly from consumers and can be resold freely among

16. *See* FED. TRADE COMM'N, *supra* note 12, at 31.

17. *Id.* at 11, 13.

18. *Id.* at 46.

19. Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 445–47 (2011).

20. *See* Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 112, 114 (2019).

21. *See generally* FORBES INSIGHTS, THE BIG POTENTIAL OF BIG DATA: A FIELD GUIDE FOR CMOS (2013), https://images.forbes.com/forbesinsights/StudyPDFs/RocketFuel_Big-Data_REPORT.pdf [https://perma.cc/WKE6-UVU8].

22. *See, e.g.*, Sabyasachi Dash, Sushil Kumar Shakyawar, Mohit Sharma & Sandeep Kaushik, *Big Data in Healthcare: Management, Analysis and Future Prospects*, 6 J. BIG DATA, no. 1, 2019, at 1; Nir Kshetri, *The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns*, BIG DATA & SOCIETY, July–Dec. 2014, at 1 (2014).

23. *See* FED TRADE COMM'N, *supra* note 12, at 46.

24. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/2NLD-LH2E].

25. *See* FED TRADE COMM'N, *supra* note 12.

26. *See* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REGUL. 667, 674 (2017).

brokers.[27] Moreover, even if a consumer shared limited personal information with an identifiable and trusted firm, she may have unknowingly granted its unrestricted use by any data broker willing to pay the price.[28]

Of course, most firms ask consumers to consent to a privacy agreement; thus, consumers arguably should know their data can be sold to third parties.[29] The voluntary transfer of data in exchange for a specific web or app product could be seen as a legitimate transaction between the user and the firm. For example, courts regularly uphold the validity of "click-wrap agreements," where users agree to the terms of complex privacy agreements with the simple click of a button.[30] However, studies indicate that users typically do not read these policies, and, even if they do, many agreements do not make it clear that user data can be sold to third parties.[31]

Overall, consumers seem to express a preference for privacy while continuing to blindly agree to policies and share personal data.[32] This phenomenon is sometimes labeled as the privacy paradox.[33] Consumers engage in a form of hyperbolic discounting, where they give up potentially valuable data in exchange for short-term and somewhat meager rewards.[34] Consumers also seem to continue to provide data to companies even after major breaches.[35] Indeed, even though consumers are concerned about their personal data generally, they have mixed attitudes concerning specific uses.[36]

---

27. *See* FED TRADE COMM'N, *supra* note 12.

28. *See* Myers, *supra* note 11, at 724.

29. *See id.*

30. *Id.* at 732–33.

31. *See id.* at 724; Auxier et al., *supra* note 24 (finding that only 22 percent of adults claim to always or sometimes read privacy polices). One study showed that 74 percent of participants consented to a fake social media website's privacy policy without even reading the terms. Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMMC'N & SOC'Y 128 (2020).

32. *See* Christine S. Wilson, Commissioner, Fed. Trade Comm'n, Remarks at the Future of Privacy Forum: A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf [https://perma.cc/YB2Y-FFYE].

33. *See, e.g., id.*

34. *See id.*

35. *See* John Naughton, *The Privacy Paradox: Why Do People Keep Using Tech Firms That Abuse Their Data?*, GUARDIAN (May 5, 2019, 2:00 AM), https://www.theguardian.com/commentisfree/2019/may/05/privacy-paradox-why-do-people-keep-using-tech-firms-data-facebook-scandal [https://perma.cc/87GQ-3PEL].

36. *See* Auxier et al., *supra* note 24. In a Pew Research survey, 48 percent of respondents believed it was acceptable for DNA testing companies to share customer genetic data to help solve

3. Externalizing Costs

There are many reasons why data breaches occur. Although sometimes the source is an outside attacker, many data breaches occur because of inadvertent disclosures by company insiders.[37] Regardless of the source, individuals tend to hold the business itself accountable.[38] Indeed, some notable data breaches have resulted in a stream of negative publicity and public outcry,[39] and firms can face tort liability, often in the form of class action lawsuits.[40] While this certainly imposes some costs on firms, they can frequently escape significant consequences.[41] For example, a data breach can lead to a decrease in stock price or negative public perception, but these negative effects are generally short-lived.[42] In addition, tort law remedies are notoriously difficult to obtain and have failed to keep pace with changing data practices.[43] Even when obtained, damages are often minimal compared to the revenue of companies dealing in data.[44] Moreover, the harm of a breach is not something that can really be undone.[45] Once released, data can be copied and shared quickly with little cost. Damages may pay for identity theft monitoring, but ultimately the disclosure costs will continue to be carried by consumers. The result is a market failure

---

crimes, while only 25 percent believed it was acceptable for makers of smart speakers to share personal audio data for the same purposes. *Id.*

37. *See* Long Cheng, Fang Liu & Danfeng Yao, *Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions*, WIRES DATA MINING & KNOWLEDGE DISCOVERY, Sept.–Oct. 2017, at 1, 3–5.

38. Tara Seals, *Consumers Overwhelmingly Blame Businesses for Breaches*, INFOSECURITY MAG. (Nov. 30, 2017), https://www.infosecurity-magazine.com/news/consumers-overwhelmingly-blame/ [https://perma.cc/LAJ5-YB25].

39. *See, e.g.*, Tony Romm, *Senators Slam Equifax, Marriott Executives for Massive Data Breaches*, WASH. POST (Mar. 7, 2019, 12:51 PM), https://www.washingtonpost.com/technology/2019/03/07/senators-slam-equifax-marriott-executives-massive-data-breaches/ [https://perma.cc/3UV7-L79V].

40. *See generally* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 634 (2018).

41. *See, e.g.*, Josephine Wolff, Opinion, *Why It's So Hard to Punish Companies for Data Breaches*, N.Y. TIMES (Oct. 16, 2018), https://www.nytimes.com/2018/10/16/opinion/facebook-data-breach-regulation.html [https://perma.cc/C84L-VC9S]; Naughton, *supra* note 35.

42. *See* Wolff, *supra* note 41. In fact, firms may not know how to utilize or value consumer data. *See* Jeanne W. Ross, Cynthia M. Beath & Anne Quaadgras, *You May Not Need Big Data After All*, HARV. BUS. REV., Dec. 2013, https://hbr.org/2013/12/you-may-not-need-big-data-after-all [https://perma.cc/XLG5-Y68G].

43. *See* Daniel J. Solove & Neil M. Richards, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1918 (2010).

44. *See* Wolff, *supra* note 41.

45. *See* Solow-Niederman, *supra* note 40, at 624.

where firms externalize a significant portion of the cost of data collection onto consumers.[46]

B. Current Privacy Regulation

The United States regulates commercial data protection through a combination of federal statutes, state statutes, tort actions, and private contracts.[47] These regulations generally fall under the umbrella of privacy law.[48] Additionally, the Supreme Court has recognized that the Constitution provides certain protections regarding individual privacy.[49] However, the type of privacy contemplated by these constitutional protections is conceptually distinct from the protection of personal data at issue here.[50]

1. Comparing Federal Statutes

Unlike other jurisdictions, such as the European Union, there is no omnibus federal privacy legislation that governs commercial data practices in the United States.[51] Instead, there is a patchwork of targeted data protection statutes at the federal level, with the Federal Trade Commission (FTC) left to fill in the gaps.[52] Federal statutes either regulate specific industry participants, such as financial institutions, health care entities, and communications common carriers, or specific categories of data, like data pertaining to minors.[53]

The scope and protections of these statutes are by no means uniform.[54] Some succeed in preventing certain abuses while failing to protect against others. For example, the Fair Credit Reporting Act (FCRA) applies to a variety of entities that handle data relating to consumer creditworthiness.[55] Regulations require that collected data are accurate and only used for limited purposes.[56] The FTC and

---

46. *See* Ben-Shahar, *supra* note 20, at 107.

47. *See* L. BUS. RSCH., THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 271–72 (Alan Charles Raul ed., 2014).

48. *See id.* at 272.

49. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 5.

50. *See id.* at 5–7.

51. *See id.* at 7–8.

52. *See id.*

53. *See id.*

54. *Id.* at 2.

55. *Id.* at 12 (including "(1) credit reporting agencies (CRAs), (2) entities furnishing information to CRAs (furnishers), and (3) individuals who use credit reports issued by CRAs (users)").

56. *Id.*

Consumer Financial Protection Bureau (CFPB) jointly enforce the provisions of the FCRA.[57] There is also a private cause of action for consumers that are injured by willful or negligent violations of the Act.[58] On the one hand, the statutory scheme limits data sharing by placing restrictions on data that are important to consumers but largely out of their control.[59] On the other hand, the scheme still allows for free disclosure of information to third parties without consumer consent and does not require entities to actually protect data from breaches.[60]

The law regulating health care entities, the Health Insurance Portability and Accountability Act (HIPAA), is a good example of a more comprehensive statute. HIPAA and the accompanying HIPAA Privacy Rule provide robust safeguards for protected health information (PHI).[61] Covered entities and their business associates cannot use or share PHI without disclosing their purpose to consumers and obtaining consent.[62] With respect to data security, covered entities must put in place certain safeguards and are required to notify individuals in the event of a breach.[63] However, since the statute regulates specific covered entities, it only protects "channels of data flow," rather than actual categories of data.[64] In other words, data that are categorically similar but generated through inferences from data collected by nonregulated entities are not protected.[65] For example, HIPAA does not apply to health data collected through Fitbit or Apple Watches.[66] The end result is vast reservoirs of data that can be bought and sold relating to the health and physiology of individuals with no specific federal protection.[67]

The Children's Online Privacy Protection Act (COPPA) does more to address the "channels of data" critique[68] by protecting data categorically.[69] COPPA prohibits websites from collecting essentially any identifiable data about children under thirteen without verifiable parental consent.[70] The requirements of COPPA are delineated and

57. *Id.* at 14.
58. *Id.*
59. *See id.* at 44.
60. *Id.* at 12.
61. *Id.* at 10–11.
62. *Id.* at 11.
63. *Id.*
64. *See* Rostow, *supra* note 26, at 677.
65. *See id.*
66. *Id.*
67. *Id.* at 678.
68. *See id.*
69. MULLIGAN & LINEBAUGH, *supra* note 8, at 24.
70. *Id.*

enforced by the FTC through the COPPA Rule.[71] Notably, firms that collect data on minors must take reasonable procedures to protect their confidentiality, comply with deletion and retention requirements, and limit sharing to third parties.[72] However, COPPA only applies to operators of websites or online activities "directed at children" (as defined by the FTC), or operators with actual knowledge they are collecting children's data.[73] In practice, firms can evade the COPPA Rule's requirements with a formal policy banning children under thirteen and either a self-identification request or not asking for a user's age at all.[74] Moreover, a violation of the COPPA Rule is treated the same as a violation of Section 5 of the FTC Act (discussed Section I.B.2 below).[75] So while the FTC may impose civil penalties, there are no criminal penalties or private causes of action available under the Act.[76]

2. The Federal Trade Commission

Personal data that are not protected by a specific statute are primarily regulated by the FTC through the FTC Act.[77] Section 5 of the FTC Act declares "unfair or deceptive acts or practices in or affecting commerce" unlawful.[78] Private actors that are not regulated by a specific federal statute include merchants such as Macy's or Amazon and prominent technology firms like Facebook and Google.[79] The FTC has brought hundreds of enforcement actions against firms under Section 5, but most of these actions result in settlements.[80] As such, there is very little case law on the subject.[81] Instead, a collection of consent decrees, although not technically binding precedent, effectively creates a common law of privacy.[82]

---

71. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions [https://perma.cc/TF8K-HVF9].

72. MULLIGAN & LINEBAUGH, *supra* note 8, at 24.

73. 16 C.F.R. § 312.3 (2020).

74. *See* Shannon Finnegan, *How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future*, 50 SETON HALL L. REV. 827, 839–41 (2020).

75. 15 U.S.C. § 6502(c); MULLIGAN & LINEBAUGH, *supra* note 8, at 25.

76. MULLIGAN & LINEBAUGH, *supra* note 8, at 25.

77. *Id.* at 30.

78. 15 U.S.C. § 45.

79. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

80. MULLIGAN & LINEBAUGH, *supra* note 8, at 32.

81. Solove & Hartzog, *supra* note 79, at 588.

82. *Id.* at 624.

The most settled principle in the FTC privacy common law is that companies are bound by their privacy and data security promises under the "deceptive" prong of Section 5.[83] Examples of deceptive behavior include violating the terms of a posted privacy policy, mispresenting intended data use, and not providing notice of data practices.[84] The "unfairness" prong, on the other hand, is employed less frequently but can still be used beyond the scope of the "deceptive" prong.[85] For example, in *FTC v. Frostwire*, the FTC alleged that a peer-to-peer file sharing application had unfair privacy settings because it shared information immediately upon installation.[86] In addition, with respect to data security in *FTC v. Wyndham Worldwide Corp.*, the US Court of Appeals for the Third Circuit maintained that a company's failure to safeguard personal data may be unfair, even if the company did not contradict its privacy policy.[87]

3. State Law

In addition to federal law, all fifty states have laws regulating privacy and implementing liability for data breaches.[88] At the most basic level, this includes tort and contract law.[89] Negligence claims and class actions can regulate businesses that are inured from data security issues or fail to protect their customers from foreseeable harm.[90] Contracts and implied contracts can protect against data breaches as part of commercial arrangements.[91] Furthermore, many states have their own regulators policing unfair or deceptive practices modeled after the FTC.[92] Unlike federal law, each state also has its own data breach law requiring a notification response or imposing liability on companies in the event of a data breach.[93]

Notably, in 2018, California passed a particularly ambitious state privacy law, the California Consumer Privacy Act (CCPA).[94] The

---

83. MULLIGAN & LINEBAUGH, *supra* note 8, at 32.

84. *Id.* at 32–33.

85. *See* Solove & Hartzog, *supra* note 79, at 628, 638.

86. Complaint at 1, 13, FTC v. Frostwire LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011).

87. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–46 (3d Cir. 2015).

88. MULLIGAN & LINEBAUGH, *supra* note 8, at 36–37.

89. *Id.* at 36.

90. *Id.*

91. *Id.* at 37.

92. *See id.*

93. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/BT55-WLPN].

94. MULLIGAN & LINEBAUGH, *supra* note 8, at 37.

CCPA categorically protects all "personal information" of Californians, which is defined broadly to include nearly any information a business might collect.[95] Its provisions apply to any business that collects information from Californians, does business in California, and satisfies one of three threshold requirements.[96] The CCPA specifies certain consumer rights, including the right to know why and what data firms are collecting, the right to opt out of the sale of personal data, and the right to demand that a company delete personal information.[97] Regarding data protection, the Act provides a private cause of action for consumers whose "nonencrypted and nonredacted personal information" is subject to an unauthorized disclosure as a result of a business's failure to "implement reasonable security procedures and practices."[98] The proceeds from penalties and settlements under the Act are deposited in a Consumer Privacy Fund, which is used to offset the administration costs.[99] When the CCPA was initially passed, the state attorney general was responsible for enforcement.[100] However, in November 2020, California passed Proposition 24, which provides for the creation of a new state consumer privacy agency.[101]

II. ANALYSIS

A. The True Cost of a Data Breach

1. Public Harms

Current law regulating the use of personal data is focused on individual consumer privacy.[102] Individual privacy is undoubtedly at

95. *See* CAL. CIV. CODE § 1798.140(o) (West 2020) ("'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."); MULLIGAN & LINEBAUGH, *supra* note 8, at 38. The CCPA, however, does not apply to data that is subject to federal regulation like PHI under HIPPA. *See* CAL. CIV. CODE § 1798.146(a) (West 2020).

96. CAL. CIV. CODE § 1798.140(c) (West 2020) (defining "business" as having gross revenues under $25 million, collecting the personal information of fifty thousand customers, or deriving 50 percent or more of annual revenue from selling consumers information); MULLIGAN & LINEBAUGH, *supra* note 8, at 38.

97. MULLIGAN & LINEBAUGH, *supra* note 8, at 38–39.

98. CAL. CIV. CODE § 1798.150 (West 2020).

99. MULLIGAN & LINEBAUGH, *supra* note 8, at 39.

100. *Id.* at 38.

101. Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS INST.: TECHTANK (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/ [https://perma.cc/L7U9-HGVT].

102. *See, e.g.*, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020) (granting rights to *consumers* with regards to their *personal data*); FTC v. Wyndham Worldwide Corp., 799 F.3d 236,

stake when firms store comprehensive profiles of information about consumers, but the release of data has far more serious implications on the public as whole.

The greatest danger from data breaches comes from the predictive power of large aggregations of data sets. Although the unauthorized disclosure of personal information tends to capture the public's attention, data can be deployed to provide insights into almost any human behavior.[103] For instance, in 2012, Facebook ran a particularly troubling experiment where data scientists skewed seven hundred thousand users' newsfeeds so that they showed either mostly positive content or mostly negative content.[104] The affected users tended to post content that corresponded to the type of content on their newsfeed, which indicated that emotional states could be manipulated through the network.[105] Alternatively, data brokers compile and sell collections of consumer profiles that identify vulnerable individuals, labeling them "Rural and Barely Making It," "Ethnic Second-City Strugglers," or "Retiring Empty: Singles."[106] There is already a potential for abuse when firms legally hold data like this, such as offering shoppers different discounts or services based on their geolocation.[107] However, it is not hard to imagine how this could be used to facilitate illegal activity, as was the case in 2004 when criminals

---

240, 245 (3d Cir. 2015) ("The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that . . . taken together, unreasonably and unnecessarily exposed *consumers' personal data* to unauthorized access and theft."); MULLIGAN & LINEBAUGH, *supra* note 8, at 1–2 (referencing privacy concerns and misuse of *personal data* by private actors as factors causing data protection to emerge as a major issue for congressional consideration); *Protecting Consumer Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security [https://perma.cc/45X5-K98Q] (last visited Feb. 2, 2021) (describing the FTC's mission: "[t]he agency uses law enforcement, policy initiatives, and consumer and business education to protect *consumers' personal information*").

103. *See* Jacob Ward, *Why Data, Not Privacy, Is the Real Danger*, NBC NEWS (Feb. 4, 2019, 2:49 PM), https://www.nbcnews.com/business/business-news/why-data-not-privacy-real-danger-n966621 [https://perma.cc/4G68-B8U2].

104. *See* Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (June 28, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ [https://perma.cc/UN2H-4CUL]; *see also* Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCIS. U.S. AM. 8788, 8788 (2014).

105. Meyer, *supra* note 104.

106. *See* STAFF OF S. COMM. ON COM., SCI., & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 17 (Comm. Print 2013) (majority staff report for Chairman Rockefeller).

107. *See* Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534 [https://perma.cc/WV49-NHUH].

bought data lists from a data broker in order to target seniors with telemarketing scams.[108] The data broker advertised the lists with labels like "Suffering Seniors," which corresponded to individuals with cancer and Alzheimer's. One list even mocked the credulity of its own constituents, saying, "[t]hese people are gullible. . . . They want to believe that their luck can change."[109]

Under these circumstances, almost any transfer or release of data can lead to public harms. Although Facebook only ran its experiment for a week, several years later Cambridge Analytica obtained personal data from millions of Facebook accounts and facilitated the Russian disinformation campaign leading up to the 2016 US Presidential Election.[110] There is a clear privacy harm when Facebook transfers its users' personal data without permission. However, this pales in comparison to the institutional harm that could come from foreign interference in US elections.[111]

2. Comparing Data Breaches to Pollution

Once understood as a public harm, it follows that data breaches should be regulated like other public harms. Here, a particularly compelling model is environmental regulation.[112] The release of data is an unintended by-product of data collection and data-driven technologies, similar to how pollution—whether it be carbon emissions or the release of hazardous waste—is an unintended by-product of manufacturing industrial goods.[113] Firms are able to externalize the costs of their activities onto the general public because the release of these by-products dilutes public goods.[114] In the case of pollution, absent regulation, firms will contaminate public goods like clean air or water by improperly disposing of waste.[115] While the release of data may not

108. Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. TIMES (May 20, 2007), https://www.nytimes.com/2007/05/20/business/20tele.html [https://perma.cc/JS6J-P526].

109. *Id.*

110. *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout so Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/MVQ4-3Q2N].

111. *See* Ward, *supra* note 103.

112. *See generally* Ben-Shahar, *supra* note 20, at 112–14; Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

113. *See* Ben-Shahar, *supra* note 20, at 112.

114. *See id.*

115. *See* STEVEN A. GREENLAW, DAVID SHAPIRO, ERIC DODGE, CYNTHIA GAMEZ, ANDRES JAUREGUI, DIANE KEENAN, DAN MACDONALD, AMYAZ MOLEDINA, CRAIG RICHARDSON & RALPH SONENSHINE, PRINCIPLES OF ECONOMICS 276–80 (2d ed. 2017).

initially seem as harmful to the public as polluting clean air or water, the social harms of data breaches can be just as serious. Preventing the misuse of data benefits society as whole, for example, by ensuring elections are fair and free from foreign interference and establishing protection for the most vulnerable from predatory criminals; without proper safeguards, the release of data diminishes these public goods.

3. Assessing the Harm

With the understanding that data breaches are public harms, a regulatory regime concerned mostly with individual privacy does not fully address the public harm associated with breaches. If a factory was to negligently dump waste on an individual's property, that individual undoubtedly has suffered a personal harm. The government would likely respond by making such dumping a criminal offense and requiring companies to dispose of waste at designated sites. But what if the factory disposes of its waste properly at a dumpsite, and, over time, this waste seeps into a river, killing wildlife downstream? While government regulation successfully prevented personal harm to the individual, the public harm associated with the loss of wildlife remains.

Similarly, a privacy-focused regulation addresses the personal harm to individuals affected by data breaches, but does not address the public harm incurred in situations where data are unidentifiable or individual privacy is not at stake. For example, Strava, a social media workout app, posted heat maps of users' movements and locations around the world.[116] Although the individuals were not named, experts were able to locate US military installations in the Middle East based on data revealed by service members using Strava.[117] Even with a privacy regime in place, this direct harm to national security could still have occurred.

B. FTC Limitations and Advantages

1. The FTC's Limited Ability to Enforce Preventative Measures

The FTC plays a significant and effective role in promoting data security through its common law regulatory regime.[118] Using the deceptive prong of Section 5 to enforce a firm's own privacy policy

116. Richard Pérez-Peña & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, N.Y. TIMES (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html?searchResultPosition=1 [https://perma.cc/S2UT-EEAA].

117. *Id.*

118. *See supra* Section I.B.2.

improves data collection practices in some ways.[119] However, what happens when a firm's data practices do not contradict its privacy policy but nonetheless remain inadequate?

The US Court of Appeals for the Eleventh Circuit faced this question in one of the few cases on Section 5, *LABMD, Inc. v. FTC*.[120] Rather than relying on the deceptive prong of Section 5, the FTC alleged the defendant's data practices violated the unfairness prong of Section 5.[121] Specifically, the FTC argued that the defendant's practices were unfair, meaning the practice was one that (1) causes substantial injury to consumers and (2) offends public policy well-grounded in statutes or the common law.[122] With respect to the second element, the court failed to definitively hold whether the FTC's unfairness claim could be grounded in a common law theory of negligence.[123] Consequently, this negligence theory remains a potential source of litigation moving forward.[124] Instead the court held the FTC's order for the defendant to overhaul its cybersecurity and implement "reasonable standards" was unenforceable.[125] This could significantly limit the FTC's ability to address unfair or inadequate data security practices before a breach occurs.[126] The FTC relies on the threat of enforcement to incentivize firms to comply with its data protection standards.[127] If the FTC is limited to merely enforcing the terms of a firm's privacy policy or the FTC's unfairness claims must allege specific data failures and remedies, then it will mostly serve as a reactive regulator rather than a proactive one.[128]

2. Limited Resources and Advantages

Aside from the legal restraints on its Section 5 authority, the FTC is also an agency with limited resources when it comes to data

119. *See generally* Solove & Hartzog, *supra* note 79, at 587, 604.

120. MULLIGAN & LINEBAUGH, *supra* note 8, at 33–34.

121. *See* LABMD, Inc. v. FTC, 894 F.3d 1221, 1225 (11th Cir. 2018).

122. *Id.* at 1228–29.

123. *See id.* at 1231 ("We will assume arguendo that the Commission [was] correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice.").

124. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 33–34.

125. *LABMD, Inc.*, 894 F.3d at 1235–37 (holding that the FTC's order to LabMD to overhaul and replace its data-security program to meet an "indeterminable standard of reasonableness" made the command unenforceable).

126. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 34.

127. *See supra* Section II.B.

128. *See LABMD, Inc.*, 894 F.3d at 1237; MULLIGAN & LINEBAUGH, *supra* note 8, at 33.

protection and privacy.[129] As a result, the FTC must be particularly careful when considering enforcement actions, only pursuing those that offer the highest reward or the most effective form of deterrence.[130] The FTC's limited resources are especially evident when compared to privacy enforcers in other countries.[131] Whereas most agencies in other countries focus entirely on privacy regulation, privacy is simply one part of the FTC's complicated and expansive regulatory jurisdiction.[132]

Despite these limitations, the FTC remains a data regulator with specific advantages that should not be overlooked. Several have to do with the agency's structure. First, it is resistant to regulatory capture in ways other agencies are not because it does not regulate a single coherent industry.[133] Second, because of its broad focus, it does not get bogged down in procedural practices for protecting information.[134] Third, the FTC is an independent agency, which allows at least some bipartisan representation as well as staggered terms for commissioners;[135] this arguably creates some political insulation.[136]

However, the most important advantage the FTC has as a regulator is experience implementing a complex privacy regulatory regime.[137] The FTC has emerged as the de facto privacy regulator governing vast segments of the private sector with little direction from Congress.[138] It is tasked with overseeing privacy provisions in eight other federal statutes, including COPPA and the Fair Credit Reporting Act (FRCA).[139] Moreover, the FTC has the ability to react nimbly to changes in the market and changes in the technology.[140] Given these

129. Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS INST.: TECHTANK (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/5W56-YA5N].

130. *Id.*

131. *See id.* ("[The FTC] carries out [its] mission with a budget of just over $300 million and a total staff of about 1,100, of whom no more than 50 are tasked with privacy. In comparison, the UK's Information Commissioner's Office (ICO) has over 700 employees and a £38 million budget for a mission focused entirely on privacy and data protection.").

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *See id.*

137. *See, e.g.*, *id.*

138. *See id.*

139. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2018 2 (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/Q55V-QPNG].

140. Solove & Hartzog, *supra* note 79, at 589.

advantages, the FTC has significant value as a data regulator, despite its limited enforcement capabilities, that would not be easily replaced.

C. Limitations of State Regulation

By responding to a data breach or imposing tougher data protection measures, states can influence businesses' behavior.[141] Yet, their limited jurisdictional reach creates problems for consumers and firms.[142] For example, most states have data breach notification requirements with strict penalties for companies that fail to comply.[143] In 2018, Uber paid a $148 million settlement for failing to notify consumers of a data breach.[144] However, this state notification system has been described as a "fragmented, incoherent liability scheme."[145] Each state has unique and sometimes inconsistent reporting requirements that impose significant compliance costs.[146] Determining whether an individual is a resident of a particular state is also difficult and might even require a company to collect more data on an individual than it would otherwise.[147] Notification laws are just one form of state regulation, but other forms of state regulation present similar problems.[148]

D. National Legislation

Given the issues with federal statutes and the costs of state regulation, a federal response to data breaches seems inevitable. Indeed, according to a 2019 Pew Research study, 75 percent of Americans believe there should be more regulation of private firms' use of personal data. Moreover, only 8 percent of firms believe they should be regulated less.[149]

One possible model for federal data breach legislation is the European Union's General Data Protection Regulation (GDPR). GDPR

---

141. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 36–37.

142. *See id.* at 37.

143. *See* GINA STEVENS, CONG. RSCH. SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 5–7 (2012).

144. Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html [https://perma.cc/P3A5-FNRH].

145. STEVENS, *supra* note 143, at 5.

146. Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1570–71 (2010).

147. *Id.*

148. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 36–37.

149. Auxier et al., *supra* note 24.

applies to any company that handles European data, so many multinational firms must already comply with its provisions.[150] It regulates the "collection, use, storage, organization, disclosure or any other operation or set of operations performed on personal data" and defines personal data broadly.[151] It is centered on a set of individual privacy and data control rights, much like the CCPA.[152] However, unlike the CCPA, it also includes specific, risk-based security measures[153] and a privacy-by-design approach in which firms only collect the data minimally necessary to complete a lawful purpose.[154] In addition, GDPR contains breach notification requirements that require firms to notify designated government authorities and affected individuals within seventy-two hours of a breach.[155] Individual member states enforce the provisions of GDPR and are permitted to issue significant fines for serious infractions.[156] Individuals are also guaranteed judicial recourse in the event of a breach.[157]

GDPR clearly addresses many of the issues associated with data breaches,[158] but such prescriptive regulations have their costs. GDPR is an incredibly complex law and continues to add significant new obligations for firms handling data.[159] The average cost of becoming GDPR compliant in 2018 was approximately $3 million per firm.[160] Notably, these heavy costs tend to strengthen the largest players with the resources and experts needed to comply with the law while pricing out smaller firms.[161] Even US firms valued in the billions like Williams Sonoma and Valve have had to exit the European market because of the

150. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 42–43.

151. *Id.* at 42–51.

152. *Id.* at 44–45, 50–51.

153. *Id.* at 46–47.

154. Matthew R. A. Heiman, *The GDPR and the Consequences of Big Regulation*, 47 PEPP. L. REV. 945, 947 (2020).

155. MULLIGAN & LINEBAUGH, *supra* note 8, at 47–48

156. *Id.* at 50.

157. *Id.*

158. *See* discussion *supra* Section II.A.

159. *See* Heiman, *supra* note 154, at 949; Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance*, CNBC, https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html [https://perma.cc/Z9KB-Y3S5] (last updated Oct. 8, 2019, 10:38 AM).

160. *IAPP-EY Annual Privacy Governance Report 2018*, IAPP RES. CTR., https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/ [https://perma.cc/H6MV-2245] (last visited Feb. 2, 2021).

161. Heiman, *supra* note 154, at 949.

costs of compliance associated with GDPR.[162] Additionally, the implementation of GDPR was accompanied by a decline in European venture capital and start-up firms.[163] While the importance of consumer data protection cannot be ignored, at a certain point, heavy regulation may impose costs that hurt innovation and deter beneficial consumer products and services.[164]

In light of these costs, the CCPA might serve as a better model for national legislation. The CCPA ultimately has fewer sweeping provisions than GDPR.[165] Regarding data protection, the "reasonable security measures" requirement allows data holders, rather than regulators, to set data security practices.[166] This is more consistent with the FTC's approach to data security, which generates an ecosystem of mutual governance between firms and regulators.[167] Compared to GDPR, the CCPA also implements far fewer stringent fines for violations. However, the cost of CCPA compliance is estimated to be quite similar to GDPR.[168] This is likely because the costs of compliance are mostly attached to privacy requirements, like hiring privacy staff, rather than technical protections against data breaches.[169] Indeed, more business executives seem to regard privacy governance as separate from the issue of data breaches altogether.[170] Congress could take an approach similar to GDPR or the CCPA, but this type of regulation is expensive, and both are primarily centered on individual privacy. Both can and should serve as useful models for Congress, but an effective and comprehensive solution to the public harm associated with data breaches will require a different approach.

---

162. *The 10 Problems of the GDPR: The US Can Learn from the EU's Mistakes and Leapfrog Its Policy: Statement Before the S. Judiciary Comm.*, 116th Cong. 3–4 (2019) [hereinafter *GDPR Hearing*] (statement of Roslyn Layton, Visiting Scholar, American Enterprise Institute).

163. *Id.* at 2–4.

164. *See* Ben-Shahar, *supra* note 20, at 134–35.

165. *See supra* Section II.B.

166. *Cf.* Anne S. Peterson, *Industry Insight: The CCPA's Elusive "Reasonable Security" Safe Harbor*, MCGUIREWOODS (Feb. 17, 2020), https://www.passwordprotectedlaw.com/2020/02/ccpa-reasonable-security/ [https://perma.cc/7FN8-9ZU4] (stating that because the CCPA does not define what constitutes "reasonable security," data-holding companies are largely left to interpret that provision themselves).

167. *See GDPR Hearing*, *supra* note 162, at 12–14.

168. Feiner, *supra* note 159.

169. *See IAPP-EY Annual Privacy Governance Report 2018*, *supra* note 160.

170. *Id.*

III. A DATA SUPERFUND STATUTE

If the release of data is to be best understood as a public harm like pollution, then an effective regulatory approach should incorporate lessons from environmental law. That said, using environmental law as a model can be difficult as environmental regulation encompasses numerous modes of regulation.[171] This is in part because the environment is a complex and highly interconnected system; as such, many of the root causes of pollution are also systematic.[172] Indeed, the data environment is no different, and with this understanding, regulating data like regulating the environment will likely require a nuanced and multifaceted regulatory approach.[173] Arguably, this is already occurring in an incremental fashion, as Congress and the states target specific industries and types of data pollution. While the United States may not be able to prevent all forms of data pollution, it could still implement a more comprehensive form of protection.

A. CERCLA as a Comprehensive Solution

1. Getting to CERCLA

Similar to data regulation, environmental regulation has developed in a piecemeal fashion in response to growing public awareness and concern about pollution.[174] The most significant environmental statutes were passed during the 1970s and 1980s.[175] The first was the National Environmental Policy Act (NEPA), which requires agencies to conduct an environmental impact statement before any major federal action.[176] Congress also enacted two particularly sweeping and ambitious statutes targeted toward specific types of pollution: the Clean Water Act (CWA), regulating discharges into the water, and the Clean Air Act (CAA), regulating emissions into the air.[177]

---

171. *See* Neil Gunningham, *Enforcing Environmental Regulation*, 23 J. ENV'T L. 169, 172–74 (2011).

172. *See generally Clean Air Act Overview, Air Pollution: Current and Future Challenges*, ENV'T PROT. AGENCY, https://www.epa.gov/clean-air-act-overview/air-pollution-current-and-future-challenges [https://perma.cc/A8L4-YSRZ] (last visited Feb. 3, 2021).

173. *See* Gunningham, *supra* note 171.

174. *See generally* Richard J. Lazarus, *The Greening of America and the Graying of United States Environmental Law: Reflections on Environmental Law's First Three Decades in the United States*, 20 VA. ENV'T L.J. 75 (2001) (discussing the creation and evolution of environmental law in the United States and the gradual means by which that occurred).

175. *See generally id.* (outlining the most relevant environmental statutes in the United States, revealing that the majority of them were passed in the 1970s and 1980s).

176. *Id.* at 77.

177. *Id.* at 78–79.

Even in the face of an energy crisis and industry resistance, these laws survived with only minor modifications.[178] Indeed, Congress went on to pass several more environmental laws targeted towards toxic and hazardous substances.[179]

This period of environmental legislative action culminated with the passage of the last major environmental legislation to date, the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), also known as the Superfund.[180] CERCLA was passed in response to alarming hazardous waste practices and management in the 1970s.[181] It was arguably the most far-reaching of all environmental statutes.[182] Its basic design is relatively simple. CERCLA imposes strict liability for the release or threatened release of any "hazardous substances," which encompasses just about any toxic substance as well as any substance the Environmental Protection Agency (EPA) deems "an imminent and substantial danger" to public health or safety.[183] Additionally, CERCLA liability is broad; it is the first environmental statute that subjects every major Fortune 500 company, many small businesses, and nonprofit institutions to environmental liability.[184]

Since its passage, CERCLA has been subject to criticism, and scholars continue to debate its effectiveness.[185] The original statute was rushed through Congress, which left courts to grapple with a number of ambiguities.[186] While there are many problems with CERCLA as a statute, a full analysis of its provisions is beyond this Note. However, the basic design of this statute still offers a particularly compelling regulatory model for data breaches.

---

178. *See id.* at 82–83

179. *Id.* at 83.

180. *Id.*

181. ROBERT V. PERCIVAL, CHRISTOPHER H. SCHROEDER, ALAN S. MILLER & JAMES P. LEAPE, ENVIRONMENTAL REGULATION: LAW, SCIENCE, AND POLICY 409 (8th ed. 2018).

182. Lazarus, *supra* note 174, at 84.

183. 42 U.S.C. §§ 9601(14), 9604(a); *see* PERCIVAL ET AL., *supra* note 181, at 410–11.

184. Lazarus, *supra* note 174, at 89.

185. *See generally* Justin R. Pidot & Dale Ratliff, *The Common Law of Liable Party CERCLA Claims*, 70 STAN. L. REV. 191 (2018) (debating the viability of CERCLA in light of the changing liability framework overseen by the EPA); Keely Maxwell, Brittany Kiessling & Jenifer Buckley, *How Clean Is Clean: A Review of the Social Science of Environmental Cleanups*, 13 ENV'T RSCH. LETTERS, no. 8, 2018, at 1 (discussing the merits of various environmental cleanup efforts, including CERCLA, through the lens of various publications that discuss the issue).

186. *See* Steven Ferrey, *The Toxic Time Bomb: Municipal Liability for the Cleanup of Hazardous Waste*, 57 GEO. WASH. L. REV. 197, 233 n.230 (1988).

2. Filling Regulatory Gaps

One advantage of CERCLA is that it serves as a backdrop to other environmental statutes without supplanting other forms of regulation.[187] Indeed, the statute was partially designed to "fill the gaps" left by other federal environmental statutes.[188] For example, while the types of hazardous waste covered by the statute are broad, it specifically exempts substances regulated by other federal statutes.[189]

Such an accommodating design would be desirable in the context of data protection. The issue with current federal data breach statutes is not that they fail to accomplish their statutory objectives; rather, it is that, together, they fail to comprehensively protect data.[190] Arguably, statutes like HIPAA, which regulates data pollution from health care providers, and COPPA, which regulates data pollution from minors, play a similar role as the CWA or CAA. Public concern over data collection varies among specific purposes and industries.[191] Protecting certain types of data, like data relating to children, may demand stricter regulations while other types may not be as critical to protect.

At the same time, CERCLA's liability regime holds nearly all environmental polluters accountable, which prevents businesses from escaping liability. CERCLA liability extends not only to parties that actually dispose of hazardous waste but also to the parties that generate and transport the waste.[192] Over time, courts have interpreted this liability to be "strict, joint and several, and retroactive."[193] Considering the data collection and resale practices of data brokers, such liability in the context of data breaches could play a critical role in holding businesses accountable. Under current law, as long as a business permits data sharing in its privacy policy, it can sell data to irresponsible third parties without any consequences.

---

187. *See* PERCIVAL ET AL., *supra* note 181, at 409.

188. *See id.* (stating that CERCLA was enacted after the CWA and the CAA and just four years after Congress "thought it closed the last remaining loop hole in environmental law").

189. *See id.*

190. *See supra* Part II.

191. *See supra* Part II.

192. 42 U.S.C. § 9607(a) (extending liability to current owners and operators, owners and operators at the time waste was disposed of at the facility, generators of the waste, and persons who transported waste to the facility); PERCIVAL ET AL., *supra* note 181, at 409.

193. DAVID M. BEARDEN, CONG. RSCH. SERV., R41039, COMPREHENSIVE ENVIRONMENTAL RESPONSE, COMPENSATION, AND LIABILITY ACT: A SUMMARY OF SUPERFUND CLEANUP AUTHORITIES AND RELATED PROVISIONS OF THE ACT 14 (2012).

3. Incentives

CERCLA's liability regime also serves as a powerful incentive for businesses to prevent environmental pollution from occurring in the first place. Under a strict liability regime, parties are held accountable for any harm that results from certain activities, often characterized as ultrahazardous activities, regardless of the level of care they exercised.[194]

Strict liability has been discussed as an effective tool to encourage data security and prevent data breaches.[195] Generally speaking, the certainty of liability in the event a breach occurs and the financial penalties that come along with it would force firms that collect and hold data to internalize the full costs of their activities.[196] Ideally, this would prevent the firms that are operating with suboptimal levels of data protection from entering the market in the first place.[197]

4. Administration

Furthermore, CERCLA, unlike other environmental statutes, not only serves to prevent environmental pollution from occurring but it also enables regulators to take direct action in response to the release of pollutants.[198] Although liability is at the heart of CERCLA, the statute complements this liability with specific response and remediation provisions.[199]

Despite many similarities, data has certain unique qualities that make this part of the CERCLA model difficult to replicate.[200] Prominent examples include the cleanup requirements, which direct the EPA to establish standards and actually clean up polluted sites.[201] Unlike the cleanup of localized hazardous waste, data cannot be scrubbed, and it may very well be impossible to retrieve once it has been released.[202]

Nevertheless, there are still two critical, ex-post provisions of CERCLA that would serve to improve federal responses to data breaches. One such provision is the notification requirements under

194. Keats Citron, *supra* note 112, at 265–66.
195. *See id.* at 287.
196. *See id.* at 266–67.
197. *See id.*
198. BEARDEN, *supra* note 193, at 1.
199. *See id.*
200. *See* Ben-Shahar, *supra* note 20, at 143.
201. BEARDEN, *supra* note 193, at 1–2.
202. *See* Ben-Shahar, *supra* note 20, at 143.

Section 103(a).[203] This Section requires a party who is responsible for a release of a hazardous substance exceeding the regulatory limit to immediately notify a National Response Center.[204] Similar notification requirements could apply to companies that release a certain amount of personal data as a result of a data breach. Another part of CERCLA that would be particularly useful for data breaches is the superfund provision, which provides the EPA with independent financing to respond to and clean up releases.[205] This provision is quite similar to the Consumer Privacy Fund provisions in the CCPA.[206] Although data cannot be cleaned, there are still mitigation techniques that can be employed to shift and spread the costs of a breach.[207] A data regulator with independent funding would not have to wait for lengthy judicial proceedings to take action when a breach occurs.

B. Implementing a Data Superfund Statute

1. Statutory Objectives

When it comes to implementing a data superfund statute, inevitably, the CERCLA model would need to be adjusted, but as a whole it offers numerous advantages compared to other models of data regulation. Importantly, a data superfund statute modeled after CERCLA would remain primarily focused on protecting data without sacrificing some privacy objectives. Privacy is no doubt important in some contexts, but prescriptive privacy regimes like GDPR and the CCPA are expensive.[208] Privacy costs may be justifiable for health care data or children's data, but they would likely lead to unacceptable inefficiencies if applied to the economy as a whole.[209] A data protection statute modeled after CERCLA would allow for a more flexible approach to privacy. Moreover, strict liability and joint liability, even in a regime focused on public harms, would allow the data superfund statute to indirectly improve consumer privacy. For instance, the risk of future liability may encourage behavior that is otherwise required by the GDPR privacy-by-design provision.[210] Instead of requiring a lawful purpose to collect minimally necessary data, firms with suboptimal

203. BEARDEN, *supra* note 193, at 5.
204. *Id.*
205. *See id.* at 38.
206. *See* MULLIGAN & LINEBAUGH, *supra* note 8, at 39.
207. *See* Ben-Shahar, *supra* note 20, at 144–45.
208. *See supra* Part II.
209. *See* Ben-Shahar, *supra* note 20, at 145.
210. *See supra* Part II.

levels of data protection would face powerful incentives to not collect more data than necessary for their business purpose.[211]

2. Allocating Responsibility

Implementing strict and joint liability under a data superfund statute would also serve to allocate responsibility for preventing breaches in a more effective way.[212] Since this type of liability essentially rises proportionately to the potential harm of a breach, firms could weigh the costs and risks of a breach on their own terms.[213] Although this could also lead to overcompliance, there are fewer opportunity costs and efficiency losses resulting from the government incorrectly weighing the risks of data collection practices.[214] Furthermore, without as many prescriptive requirements, companies may be spared the heaviest GDPR expenses that result from mandatory compliance personnel.[215]

Holding firms jointly liable would also make sense in the context of data because firms are usually in a better position than consumers to assess the quality of a business's data protection measures.[216] This is particularly salient considering consumers' behavior towards privacy policies and the privacy paradox more generally.[217] While consumers will continue to provide information to firms with suboptimal data practices, a firm is unlikely to ignore the risk of liability.[218] In particular, even if firms were to transfer data to third parties or protect themselves with a contract, they would still ultimately be responsible to the public.[219]

Nevertheless, there are downsides to this approach. A single business with adequate security standards could be left footing the bill because another business was irresponsible. CERCLA allows parties to seek out contribution from other liable parties, but this can be difficult in practice.[220] However, many of these concerns were created by court

---

211. *See* Keats Citron, *supra* note 112, at 256.

212. Since the law took effect in January 2020, the attorney general has pointed to specific guidelines, but no California precedent establishes the "reasonableness" of the guidelines. *See supra* Part II; Peterson, *supra* note 166.

213. *See* 42 U.S.C. § 9609(a)(3).

214. *See* Ben-Shahar, *supra* note 20, at 134–35.

215. *See supra* Part II; *IAPP-EY Annual Privacy Governance Report 2018*, *supra* note 160.

216. *See* Keats Citron, *supra* note 112, at 284–85.

217. *See supra* Part I.

218. *See supra* Part I; Keats Citron, *supra* note 112, at 266–67.

219. PERCIVAL ET AL., *supra* note 181, at 445.

220. *See* Pidot & Ratliff, *supra* note 185, at 222, 243–48.

interpretations of a hastily written statute.[221] A data superfund statute could avoid these mistakes, for example, by making joint liability explicit in the statute.

3. Utilizing Existing Structures

Another advantage to the CERCLA model is that Congress could use existing state and federal regulatory structures to implement a data protection equivalent. The FTC could serve the same role for the data superfund statute as the EPA does for CERCLA.[222] As discussed in Section II.B.2, the FTC already has significant expertise and experience enforcing privacy regulation in the United States.[223] The FTC Commissioner has a narrower set of responsibilities than an attorney general but retains the advantage of having a broader interest than European data regulators.[224] Moreover, companies seeking to avoid liability under the data superfund statute could largely follow FTC guidance. Since the Act would center around liability rather than specific terms, the FTC and courts could continue to build off the Section 5 common law of privacy.[225] This would provide more flexibility—similar to the reasonable security duty in the CCPA—with less uncertainty.[226]

Furthermore, the FTC would administer the data trust fund and initiate data cleanups. To mitigate private costs, the FTC could ensure that consumers immediately receive identity theft protection. This is already something the FTC incorporates into settlements after a data breach, except with a trust fund it could be done without lengthy judicial proceedings.[227] For more public costs, the FTC could provide Congress, other government agencies, and state governments the information they need to implement new policies to respond to a breach. It could also coordinate an industry response among major stakeholders, such as data insurers, cybersecurity firms, and banks.

As part of enforcement, CERCLA also enables a private cause of action; thus, private individuals bear the burden of enforcement along

---

221. *See id.* at 223.

222. PERCIVAL ET AL., *supra* note 181, at 410.

223. *See supra* Part II.

224. *See supra* Part II.

225. *See supra* Part I.

226. *See supra* Section III.D; Peterson, *supra* note 166.

227. *See e.g.*, Robert Schoshinski, *Equifax Data Breach: Pick Free Credit Monitoring*, FED. TRADE COMM'N: CONSUMER INFO. BLOG (July 31, 2019), https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring [https://perma.cc/Y8W3-NR4E].

with government regulators.[228] This is present in both GDPR and the CCPA but absent from many federal data protection requirements.[229] However, unlike the CCPA, a data superfund statute would contain no qualifying language or "reasonable security" safe harbor to prevent lawsuits.[230] This feature has the potential to relieve regulatory burdens that would be more prominent for an agency like the FTC, which already faces limited resources.[231]

A data superfund statute could work in tandem with state law when it comes to notification requirements. A national data breach response center would provide a uniform reporting system for businesses while utilizing state frameworks to carry out the response. This would allow federal regulators to build off the experiences of state regulators enforcing state notification laws while addressing the problems associated with the current patchwork of state and federal statutes.[232] Much like GDPR, it could coordinate responses and require notification in the event of a breach. Although regulators cannot necessarily retrieve data, a national response system could still improve accountability and give victims and policy makers more of an opportunity to mitigate damages.[233]

IV. CONCLUSION

The current regulatory approach and public concerns associated with data breaches are overwhelmingly focused on protecting individual privacy. While consumer privacy is important, this framework only addresses one aspect of the data problem. The harms associated with data breaches go beyond identity theft or personal exposure. As personal data are collected on an increasingly massive scale, the predictive capacity of this data will correspondingly expand. With this will come insight into human behavior that could provide substantial benefits to society, but it could also serve as a potent weapon to exploit the public. Data breaches are fundamentally social problems, and the federal government must do more to prevent these social harms.

---

228. Jeffrey M. Gaba, *The Private Causes of Action Under CERCLA: Navigating the Intersection of Sections 107(a) and 113(f)*, 5 MICH. J. ENV'T & ADMIN. L. 117, 119 (2015).

229. *See supra* Part II.

230. *See supra* Part II; Peterson, *supra* note 166.

231. *See supra* Part II.

232. *Supra* Section III.C.

233. *See* Ben-Shahar, *supra* note 20, at 143; Gabe Maldoff & Omer Tene, *Born in the USA: The GDPR and the Case for Transatlantic Privacy Convergence*, 17 COLO. TECH. L.J. 295, 305–06 (2019).

GDPR and the CCPA exhibit a primarily privacy-based approach to data breaches. Although they are comprehensive, these statutes present significant costs to businesses and regulators alike. A data superfund statute, by contrast, would incorporate some data protection models from both laws without the significant compliance costs. Perhaps with advances in technology, expansive measures ensuring consumer control over personal data might be justified. Yet, for now, individual privacy would be better served by a sector-specific approach. A liability-focused regime with limited prescriptive requirements would provide a flexible but effective regulatory regime as society defines the contours of privacy rights in the modern world.

Kyle McKibbin[*]

* J.D. Candidate, Vanderbilt University Law School, 2021; B.A., University of Maryland, College Park, 2016. The Author would like to thank Professor Michael P. Vandenbergh for his guidance and his environmental law course which served as the inspiration for this Note. The Author would also like to thank his family, friends, and mentors who encouraged him while he pursues a career focused on the legal implications of privacy and technology. The board and staff of the *Vanderbilt Journal of Entertainment and Technology Law* deserve a special thank you for their meticulous work in helping bring this Note to publication.