MERCATUS POLICY RESEARCH

NAVIGATING DATA SECURITY CHALLENGES

POLICY INNOVATIONS AND REFORM OPTIONS

Tracy C. Miller

MERCATUS.ORG

MERCATUS CENTER
George Mason University

Tracy C. Miller. "Navigating Data Security Challenges: Policy Innovations and Reform Options." Mercatus Research, Mercatus Center at George Mason University, Arlington, VA, March 2024.

ABSTRACT

Data breaches create a serious problem that increases the risk of identity theft and credit card fraud. Although sometimes caused by the intentional actions of hackers, data breaches are often the result of consumer, employee, or contractor carelessness, or inadequate precautions by firms to safeguard data. This research explores policies that influence firms' decisions about managing the sensitive data they collect, acquire, or process. This paper considers the advantages and disadvantages of litigation and Federal Trade Commission (FTC) regulation in motivating firms to take data security precautions. Today, neither FTC regulation nor litigation gives firms enough incentives to take stricter precautions; the FTC generally lacks the authority to require monetary restitution, and courts often deny standing to breach victims. Because determining negligence is difficult, Congress or state legislatures might consider giving the courts authority to hold firms liable for consumer-data breaches. It would heighten security if the FTC in cooperation with state attorneys general continue to play an important role in penalizing firms on a case-by-case basis for unreasonable data-security practices. Congress could affirm this role by granting the FTC authority to obtain monetary restitution.

JEL codes: H7, K2, K41

Keywords: data security, externality, risk, incentives, standing, negligence, strict liability, common law, second best, moral hazard, fiduciary

INTRODUCTION

Data security is a serious problem. As people spend more time online buying and selling goods and services, communicating medical information, managing their investments, and interacting with friends and coworkers, sensitive information may be revealed to those who could use it for harm. In the first four months of 2023, almost 340 million people were affected by publicly reported data breaches or leaks.[1] The sensitive data exposed by data breaches often results in identity theft, fraudulent use of credit cards or financial accounts, or disclosure of personally sensitive information to those who have no right to know it.

Legislation has been enacted on the data-security responsibilities of banks and other financial institutions, educational institutions, and some health providers. But for data collected in most other sectors, there is no federal legislation requiring companies to safeguard the personal information they collect, process, and store. In some cases, those whose data was exposed via data breaches have pursued lawsuits against the firm that experienced the data breach. The Federal Trade Commission (FTC) and state attorneys general have also taken action against firms that have experienced data breaches.

But there are good reasons to conclude that firms that collect and process data are not taking enough precautions to prevent breaches. This can be blamed on the fact that in many cases for firms, the cost of a data breach is small relative to the cost of preventing it. Although courts and regulatory agencies should continue to play a complementary role in data-security regulation, legislation establishing a strict liability standard could result in larger and more consistent penalties. This in turn could reduce the number and severity of data breaches and result in a more optimal balance between harm and the spending needed to reduce it.

1. Howard Solomon, "Data on Over 340 Million People Exposed so far This Year," *Cyber Security Today*, podcast, April 28, 2023.

Data security has multiple dimensions. It includes preserving access to data as well as preventing unauthorized acquisition and use of data, whether the data consists of personal information or proprietary information of a business or government agency. This research focuses on the problem of unauthorized access and use of personal information, with emphasis on data breaches involving data collected or stored by firms. The next section describes the nature of data-security problems; then I discuss the role played by legislation, litigation, and regulation in promoting data security, and reforms that might help. I conclude that data security could be improved if Congress enacts legislation imposing a regime of strict liability for data breaches. I also consider second-best approaches to policy for improving data security.

THE PROBLEM OF DATA BREACHES

Data breaches may be the result of deliberate attempts by hackers or careless actions of employees or contractors who have access to a firm's data. It is difficult to apprehend hackers who obtain unauthorized access to data for harmful purposes, but firms can take precautions to reduce the risk of data breaches due to carelessness. Prevention is likely to be much more effective in reducing the frequency and severity of data breaches than attempts to apprehend hackers.[2]

Although data security is often lumped together with privacy, they are different in important ways. Security is about preventing unauthorized parties from having access to data; privacy is based on a "normative framework" for determining who should be allowed to access and alter information.[3] Discussions of policy regarding data security tend to revolve around the extent of firms' obligations. What precautions should firms be expected to take? Taking precautions is costly, and at some point the costs exceed the benefits at the margin.

The goal of data-protection policy is not to eliminate all data breaches but to find cost-effective ways to limit their number. To reduce data breaches, firms should consider some combination of technology, training, and changes to data-protection practices. Firms have incentives to keep data secure even if the government does not enforce rules or penalize them for security lapses. Firms risk reputational costs and stock-price declines if they have lax security practices

2. It is very difficult to determine the identity of hackers or where hacks come from. See Larry Greenemaier, "Seeking Address: Why Cyber Attacks are so Difficult to Trace Back to Hackers," *Scientific American* (June 11, 2011).
3. Derek Bambauer, "Privacy vs. Security," *Journal of Criminal Law & Criminology* 103 (2013): 667–9.

that lead to data breaches,[4] and a chief executive may be removed in response to a serious breach. Still, some firms may not have adequate incentives to invest in security measures, either because of agency problems or externality problems.

THE ROLE OF GOVERNMENT

To address misaligned incentives of firms that collect, store, and process data, courts and regulatory agencies, such as the FTC and the Securities and Exchange Commission, have enforced information-security laws. In theory, consumers could weigh the expected costs of data breaches in their purchase decisions, which would give firms an incentive to find ways to reduce those costs. But this does not work if external costs are substantial, as when most of those harmed by a breach are not customers of the firm: This can be the case with credit-reporting agencies, ad tech firms, small online and offline retailers, and data brokers.[5] Also, many (possibly most) consumers do not have the requisite information to compare and evaluate firms' data-security practices, so firms may be able to get away with lax practices—at least until they experience a breach.[6]

Federal and state governments have enacted some statutes concerning data protection. All fifty states and the District of Columbia have passed breach notification laws. But "these laws usually only require data collectors to alert data subjects" if an unauthorized third party has gained access to their personal information; they do not provide additional recourse to consumers.[7]

Notification laws have required firms suffering data breaches to be much more transparent. But sending letters to everyone affected by a breach can be quite costly, and requiring such letters works like a strict liability fine, involving

4. Sangchui Park, "Why Information Security Law has been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records," *International Review of Law and Economics* 58 (2019): 132–45.
5. When credit-card data are stolen from online or offline retailers, most of the cost is born by the issuing banks, not by the owners of the credit cards. For more on externalities, see Park, "Why Information Security Law has been Ineffective," 132–45.
6. James C. Cooper and Bruce H. Kobayashi, "Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem," *Michigan Technology Law Review* 28 (May 2022): 277–304.
7. Daniel M. Filler, David M. Haendler, and Jordan L. Fischer, "Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data," *Connecticut Law Review* 54 (2022): 116.

costs whether or not an organization was at fault for the breach.[8] In violation of the law, many data breaches are not reported.[9]

Besides data-breach notification laws, the federal government and some state governments also regulate data-security protection in other ways. Some industry-specific federal regulations require firms to take proactive measures in collecting or securing personal information. These apply to the health care, finance, and education industries.[10] For example, the Gramm–Leach–Bliley Act requires that financial institutions provide notice to consumers about what information the firm collects, with whom it shares that information, and how it protects it.[11]

Several federal agencies, including the Office of Civil Rights, the Federal Communications Commission, the SEC, and the FTC, are involved in the enforcement of privacy and data security. The FTC plays a particularly prominent role as part of its mission of "protecting the public from deceptive or unfair business practices."[12]

Several state governments, including Massachusetts, Oregon, and Nevada, have enacted data-security laws. In 2016, New York enacted a cybersecurity regulation, which applies to financial-services institutions. New York regulators have imposed standards for data encryption, multifactor authentication, annual certification, and incident-response plans that go beyond current regulatory requirements and industry practices.[13] Data-security regulation can take a standards approach, as pursued by the states listed above, or a reasonableness approach, usually taken by federal regulatory agencies.[14] The reasonableness approach is similar to a negligence standard and is discussed in more detail below. Before considering the role of regulatory agencies in dealing with data breaches, we must discuss the role of private litigation.

---

8. Daniel J. Solove and Woodrow Hartzog, *Breached! Why Data Security Fails and How to Improve It* (Oxford, England: Oxford University Press, 2022), 45.
9. In a survey of over 400 IT and security professionals who work in companies with 1,000 or more employees, 29.9 percent admitted to keeping a breach confidential instead of reporting it. See Tim Keary, "A Third of Organizations Admit to Covering Up Data Breaches," *VentureBeat*, April 5, 2023.
10. The Health Insurance Portability and Accountability Act was enacted in 1996. The Gramm-Leach-Bliley Act, governing financial information, was enacted in 1999. The Family Education Rights and Privacy Act was enacted in 1974. See Filler et al., footnote 22.
11. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 106th Congress (1999), https://www.congress.gov/106/plaws/publI02/PLAW-106publ102.pdf.
12. "About the FTC," Federal Trade Commission.
13. Summary of New York State Dept. of Financial Services' proposed cybersecurity requirements for Financial Services Companies. See *Journal of Internet Law*, October 2016, 27–31.
14. Solove and Hartzog, "*Breached!*," 48–49.

Litigation

When consumers can identify which firm was responsible for a breach of their data, they may be able to overcome agency problems by suing the firm. Even if only a minority of consumers have enough information to implicate a specific firm, they can initiate a class-action suit on behalf of everyone who may have been harmed by a data breach. By raising the expected costs of a data breach, litigation can give firms greater incentives to take steps to secure the data they collect, store, or process.

Law, technology, and employee training can work together to reduce the likelihood and severity of data breaches. Ideally, firms should have an incentive to implement technology and training that reduces the incidence of breaches in a cost-effective way. One purpose of litigation is to impose costly consequences for harmful outcomes to motivate responsible parties to take precautions.

The advantage of litigation over regulation is that those who suffer damages make their decision to litigate on the basis of the magnitude of the costs they experience from a breach. By contrast, regulatory agencies select cases on the basis of political and bureaucratic motivations, which are not closely related to the expected costs of a breach.[15]

Litigation involves ex post harm-based remedies. Such remedies may work better than ex ante rules that specify required preventive measures if data subjects have good information about when a firm that collects their data experiences a breach and if costs of enforcing ex ante rules are high.[16] An ex post harm-based remedy is more desirable if the occurrence of a data breach, the likelihood of which depends on "unobservable efforts for information security," makes it possible to determine fault at lower cost.[17] Such a remedy may also work better if courts were to hold firms strictly liable for data breaches, as discussed below.

Litigation is usually brought by private individuals or firms in response to losses they experience because of their interaction with others. Data breaches often result in class-action lawsuits. These are based on "common law claims such as negligence, misrepresentation or breach of contract" or "private actions available under some state consumer protection statutes."[18] Data-breach lawsuits are typically brought by consumers, but banks that process credit card payments also file lawsuits against retailers for failing to adhere to the data-security

15. Park, "Why Information Security Law has been Ineffective," 132–45.
16. Steven Shavell, "The Optimal Structure of Law Enforcement," *Journal of Law and Economics* 36 (1993): 255–87.
17. Park, "Why Information Security Law has been Ineffective," 134.
18. Jeff Kosseff, *Cybersecurity Law* (Hoboken, NJ: John Wiley & Sons, 2017), 1.

standards of the payment-card industry.[19] Consumers' individual losses are usually too small relative to the cost of bringing a lawsuit unless the consumers can be represented jointly in a class-action case.

Target, which experienced a data breach in 2013, settled a class-action lawsuit in 2015, providing a fund of up to $10 million to compensate victims who experienced identity theft as a result of the breach.[20] In one other famous class-action case involving a data breach, *Remijas v. Neiman Marcus, LLC*, the plaintiffs lost the case: the judge threw out the settlement by decertifying the class action because of differences in the amount of compensation to be received by different members.[21]

Many data-breach victims have sought assistance from tort law.[22] Over the years, between 4 and 6 percent of publicly reported data breaches have resulted in class-action litigation.[23] Plaintiffs' attorneys file multiple lawsuits against companies that experience "the largest and most publicized breaches" but bypass the majority of companies reporting data breaches.[24] The most common primary theory under which plaintiffs have sought recovery is negligence.[25] According to Judge Learned Hand, an actor should be considered negligent for a mishap that occurs if the "marginal burden of an untaken precaution is less than the reduction in the expected loss" that would have resulted from taking the precaution.[26]

In court cases, a plaintiff must have standing in order to win a lawsuit or incentivize settlement for the defendant. For standing to exist, the plaintiff must suffer an injury-in-fact that is sufficient.[27] There are three kinds of injuries from data breaches: (a) the cost of fraudulent transactions or identity theft, (b) increased risk of future identity theft or fraud, and (c) the burden of closing or monitoring affected accounts.[28]

Courts are less likely to grant standing when a data breach cannot be clearly shown to have resulted in fraudulent transactions or identity theft. The Supreme

19. Kosseff, *Cybersecurity Law*.
20. "Target Settlement May Strengthen Bank's Case," *Northwestern Financial Review*, May 2015. https://bankbeat.biz/target-s-settles-consumer-data-breach-suit-strengthens-banks-case/.
21. Lior Strahilevitz, "Data Security's Unjust Enrichment Theory," *University of Chicago Law Review* 87 (2020): 2477–92.
22. Filler et al., "Negligence at the Breach."
23. Jean Valdetero, David Zetoony, and Andrea Maciejewski, "Data Breach Litigation Report," 2019 ed., Bryan Cave Leighton Paisner LLP.
24. Valdetero et al., "Data Breach," 2.
25. Valdetero et al., "Data Breach."
26. Cooper and Kobayashi, "Unreasonable," 280, footnote 90.
27. J. Thomas Richie, "Data Breach Class Actions," *The Brief* (Chicago) 44 (Spring 2015): 12, 14–19.
28. Richie, "Data Breach Class Actions."

Court has not decided any data-breach cases but has decided two recent privacy-related cases, *Spokeo v. Robbins* and *Clapper v. Amnesty International USA*, in which it was unwilling to allow plaintiffs to establish standing on the basis of the risk of a future, intangible injury.[29] Following a similar approach, several circuit courts as well as district courts within some circuits have made it more difficult for plaintiffs to establish injury-in-fact.[30] These courts hold that a data breach, by itself, is insufficient proof of injury-in-fact, reasoning that standing requires harm that is more certain than "the mere possibility of identity theft."[31]

The Sixth, Seventh, Ninth, and DC Circuit Courts of Appeals have been more inclined than courts in other circuits to grant standing on the basis of increased risk of future harm and the cost of mitigating the risk of future identity theft.[32] Although some states have required firms to provide free credit monitoring to data-breach victims, in several breach cases the alleged injury was "from the financial loss suffered because plaintiffs must pay for credit monitoring and other fraud prevention services."[33] The Seventh Circuit granted standing in *Remijas* because of the increased risk of harm from identity theft and because of the cost of consumers' mitigation strategies.[34]

The fact that the circuits are split on the question of the circumstances under which to grant standing in data-security cases opens the door for a possible Supreme Court case in the future. The Supreme Court in its *Spokeo* and *Clapper* decisions did not completely rule out "the possibility of allowing" lawsuits based on the risk of a future intangible injury to proceed.[35] The court may be willing to grant standing if the plaintiffs bringing the lawsuit suffer harm in a "direct and meaningful way."[36]

Even after surviving challenges to standing, many cases are dismissed because "the plaintiff has not alleged an injury sufficient to satisfy the damages requirement of a tort claim."[37] Where courts grant standing to the plaintiff, they will not necessarily grant class certification, which is necessary for the case to

29. Kosseff, *Cybersecurity Law*.
30. Patrick Lorio, "Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution," *Columbia Journal of Law and Social Problems* 51 (2017): 79–128.
31. Kosseff, *Cybersecurity Law*, 81.
32. Devin Urness, "The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution," *Vanderbilt Law Review* 73, no. 5 (2020): 1517–60.
33. Patrick Lorio, "Access Denied," 91.
34. Strahilevitz, "Data Security's Unjust Enrichment Theory."
35. Kosseff, *Cybersecurity Law*, 77–78.
36. Maxwell L. Stearns, "Standing Back from the Forest: Justiciability and Social Choice," *California Law Review* 83, no. 6 (1995): 1413.
37. Richie, 15.

proceed. As in *Remijas*, some classes are not certified because of variance in the actual impact of a breach on different class members.[38] Several factors can prevent a class action from being certified, including (a) individualized issues that take predominance over common issues and (b) the inability to provide objective criteria for identifying class members.[39]

Another obstacle to plaintiffs' winning compensation for losses in data-breach cases is the *economic loss doctrine* (ELD). If the ELD applies to a claim, then the plaintiff will be denied compensation for that claim. The ELD applies in certain kinds of cases in which a plaintiff has suffered purely financial losses: (a) when the plaintiff and defendant are not in any consensual relationship or (b) when the plaintiff and defendant have a contractual relationship.[40] The first is referred to as the *stranger paradigm*, the second as the *contracting-parties paradigm*.

States apply the ELD in different ways, in some cases acknowledging certain kinds of exceptions when the doctrine does not apply.[41] The ELD reflects important policy goals. The application of the stranger paradigm when no legal relationship exists between the parties is intended to prevent unforeseeable and "potentially unlimited liability" from economic damages.[42] The contracting-parties paradigm is concerned with private ordering—it encourages parties to a contract to consider and "bargain over the economic losses that may arise from the contract" and respects the decisions of the parties about loss allocation.[43]

Critics of applying the ELD to data-breach litigation point out that firms' data-protection policies are usually contracts of adhesion, so that "inherent bargaining power imbalances" exist "between individual consumers and multinational corporations."[44] Data security is a complex issue and "outside the informed contracting capabilities of most customers."[45] Thus, contracts do not necessarily give adequate weight to the interests of consumers in protecting their data. Also,

38. Richie.
39. Richie.
40. Catherine Sharkey, "Can Data Breach Claims Survive the Economic Loss Rule?" *DePaul Law Review* 66, no. 2 (2017): 339–84.
41. Sharkey, "Can Data Breach Claims Survive?"
42. Nicolas N. LaBranche, "The Economic Loss Doctrine & Data Breach Litigation: Applying the 'Venerable Chestnut of Tort Law' in the Age of the Internet," *Boston College Law Review* 62, no. 5 (2021): 1681.
43. Vincent Johnson, "The Boundary-Line Function of the Economic Loss Rule," *Washington & Lee Law Review* 66 (2009): 548.
44. LaBranche, "The Economic Loss Doctrine," 1682.
45. Mark A. Geistfeld, "Protecting Confidential Information in Business Transactions: Data Breaches, Identity Theft, and Tort Liability," *DePaul Law Review* 66, no. 2 (2017): 389.

the ELD's concerns about unforeseeable economic damages are less applicable to data protection, because anyone who collects, processes, or stores consumers' personal information should be able to anticipate the possibility of data breaches and the accompanying consequences.

Tort law has thus far failed to provide incentives for firms to provide optimal levels of data security because of the reluctance of courts to grant standing to plaintiffs. This is due largely to uncertainty over causal links between data breaches and specific victims who suffer concrete harms, such as identity theft.[46] Courts have been reluctant to base their decisions in data-breach cases on the risk of harm "without any additional showing of imminent or actual harm."[47]

The Role of Regulatory Agencies

Most data-security legislation is enforced by regulatory agencies or state attorneys general. Regulatory agencies sometimes conduct audits of organizations' security practices but often do not punish them for failure to comply with existing rules or best practices. Most enforcement occurs only after a data breach has occurred.[48]

The FTC has taken responsibility for enforcement of statutes such as the Gramm–Leach–Bliley Act and for data security in sectors where legislation has not been enacted. It has done so as part of its responsibility to protect consumers from unfair and deceptive acts and practices (UDAP). According to one former FTC chairman, the core of consumer-protection policy, which is the responsibility of the FTC, "is to protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices."[49]

Early privacy and data-security cases were based on deceptive acts and practices—the failure of companies to do what they promised. When deception was central in early enforcement, the FTC encouraged self-regulation—"companies would create their own rules and the FTC would enforce them."[50]

46. Omri Ben-Shahar, "Data Pollution," *The Journal of Legal Analysis* 11, no. 24 (2019): 104–59.
47. Kosseff, *Cybersecurity Law*, 81.
48. Solove and Hartzog, *Breached!*, 53.
49. Timothy Muris, "The Federal Trade Commission and the Future Development of US Consumer Protection Policy," August 19, 2003.
50. Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014): 598.

Since then, "the Commission has aggressively sought to expand the scope of its authority under section 5 of the FTC Act."[51] This is exemplified by its use of its unfairness authority in data-security cases, which it could apply to any firm in the country that collects online data. Congress codified in 1994 that in order for a practice to be unfair, "the injury it causes must be (1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid."[52]

The FTC filed its first data-security complaint against BJ's Wholesale Club, which experienced a data breach in 2005. The complaint, which alleged unfair practices in data-security policy, was based on "BJ's failure to provide 'reasonable security' for its computer network" by, among other things, failing to employ various measures, such as encryption, to secure its information and limit access to its networks, and by storing data longer than necessary.[53]

The FTC has relied almost exclusively on case-by-case adjudication in dealing with data-security problems. The FTC generally takes action against firms that have experienced a data breach when one or more parties have gained unauthorized access to consumer data, such as Social Security or credit card numbers. In its data-security enforcement, the FTC requires firms to implement reasonable security practices: "[A] company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[54]

The FTC's policy toward data security has recently been subject to considerable criticism. Critics assert that by using "enforcement actions against individual companies, the FTC is creating 'a patchwork of data security standards' and 'businesses do not have fair notice of how the FTC will apply the standards to their own practices.' "[55] In two recent cases, *FTC v. Wyndham Worldwide Corporation* and *LabMD, Inc. v. FTC*, in which the defendants initially refused to settle with the FTC, a central question was "whether the FTC's past settlements form a common-law-like body of precedent sufficient to give firms fair notice" of its data-security standards.[56] Both administrative law and the due-process clause

51. Justin Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101, no. 3 (2016): 958.
52. J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," *Journal of Public Policy & Marketing* 22 (2003): 192.
53. Michael D. Scott, "The FTC, the Unfairness Doctrine and Data Security Breach Litigation: Has the Commission Gone too Far?" *Administrative Law Review* 60 (2008): 146.
54. "Protecting Consumer Information: Can Data Breaches Be Prevented?" (prepared statement of the Federal Trade Commission before the Committee on Energy and Commerce), February 5, 2014.
55. Filler et al., "Negligence at the Breach," 113.
56. Hurwitz, "Data Security," 958.

of the Fifth or Fourteenth Amendment "require adequate notice of laws and regulations before agency enforcement occurs."[57] Although the question of fair notice did not affect court decisions in either the *Wyndham* or *LabMD* case, the court did express concern about it as part of its *Wyndham* opinion.[58]

The vast majority of FTC data-security cases have settled. These settlements "provide a lot of information about what type of practices the FTC will consider unreasonable, but very little about what type of practices might *satisfy* a reasonableness standard."[59] FTC complaints and consent orders list data-security practices that "taken together" are considered unfair, but they do not provide sufficient information about what combination of practices are required to avoid liability.[60] Even if the FTC requires a firm to implement a certain practice with regard to one complaint, the FTC might not consider failure to follow that practice a violation in the next case.[61]

The requirement that firms implement reasonable security practices might be expected to mimic the application of a negligence standard under tort law.[62] Under a negligence standard, a firm is only liable for a breach if it fails to take cost-effective precautions. One problem with FTC's enforcement is that it is too quick to infer "unreasonable security practices from the fact of unauthorized disclosure" of data, without sufficient evidence of concrete harm or its likelihood.[63] "Proper economic analysis" can illuminate the distinction between harm that is "substantial" and that which is trivial or speculative, but "the FTC regularly falls short of meaningful analysis."[64]

Going forward, the prospect of FTC enforcement actions in the event of a breach will have limited incentive effects on firms. This is because, with only a few exceptions, the FTC—unlike plaintiffs in private lawsuits—is unable to secure monetary relief when it brings a case against a firm for the first time.[65] Until recently most courts interpreted the language of section 13(b) of the FTC

57. Gerald Stegmaier and Wendell Bartnick, "Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements," *George Mason Law Review* 20, no. 3 (2013): 678.
58. Hurwitz, "Data Security."
59. Cooper and Kobayashi, "Unreasonable," 268.
60. Timothy E. Deal, "Moving Beyond Reasonable: Clarifying the FTC's Use of its Unfairness Authority," *Fordham Law Review* 84 (2016): 2252.
61. Stegmaier and Bartnick, "Psychics, Russian Roulette, and Data Security."
62. Cooper and Kobayashi, "Unreasonable."
63. Geoffrey A. Manne and Kristian Stout, "When Reasonable Isn't: The FTC's Standard-less Data Security Standard," *Journal of Law, Economics & Policy* 15, no. 1 (2019): 118.
64. Manne and Stout, "When Reasonable Isn't," 107–8.
65. The only exception to this is that the FTC can obtain monetary relief after issuing a cease-and-desist order for engaging in an act or practice "which a reasonable man would have known under the circumstances was dishonest or fraudulent." See 15 U.S.C. § 57b(a)(2).

Act to authorize district courts to award monetary restitution to consumers in a variety of cases.[66] But in 2021, the Supreme Court ruled in *AMG Capital Management, LLC v. FTC* that section 13(b) does not authorize the FTC to seek equitable monetary relief in its enforcement actions.[67] This limits the FTC's ability to seek monetary penalties except under very limited circumstances, such as "when companies violate cease-and-desist orders, consent orders or rules issued under Section 18(a)(1)(B) that define particular types of acts or practices as unfair or deceptive."[68] When state attorneys general bring a data-breach case, they can seek civil penalties under UDAP and other state statutes.[69]

As proponents of expanding the power of the FTC, Solove and Hartzog argue that the FTC's case-by-case approach to data protection operates like the common law and has yielded a coherent body of precedent that can form the basis for an expanded role of the FTC.[70] One way it works like the common law is that formal adjudication is "binding on the agency that employs the process; subsequent decisions in similar cases cannot without explanation contradict previous orders."[71]

Hurwitz argues that there are "fundamental differences between what the FTC is doing and the judicial common-law approach" which "call into question the basic jurisprudential legitimacy" of its approach.[72] In particular, the FTC is not an independent adjudicator responding to disputes between other parties but is a party to the enforcement actions it brings, choosing cases that are "likely to advance its policy goals."[73] By contrast, judges in common-law courts do not choose which cases to hear; instead, they hear those cases for which existing rules (such as criteria for assigning liability) are inefficient, because such rules impose higher costs on each party and are thus more likely to be litigated rather

66. Federal Trade Commission, "The Urgent Need to Fix Section 13(b) of the FTC Act," Comm. on Energy and Commerce, Subcomm. on Consumer Protection, US House of Representatives (April 27, 2021).
67. *AMG Capital Management, LLC v. Federal Trade Commission*, No. 19-508 (April 22, 2021)
68. Chris Linebaugh, "*AMG Capital Management v. FTC*: Supreme Court Holds FTC Cannot Obtain Monetary Relief in Section 13(b) Suits," *Congressional Research Service Legal Sidebar*, Report No. LSB10596 (April 30, 2021).
69. States have obtained civil penalties as large as $9 million. See Danielle K. Citron, "The Privacy Policymaking of State Attorneys General," *Notre Dame Law Review* 92, no. 2 (2016): 747–816.
70. Solove and Hartzog, "The FTC and the New Common Law," 583–676.
71. Stephen P. Croley, "Theories of Regulation: Incorporating the Administrative Process," *Columbia Law Review* 98, no. 1 (1998): 115.
72. Hurwitz, "Data Security," 967.
73. Hurwitz, "Data Security," 984.

than settled out of court.[74] The behavior of litigants guides the evolution of the common law.[75]

The principle of stare decisis enhances the rationality of court decisions so that the common law evolves in a more stable manner.[76] By contrast, the FTC's approach has the potential to result in policy that is inconsistent over time and that reflects the priorities of the political party that appoints the chair.[77]

FTC Rulemaking

Although the FTC has relied on adjudication to deal with data-security issues in the past, it has the option of rulemaking. Rulemaking has several advantages over adjudication: it "can better deter unlawful abuses, provide greater clarity for regulated parties, streamline enforcement proceedings and incorporate public input."[78] If an agency uses legislative rulemaking, it has the authority to pursue civil penalties and equitable remedies for rule violations, which, since the *AMG Capital Management* decision in 2021, is generally not the case with adjudication.[79]

The FTC has recently begun to focus more of its efforts on rulemaking using two kinds of rulemaking authority: legislative and nonlegislative.[80]

If the FTC promulgates legislative rules, those rules are legally binding on the agency and the public.[81] The Magnuson–Moss Warranty—Federal Trade Commission Improvements Act gives the commission authority to enact legislative rules "which define with specificity acts or practices which are unfair or

74. George L. Priest, "The Common Law Process and the Selection of Efficient Rules," *The Journal of Legal Studies* 6, no. 1 (1977): 65–82.
75. Paul H. Rubin, "Why is the Common Law Efficient?" *The Journal of Legal Studies* 6, no. 1 (1977): 51–63.
76. Maxwell L. Stearns, "Standing Back from the Forest: Justiciability and Social Choice," *California Law Review* 83 (December 1995): 1309–414.
77. This is becoming evident as a result of FTC actions under the Biden administration, which have deviated from the stable policies of the commission during three previous administrations. See Hurwitz, "Data Security," 987.
78. Kurt Walters, "Reassessing the Legacy of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC," *Harvard Law and Policy Review* 16 (2022): 524.
79. 15 USC § 47(m)(1)(A) and 57b(a)-(b), cited in Walters, "Reassessing the Legacy of Magnuson-Moss," 525.
80. Ian Davis, "Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads," *Emory Law Journal* 69, no. 4 (2020): 781–832.
81. National Petroleum Refiners Ass'n v. F.T.C., 482 F.2d 672, 678, 698 (D.C. Cir. 1973).

deceptive acts or practices in or affecting commerce."[82] The FTC can impose a civil penalty of $50,520 for each violation of a legislative rule.[83]

To engage in Magnuson–Moss rulemaking, the FTC is required to follow strict procedures, which include providing for a public notice and comment period as well as an informal hearing. This makes the section 5 rulemaking, which applies to UDAP, especially arduous, giving the FTC an incentive to rely on adjudication instead.[84] In some instances, Congress has directed the FTC to follow the rulemaking procedures set forth in the Administrative Procedures Act (APA). They have done this in promulgating regulations to enforce the Children's Online Privacy Protection Act (COPPA) and the Gramm–Leach–Bliley Act.[85] Both the APA and the Magnuson–Moss Act require giving notice to the public and soliciting public comments, but the Magnuson–Moss rulemaking process is more burdensome.

Although some have advocated for the FTC to pursue legislative rulemaking as it did in the 1970s, the drawbacks are substantial. Not only is the process burdensome, but it is not clear that in the past it was carried out in the way intended. The law states that FTC actions must be supported by "substantial evidence in the rulemaking record."[86] In practice, the FTC implemented most rules with very limited evidence and often lacked clear theories of why a particular practice should be illegal or why a proposed remedy would be likely to solve a problem.[87] The FTC approved a care-labeling rule and a funerals rule in spite of survey evidence that raised questions about the need.[88] And recently, FTC steps to simplify the legislative rulemaking process have been found to "fast-track

82."15 U.S. Code § 57a - Unfair or Deceptive Acts or Practice Rulemaking Proceedings," Legal Information Institute, Cornell Law School.
83. Federal Trade Commission, "FTC Publishes Inflation-adjusted Civil Penalty Amounts for 2023," press release, January 6, 2023.
84. Timothy E. Deal, "Moving Beyond "Reasonable": Clarifying the FTC's Use of its Unfairness Authority in Data Security Enforcement Actions," *Fordham Law Review* 84, no. 5 (2016): 1084, 2227–60.
85. J. William Binkley, "Fair Notice of Unfair Practices: Due Process in FTC Data Security," *Berkeley Technology Law Journal* 31 (2016): 1079–108.
86. 15 U.S.C. § 57a(e)(3)(A).
87. Muris discusses a number of FTC rules that were enacted during the 1970s, only one of which, the Eyeglass rule, was based on "a systematic effort to collect projectable evidence that tests a clear theory" (p. 25). See Timothy J. Muris, "Rules Without Reason: The Case of the FTC," *AEI Journal on Government and Society*, October 14, 1982, https://www.aei.org/articles/rules-without-reason-the-case-of-the-ftc/.
88. One problem is that the FTC conducts the surveys only after it has closed the rulemaking record and tentatively decided that a rule is necessary (Muris, "Rules Without Reason," 23).

regulation at the expense of public input, objectivity and a full evidentiary record."[89]

Nonlegislative rules have few, if any, of the disadvantages of legislative rules. Nonlegislative rules are "interpretive rules and general statements of policy with respect to unfair or deceptive practices."[90] Such rules are referred to as *guidance documents*, and unlike legislative rules, they are not unencumbered by "procedural constraints."[91] The FTC can solicit industry input as part of the rulemaking process.[92] Agencies have more flexibility if they choose to use nonlegislative rules to communicate policy to the public, but courts do not give nonlegislative rules the same kind of deference they give to legislative rules.[93]

The FTC has posted numerous documents that provide nonlegislative guidance to the public.[94] This guidance is used to convey information on standards that will be enforced by the FTC in UDAP cases. Firms take these documents seriously in making decisions about security practices.[95]

HOW TO ACHIEVE BETTER DATA SECURITY

Achieving better data security requires considering the incentives that affect each of the diverse participants in the data ecosystem. The firms that collect and process data are not the only participants who can take steps to reduce data breaches and associated data misappropriation. Consumers, employees, software developers, device manufacturers, app providers, advertising networks, internet service providers, and providers of cloud-based services are among those who may contribute in important ways to securing data and reducing breaches.

Because of the complexity of the data ecosystem, a firm that experiences a data breach may blame another participant in order to avoid being considered at fault. For example, the firm may argue that the software it was using was defective, or that a vendor hired to maintain its system did not do so correctly.[96] Those who acquire software do not sufficiently consider software bugs that contribute to data insecurity. Platforms might not be doing enough to ensure the apps they

89. Noah Joshua Phillips, Christine S. Wilson, "Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Commission Statement on the Adoption of Revised Section 18 Rulemaking Procedures," July 9, 2021.
90. 15 U.S.C. § 57a(a)(1)(A), cited in Davis, footnote 117.
91. Davis, "Resurrecting Magnuson-Moss Rulemaking," 798.
92. Deal, "Moving Beyond 'Reasonable.'"
93. Deal, "Moving Beyond 'Reasonable.'"
94. Federal Trade Commission, "Data Security," webpage, last accessed March 6, 2023.
95. Solove and Hartzog, "*Breached*!"
96. Justin Hurwitz, "Cyberensuring Security," *Connecticut Law Review* 49, no. 5 (2017): 1495–547.

distribute are secure. And the party whose data is less secure because of bugs or other vulnerabilities in the data ecosystem does not always have the option of forgoing a relationship with the entities whose choice of precautions contributed to the problem. For example, consumers cannot choose whether their personal data are collected and processed by a particular credit-reporting agency.

Self-regulation

Self-regulation plays an important role in promoting data security in some industries such as the payment-card industry, which has experienced a number of data breaches. The payment-card industry's standards for handling data are known as the *PCI DSS system*. These requirements are unregulated by government but are often part of contractual obligations and are adhered to by all entities that accept, process, store, or transmit cardholder data.[97] They were established by the PCI Security Standards Council and are regularly updated by that group, which serves the interests of payment-card brands such as American Express, Discover, MasterCard, and Visa.

The PCI DSS system seeks to accomplish six goals, with 12 high-level standards and over 200 line-item requirements.[98] The goals are as follows:[99]

- Strengthen network security
- Protect cardholder data
- Manage vulnerability
- Maintain access control
- Monitor and test networks
- Maintain information security

Individual payment-card brands enforce the standards primarily with noncompliance fines to the acquiring bank, which processes card payments to the merchant or contracts with other payment processors or service providers.[100] The acquiring bank in turn passes fines along to any noncomplying merchant or service provider. The only states that require compliance with PCI DSS standards are Nevada and Washington, and their laws also specify that compliant

97. Donna Wilson, Ethan Roman, and Ingrid Beierly, "PCI DSS and Card Brands: Standards, Compliance, and Enforcement," *Cyber Security* 2, no. 1 (2018): 73–82.
98. Wilson et al., "PCI DSS and Card Brands."
99. Andrew Gorecki, *Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk* (Hoboken, NJ: John Wiley & Sons, 2020).
100. Wilson et al., "PCI DSS and Card Brands."

firms are shielded from liability for data breaches.[101] Minnesota law requires a company that suffers a data breach and is "found to have been storing prohibited card data on its system" in violation of PCI DSS standards to reimburse financial institutions for the cost of blocking and replacing cards.[102]

Some merchants have been critical of PCI DSS standards for being expensive, confusing, and subjective in interpretation and enforcement.[103] But enforcing the standards forces all parties involved to be more careful about securing the data they collect, store, and process.

One possible approach to improving data security in sectors where no legislation applies—including tech platforms and other nonfinancial firms outside of health care—could involve self-regulation, which would not require that all firms implement the same kind of security practices. Instead, the FTC could require firms to provide consumers with affirmative assurances about how their data will be handled.[104] They could consider any firm that collects data without having a public data-security policy to be engaging in unfair practices and subject to FTC sanction.[105] Firms that fail to abide by policies they have established could be sanctioned for deceptive practices.[106]

The Role of Courts vs. Regulatory Agencies

An important question is whether to increase or reduce the role of public enforcement of data security by regulatory agencies and state attorneys general or to rely more on private enforcement through the court system. Both courts and regulatory agencies rely on adjudication to develop principles governing information security. Theory and anecdotal evidence suggest some advantages to greater reliance on courts than on regulatory agencies, particularly the FTC, to develop a common set of principles to govern information security. The common law develops as judges in appellate courts make decisions in response to conflicts between legal principles.[107] Courts take and decide whatever cases come to them, whereas the FTC can avoid close cases. Critics say the FTC does not necessarily give firms a fair hearing in adjudication because it acts as both prosecutor and

101. Nev. Rev. Stat. § 603A.215 (2009); Wash. Rev. Code § 19.255.020, cited in Wilson et al., footnote 15.
102. Wilson et al., "PCI DSS and Card Brands," 79.
103. Wilson et al., "PCI DSS and Card Brands."
104. Hurwitz, "Data Security."
105. Hurwitz, "Data Security."
106. Hurwitz, "Data Security."
107. Hurwitz, "Data Security."

judge.[108] Firms subject to FTC action do have a right to appeal, but successful appeals have become less common in recent years as the FTC has dismissed fewer cases.[109] Rather than reflecting growing bias against the firms it investigates, the FTC's failure to dismiss cases it has brought in recent years could be the result of improvements in the FTC's ability to select cases it is likely to win in court. But if the FTC avoids bringing enforcement actions against firms in close cases, then some who may have been harmed are disadvantaged.

Other concerns in comparing courts and regulatory agencies include the quality and consistency of decisions and whether regulation or litigation give firms too little or too much incentive to implement precautions to secure data.

Critics have noted that those appointed as FTC commissioners have not had the diverse qualifications or expertise that Congress intended when it created the agency.[110] Few economists or people with substantial business-management experience have been appointed as commissioners. One empirical study on the quality of judicial decisions versus agency decisions in antitrust cases has suggested that courts make better decisions than agencies even when agencies possess more disciplinary expertise.[111] Even if an agency provides more expert input than courts do, the quality of the decisions it makes depends on the institutions and processes that translate inputs to outputs.[112]

Centralized public enforcement of data security may enjoy economies of scale that result in lower costs than private enforcement through courts.[113] However, private enforcers may have lower costs than government agencies because of greater organizational dexterity or because of access to individuals with inside information about misconduct—misconduct that contributes to data breaches.[114]

---

108. Malcolm B. Coate and Andrew N. Kleit, "Does it Matter that the Prosecutor is also the Judge? The Administrative Complaint Process at the Federal Trade Commission," *Managerial and Decision Economics* 19, no. 1 (1998): 1–11.
109. Maureen K. Ohlhausen, "Administrative Litigation at the FTC: Effective Tool for Developing the Law of Rubber Stamp?" *Journal of Competition Law & Economics* (2016): 1–37.
110. William E. Kovacic, "The Quality of Appointments and the Capability of the Federal Trade Commission," *Administrative Law Review* 49, no. 4 (1997): 915–61.
111. A higher quality decision is one that is less likely to be appealed or to be reversed on appeal. See Joshua Wright and Angela Dively, "Do Expert Agencies Outperform Generalist Judges? Some Preliminary Evidence from the Federal Trade Commission," in *The Regulatory Revolution at the FTC: A Thirty-Year Perspective on Competition and Consumer Protection*, ed. James C. Cooper (Oxford, England: Oxford University Press, 2013), 40–60.
112. Wright and Dively, "Do Expert Agencies Outperform Generalist Judges?"
113. David Freeman Engstrom, "Agencies as Litigation Gatekeepers," *Yale Law Journal* 123, no. 3 (December 2013): 616–712.
114. Engstrom, "Agencies as Litigation Gatekeepers."

Ideally, regulatory agencies would compare the benefits to the costs in deciding whether to bring a case against a firm for lax data security. Agencies, however, may be susceptible to political incentives that might not be consistent with estimating and comparing benefits to costs.[115] Although private parties pursuing litigation compare benefits to costs, outcomes involve substantial external costs and benefits. Litigating parties might not account for the costs to the opposing party or third parties such as taxpayers, but they also might not account for how court decisions and settlements influence the incentive of firms to take precautions to secure the data they collect and process.[116]

Further, an agency such as the FTC may often enforce the law unevenly. As a result, "it does not meaningfully inform or educate anyone about good security practices."[117] Agency decisions may not be consistent over time because of changes in the political party that controls the presidency.

One problem with litigation is the unwillingness of courts to grant standing. Besides upholding a high standard for establishing injury-in-fact, the Supreme Court refused to grant standing and overrode the judgment of Congress about what constitutes cognizable harm in *Transunion v. Ramirez* and *Spokeo*.[118] It is possible that as the problem of data breaches grows, the Supreme Court could affirm a more liberal approach to granting standing in data-breach cases. However, if federal courts are unwilling to grant standing, plaintiffs have the option of filing suit in state courts.[119]

To the extent that there is a problem with underdeterrence, the FTC and other regulators may choose high-profile targets to make examples of them—to showcase the consequences of lax data-security practices.[120] But the FTC's inability to secure monetary relief and the hesitancy of Congress to grant additional power to the FTC add up to another reason why the litigation option is important, even if the FTC continues to play a significant role.

---

115. For a classic study applied to the FTC, see Barry R. Weingast and Mark J. Moran, "Bureaucratic Discretion or Congressional Control? Regulatory Policymaking at the Federal Trade Commission," *Journal of Political Economy* 91, no. 5 (1983): 765–800.

116. Steven Shavell, "The Fundamental Divergence Between the Private and the Social Motive to Use the Legal System," *The Journal of Legal Studies*, 26, no. S2 (1997): 575–612.

117. Hurwitz, "Cyberensuring Security," 1520.

118. Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," *Boston University Law Review* 102 (2022), 793–863.

119. "Article III – Standing – Separation of Powers – Class Actions = *TransUnion LLC v. Ramirez*," *Harvard Law Review* 135 (2021): 333–42.

120. I am grateful to an anonymous reviewer for suggesting this advantage of regulation.

How Legislation Can Enhance Litigation and Regulation

The existing combination of regulation and litigation has not worked well in promoting an optimal level of data security. The difficulty of obtaining standing means that those whose data are compromised in breaches have often not been compensated for their losses. FTC regulation, with its emphasis on reasonable data-security practices, has also fallen short, as discussed above.

Part of the problem with both litigation and FTC regulation is the difficulty of applying a negligence standard to data-breach cases. The big problem with a negligence standard is how to determine whether the data controller adopted reasonable data-security precautions. There are many different ways a firm or its employees could be negligent, and it is difficult to identify what the firm did or failed to do that caused a breach and whether doing something different would have reduced the risk of a breach in a cost-effective way. The complex problem of determining whether a firm was negligent partly explains why courts apply a strict liability standard for harm caused by defective manufactured products.[121] Thus, some experts argue for a strict liability standard to be applied to data-security problems, particularly data breaches.[122]

With a strict liability standard, each firm that experiences a data breach would be required to pay for the harm to consumers regardless of the level of care the firm took.[123] A strict liability standard has several advantages over a negligence standard: It would eliminate the difficult and costly exercise of determining negligence—that is, whether firms have taken all cost-effective measures to secure the data they collect and store. Because firms would be fined in proportion to the expected losses caused by a data breach, this approach would also give firms an incentive to collect less personal information.[124] If liability is assessed accurately, firms will compare the expected risk of harm to consumers from collecting or storing additional data with the marginal benefits of doing so. It would give firms an incentive to find the most cost-effective way to secure clients' data; it would also give them an incentive to purchase cyberinsurance to cover the residual risk of harm after they choose the level of precaution to take. Firms that collect and store data can likely estimate more accurately the probability of a

121. Mark A. Geistfeld, "Protecting Confidential Information in Business Transactions: Data Breaches, Identity Theft, and Tort Liability," *DePaul Law Review* 66, no. 2 (2017), 385–412.
122. See Danielle K. Citron, "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age," *Southern California Law Review* 80 (2007): 241–98; Peter Ormerod, "A Private Enforcement Remedy for Information Misuse," *Boston College Law Review* 60 (2019): 1893–948; Cooper and Kobayashi, "Unreasonable"; and Hurwitz, "Cyberensuring Security."
123. Cooper and Kobayashi, "Unreasonable," 263.
124. Cooper and Kobayashi, "Unreasonable," 273.

breach, given the preventive measures they have taken, than can data subjects or courts.[125] As long as firms can make a reasonably accurate estimate of the loss to data subjects, they may be better able to choose a close to optimal level of precautions.

Firms will determine the level of precautions to take on the basis of what they expect courts to do. Even if courts make systematic errors, firms are likely to err less in choosing the optimal level of precautions under a strict liability standard than under a negligence standard.[126] This is because a negligence rule sets up a discontinuity—if the firm satisfies the standard, it will not be liable no matter how much harm results. So if liability is determined on the basis of negligence, and if the standard that firms expect courts to enforce is too high relative to the optimal standard, this will lead to an error in precautions that is proportional to the error in the standard. If the standard is strict liability, the increase in precautions firms will take in response to an overestimate of expected harm will be limited by the declining marginal effect of additional precautions on expected harm.[127]

Whether strict liability could lead to more optimal precautions to limit data breaches depends on the extent to which firms and their employees, rather than consumers, can implement cost-effective ways to enhance data security.[128] Strict liability requires data controllers to bear a greater share of the risk from data breaches. Data subjects would be charged more for goods and services in exchange for incurring less of the risk. Strict liability helps to spread the cost of data breaches among all those whose personal information is collected commercially and over time, which is likely to be less burdensome than having a few people bear large losses over a short time period.[129] It would likely also hasten the growth of the market for third-party cyberinsurance.

Insurance markets do not work well if moral hazard problems are too serious. Moral hazard has to do with the effect insurance coverage would have on the

---

125. Consumers tend to "underassess the accident costs associated with defective products and services, leading to overconsumption" of risky products and services" (p. 1040). See James A. Henderson Jr., "Extending the Boundaries of Strict Products Liability*:* Implications of the Theory of the Second Best," *University of Pennsylvania Law Review* 128 (May 1980): 1036–93.

126. Cooper and Kobayashi, "Unreasonable," 290.

127. There is an upper limit to how much consumers will spend on a negligence standard, but the comparison is valid within a reasonable range. For more details, see Cooper and Kobayashi, "Unreasonable," 282–89.

128. For consumer facing firms, it is possible that the expected reputational costs of data breaches would lead firms to take optimal precautions in the absence of strict liability.

129. The basic principles involved are discussed in Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis* (New Haven, CT: Yale University Press, 1970), 39–45.

precautions taken by data subjects or by firms that collect data. Because of the complexity of data ecosystems and the inability of data subjects to understand risks or consequences of the precautions they take, it is not likely that increased firm liability would have much effect on data subjects' behavior. Insurance companies could also limit moral hazard of firms and their employees by monitoring precautions firms take.

If strict liability contributes to the growth of cyberinsurance and, as a result, insurance providers gain expertise in cost-effective ways to reduce the risk of data breaches, an increased role for insurance providers could reduce the combined costs of data breaches and measures taken to prevent them. Insurance providers could offer firms lower premiums in exchange for implementing precautions they recommend that reduce risk of data breaches. One study of cyberinsurance practices argues that "insurance institutions . . . are actively managing the underlying risk of data breach."[130] Strict liability improves the ability of cyberinsurers "to function as *de facto* regulators."[131]

Given the important role Congress plays in data security, some argue that Congress should pass legislation empowering the FTC to enforce a strict liability standard.[132] But as noted above, the personnel and process involved when the FTC decides cases may lead to lower-quality decisions than those reached through litigation. And it is doubtful whether Congress would be willing to grant the FTC the additional authority or the funding necessary to enforce a strict liability standard. The FTC cannot be counted on to be impartial in deciding cases when it is acting as both enforcer and adjudicator.

Although the courts could arguably do a better job than the FTC of enforcing a strict liability standard impartially, the unwillingness of the federal courts to grant standing to plaintiffs in many data-breach cases raises doubts about the efficacy of relying on the courts to enforce data security. But in addition to the willingness of some circuit courts to grant standing even in cases of uncertainty about harm, there is reason to hope that the Supreme Court may be more liberal in granting standing when it eventually hears a data-security case.[133] If the federal

130. Shauhin A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Law & Social Inquiry* 43, no. 2 (2018): 428.
131. Cooper and Kobayashi, "Unreasonable," 292.
132. Cooper and Kobayashi, "Unreasonable."
133. Although it may appear that courts are using standing to achieve certain case outcomes or override the intent of the Congress in legislation it has passed, Stearns makes a convincing case that the reason courts deny standing is to limit the ability of interest groups "to seize control of the order of case presentation to affect the substantive evolution of the law." This is done by choosing cases on the basis of facts that are beyond the litigant's control. See Stearns, "Standing Back from the Forest: Justiciability and Social Choice," 1412–13.

courts are not doing enough to uphold data security, there is the option of relying on the state courts.

Ormerod makes a convincing case for state laws imposing a fiduciary duty on entities that collect and use information about users.[134] He also argues that breach of this duty should be a strict liability tort with an enforcement remedy that begins with a schedule of "nominal damages and attorney's fees" plus higher penalties for more culpable defendants.[135] If the defendant does not disclose the breach in a timely manner or is responsible for willfully contributing to it, then punitive damages will be due.[136]

If Congress or state legislatures do impose strict liability, it should be limited to firms that are custodians of consumer data, including data brokers and credit-reporting agencies.[137] Strict liability could be understood as connected to a fiduciary duty that applies to firms that collect, store, or process personal data. An information fiduciary would have a duty of loyalty and trustworthiness toward its clients, similar to the fiduciary responsibilities of doctors, accountants, and lawyers.[138] Although any data breach would be costly if a firm is liable, it makes sense to limit the liability of firms who make some effort to secure data and warn consumers when their data may have been stolen. As long as firms do not violate the law by failing to disclose a breach in a timely manner and do not willfully contribute to that breach, they should not be subject to punitive damages.

Short of major legislation imposing strict liability, other legislative strategies could contribute to enhancing data security. Congress could increase the willingness of courts to confer standing by enacting a statute that requires companies to reimburse those whose data are compromised for the costs to safeguard their data.[139] Arguably, such a statute would result in courts being more willing to confer standing, because in the statute Congress is defining a new injury.[140]

---

134. Ormerod, "A Private Enforcement Remedy."
135. Ormerod, "A Private Enforcement Remedy," 1917–18.
136. Ormerod, "A Private Enforcement Remedy."
137. Cooper and Kobayashi argue for the importance of including firms that store and process consumer data and are not consumer-facing; they argue for excluding firms that are not custodians of data but whose products or role may contribute to data misuse. Thus, retailers who accept credit cards would not be strictly liable for stolen card information.
138. Jack M. Balkin, "Information Fiduciaries and the First Amendment," *UC Davis Law Review* 49, no. 4 (2016): 1185–234.
139. See Lorio, "Access Denied," 118–19, for a description of an example of a proposed statute.
140. In a Supreme Court decision, Justice Kennedy noted, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before ..." See *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 580 (1992).

There is room for a continuing role for the FTC in regulating data security through adjudication. FTC action could be more effective if Congress passed legislation explicitly granting the agency the authority to obtain equitable monetary relief under section 13(b).[141] Without this authority, the FTC may be able to coordinate with state attorneys general to leverage state consumer-protection laws to obtain restitution, but this would be difficult and would work better in some states than others.[142]

CONCLUSION

Consumers, the courts, the FTC, and state attorneys general all play a role in penalizing firms for data breaches, thereby giving them few incentives to take precautions. The FTC has had a limited role in deterring data breaches because in most cases it is not permitted to collect damages that could be used to compensate victims. Courts, given their frequent unwillingness to grant standing to plaintiffs in data-breach class actions, also have not done enough to deter data breaches.

Because data breaches have much in common with accidents from the use of industrial products, and because consumers cannot do much to protect themselves against the risk of a breach, Congress should consider imposing strict liability for data breaches on firms that are custodians of consumer data. Since federal courts have been hesitant to grant standing to those whose data are exposed in a breach, an alternative approach would be for state legislatures to impose a fiduciary duty on data controllers that can be enforced by state courts.

If neither Congress nor state legislatures impose a strict liability standard, then a second-best approach is for the FTC to continue to enforce a reasonableness standard, providing guidance through nonlegislative rules to clarify how it applies the standard and to seek the assistance of state attorneys general, with courts stepping in when the losses are large enough and widespread enough to justify a class action. This will work better if more and more courts eventually grant standing to plaintiffs for harms that result from a breach if there is a reasonable probability that as a consequence, victims will experience identity theft or financial fraud.

---

141. FTC (2021).

142. In some states, the attorney general may only be authorized to collect civil penalties, and the value of penalties that may be collected is limited in some states. See Larissa Bergin, "AMG v. FTC: What's Next for Equitable Monetary Relief," *Journal of Health Care Compliance* 23 (May–June 2021): 13–20.

ABOUT THE AUTHOR

Tracy Miller is a senior research editor at the Mercatus Center at George Mason University. He has published articles on privacy policy, antitrust policy, transportation policy, environmental policy, and agricultural policy. He holds a PhD in economics from the University of Chicago, an MS degree in agricultural economics from Michigan State University, and a BS in forestry from Virginia Polytechnic Institute and State University.

ACKNOWLEDGMENTS

The author thanks Alden Abbott, Patrick McLaughlin, and anonymous referees for thoughtful feedback.

ABOUT THE MERCATUS CENTER AT GEORGE MASON UNIVERSITY

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, the Mercatus Center advances knowledge about how markets work to improve people's lives by training students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper, and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington and Fairfax campuses.