2022

Understanding American Privacy

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

Andrew B. Serwin

Tyler Blake

Understanding American Privacy

Neil Richards[1]

Andrew Serwin[2]

Tyler Blake[3]

Draft, Sept. 2018

It is frequently suggested, particularly by European observers, that the United States lacks much in the way of privacy law. Some American consumers, lawyers, and academics also lament that their personal information receives little protection in the law once it is collected and placed "out there." Foreign regulators and lawyers trained in European notions of data protection may also look at the American system and see an absence of an overarching generally-applicable data protection statute and conclude that American privacy law is either nonexistent or woefully inadequate.

The lack of a European-style data protection law in the United States is not be the end of the analysis. American privacy law is not perfect, but U.S. privacy law exists, it provides substantial regulatory effect, and it is surprisingly complex,

1 Thomas & Karole Green Professor of Law, Washington University in St. Louis.
2 Partner, Morrison Foerster.
3 Associate, HoganLovells.

particularly once the full ramifications of state-level laws are considered. American privacy law is not as easy to appreciate as other bodies of law that have, for example, a general statute that is interpreted by a thick body of cases, and understanding American privacy law therefore must require a wider lens. That does not mean that American privacy law is not real, or that it is insignificant. In fact, in some areas, American law is both denser and more regulatory than its European counterpart, and in some ways state law has driven global privacy laws, such as in the area of data breach laws. The United States also has an active and aggressive plaintiffs' bar, and a number of state and federal privacy regulators who are also quite willing to bring enforcement actions. In many ways, companies in the United States face more regulatory oversight because of the multiple layers of laws and the numerous regulators they must be concerned with.

This article offers a basic roadmap to American privacy law for the uninitiated. Because of the nuances of American privacy law, including the substantial state privacy and security laws, our roadmap is not top-down, but thematic. In order to understand American privacy, we believe that it is important to understand five of its guiding principles. First, American privacy law is *bifurcated* into two discrete regulatory regimes – one covering the government and the other covering the private sector of individuals, corporations, and other institutions. Second, American privacy law takes a *sectoral* or *sectorized* approach, meaning that rather than having a federal omnibus privacy or data protection law,

U.S. law regulates particular sectors of human activity in a way that is both piecemeal and more specific where it applies. Third, it is impossible to understand American privacy without taking account of the role of the *Federal Trade Commission*, a consumer protection regulator that is more than a century old, and which functions something like a data protection authority with a limited but general authority over trade practices that are unfair or deceptive. Fourth, American privacy law is *federalized*: both the national government and the fifty state governments have passed privacy laws. In this regime, national ("federal") law is supreme where it applies, but the state privacy laws remain very important, particularly those of California which has been an aggressive privacy regulator. Fifth, and finally, questions of *privacy harm* run throughout American privacy law, both as a threshold question required for private litigants to sue, again at the level of damages, as well as in the class certification process for private enforcement in the United States.

Once these five principles are appreciated, the body of American privacy law – its system of protections for personal information, as well as the numerous enforcement avenues that exist, – become much easier to appreciate, and American privacy law becomes much more comprehensible.

I. BIFURCATION

Privacy law in the United States is schematically very different from privacy law in Europe. American privacy and security law is bifurcated into two separate, distinct regulatory schemes; one covering the government and the other covering the private sector. While some laws cross over, affecting both the government and the private sector,[4] most laws address one or the other. While this chapter will focus primarily on regulation in the commercial sphere, it is important to understand that American privacy laws constrain the government as well.

Before one can understand what American privacy law is, one must first understand what privacy is, particularly in the legal or regulatory context. Privacy is a societal norm, often expressed in law,[5] that reflects a society's concern over the collection, protection, processing, and deletion of data regarding an individual. It is not concerned with other forms of data, such as that about an entity, and it does not focus on the activities of third-parties who should not have the data, such as identity thieves, but rather on what a person or entity that is authorized to have an individual's data does with it.

Modern American privacy law has often reflected the influence of three different sources of law: the Fair Information Practices, the U.S, Constitiution, and federal statutory law. In 1973, the Department of Health, Education, and Welfare (the

---

[4] E.g., the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2501 et seq., which regulates wiretapping and access to electronic communications by both government and private actors.

[5] The most famous early expression of this concept is, of course, the famous Warren and Brandeis Article, Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890). It was not the first discussion of privacy rights in American law, which has protected privacy rights (though often in other names and guises) for much longer. See Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L. J. 123 (2007).

precursor agency to the modern Department of Health and Human Services) released a report, titled *Records Computers and the Rights of Citizens*, looking at electronic recordkeeping and data storage practices in the United States.[6] The HEW Report proposed that the federal government enact a "Code of Fair Information Practice," centered on five basic principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose to be used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[7]

These principles, collectively referred to as the Fair Information Practices (or "FIPs"), are reflected in many of the sectoral laws that govern American privacy and

---

6 *Records Computers and the Rights of Citizens*, Department of Health, Education, and Welfare (July 1973).

7 *Id.*

security law.[8] The FIPs are fundamentally based on the concept of "notice and choice," or the idea that fair information collection and use should provide the consumer with notice about what information is being collected and a choice about whether to agree to the collection or not. However, this principle has been subject to wide-ranging criticism by scholars writing in American privacy law.[9]

The FIPs form the basis of the Privacy Act of 1974, which regulates the collection, use, dissemination, and destruction of personal information held by federal government agencies.[10] The Act was passed in response to rising concerns about the federal government's surveillance and collection of personal data on private citizens, and it was broadly aimed to give citizens the right to access and correct personal information held about them and to restrict the ability of the federal agencies holding these records to disseminate that information.[11]

Other statutes that constrain the U.S. government include the Freedom of Information Act ("FOIA")[12] and the Foreign Intelligence Surveillance Act ("FISA").[13] FOIA permitted individual citizens to request information from various government agencies, and required agencies to post certain frequently-requested information

---

8 Daniel J. Solove & Paul M. Schwartz, CONSUMER PRIVACY AND DATA PROTECTION (2015), 19-20.

9 E.g., Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STANFORD TECHNOLOGY LAW REVIEW 431 (2016); Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J. L. POL'Y INFO. SOC'Y 543 (2009); Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1879 (2013); Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. 583 (2014); JULIA ANGWIN, DRAGNET NATION (2014).

10 *Overview of the Privacy Act of 1974: Introduction*, United States Department of Justice, https://www.justice.gov/opcl/introduction.

11 *Overview of the Privacy Act of 1974: Policy Objectives*, United States Department of Justice, https://www.justice.gov/opcl/policy-objectives.

12 5 U.S.C. § 552.

13 50 U.S.C. § 1801 *et seq*.

publicly.[14] FISA is most notable for creating the Foreign Intelligence Surveillance Court ("FISC"), a secret court which is empowered to authorize surveillance on U.S. persons who are deemed to be operating as "agents of a foreign power" as long as foreign intelligence gathering is a "significant purpose" of the investigation.[15]

The United States Constitution also plays a significant role in shaping how the government can act with respect to privacy issues for United States citizens and "persons," primarily based on the First and Fourth Amendments. The Fourth Amendment, which protects citizens against unreasonable searches and seizures by law enforcement, has been the primary driver of privacy rights in the criminal law sphere. The landmark Supreme Court case *Katz v. United States* established the modern touchstone for Fourth Amendment application in criminal law - the defendant's "reasonable expectation of privacy."[16] In the modern context, the Court has interpreted the Fourth Amendment to prohibit the warrantless use of GPS tracking devices on automobiles[17] and the search of data on a cell phone incident to a lawful arrest.[18] The First Amendment, in particular the freedom of association clause, has also seen use as a source by the Supreme Court for enforcing the privacy rights of citizens against the government.[19]

---

14 *What is FOIA?*, UNITED STATES DEPARTMENT OF JUSTICE, https://www.foia.gov/about.html.

15 50 U.S.C. § 1804.

16 389 U.S. 347 (1967).

17 *Jones v. United States*, 565 U.S. 400 (2012).

18 *Riley v. California*, 134 S. Ct. 2473 (2014).

19 *See National Association for the Advancement of Colored People v. State of Alabama*, 357 U.S. 449 (1958) ("*NAACP*"). In *NAACP*, the Court held that a state cannot compel an association to disclose its membership list to the state absent a substantial showing of need by the state. For an explanation of the relationship between the First Amendment and privacy, see generally NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).

Two important statutes that apply to both the government and the private sector are the Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act ("CFAA"). ECPA itself is divided into three substantive parts - the Wiretap Act,[20] the Stored Communications Act ("SCA"),[21] and the Pen Register Act.[22] The Wiretap Act prohibits the interception of any "wire, oral, or electronic communication" by any person, including U.S. government agents and employees.[23] It contains both civil and criminal penalties for violations, including jail time. The Stored Communications Act prohibits accessing stored electronic communications of all forms, including emails stored on a serves, internet service provider ("ISP") records, subscriber records, and metadata.[24] Like the Wiretap Act, the SCA provides both civil and criminal penalties for violation, and protects against intrusion by both governmental and private actors.[25] To access emails and other stored communications less than 180 days old, the government must acquire a warrant.[26] Under the statute, communications older than 180 days required only a subpoena or court order to obtain. However, some courts have held that this lower standard is unconstitutionally permissive and that a warrant is required to access these

---

20 18 U.S.C. § 2510 *et seq*.

21 18 U.S.C. § 2701 *et seq*.

22 18 U.S.C. § 3121 *et seq*.

23 18 U.S.C. § 2511. Government employees, such as law enforcement officers, can intercept communications covered by the Wiretap Act after going through an extensive warrant process. *See* 18 U.S.C. §§ 2516, 2518.

24 18 U.S.C. §§ 2510, 2701.

25 18 U.S.C. §§ 2510, 2701, 2707.

26 18 U.S.C. § 2703.

communications as well.[27] Finally, the Pen Register Act permits law enforcement officials to attach a device (called a "pen register" or a "trap and trace device") to a telephone line that logs outgoing calls made by a particular telephone. This provision of ECPA applies only to law enforcement and telephone company personnel.

The other major statute that covers acts both by the government and the private sector is the Computer Fraud and Abuse Act. The CFAA was passed in 1984, inspired in part by then-President Ronald Reagan's reaction to the 1983 film *WarGames*, starring Matthew Broderick.[28] Reagan is believed to have said to his advisers, "I don't understand these computers very well, but this young man obviously did. He had tied into NORAD!" [29] The CFAA, originally enacted to protect critical government and military infrastructure (like NORAD), expanded through a series of amendments to include expanded criminal jurisdiction, increased penalties for criminal offenders, a civil cause of action, and an expansive definition of

---

27 *See Warshak v. United States*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the U.S. Court of Appeals for the Sixth Circuit held that individuals have a reasonable expectation of privacy in the contents of emails that are stored with or sent through a commercial ISP. *Id.* at 288. In the October 2017 term, the Supreme Court will address whether a warrant is required to access historical cell phone location data under the SCA in *Carpenter v. United States*. *See* Amy Howe, *Justices to tackle cellphone data case next term*, SCOTUSBlog (June 5, 2017).

28 Declan McCullagh, *From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray*, CNET (Mar. 13, 2013). In *WarGames*, a teenage hacker played by Matthew Broderick hacks into the U.S. strategic aerospace defense command using a personal computer and almost inadvertently starts a thermonuclear war. A House Committee Report on the CFAA explicitly references the film as a realistic representation of a personal computer's capacity. *See* 1984 U.S.C.C.A.N. 3689, 3696.

29 Lou Cannon, The Reagan Presidency: Every Night at the Movies : White House: A creature of Hollywood, Ronald Reagan drew his reality from the films he watched, not from his aides or his briefing books, L.A. Times, April 28, 1991

computer than now covers almost every computer in the United States.[30] The CFAA, at its core, makes it illegal to access a computer (1) without authorization or (2) beyond the scope of prior granted authorization for a variety of illicit purposes.[31] The CFAA has been used extensively by both federal prosecutors seeking to prosecute a wide variety of computer-related crimes and by private litigants, particularly employers seeking damages for employee theft of sensitive or confidential business information.[32]

II. SECTORIZATION

Unlike its European counterparts, as noted above, the United States does not have a federal omnibus privacy or data protection law. Instead, the federal government has taken a sectoral approach by enacting laws that regulate privacy and data security by focusing on a particular sector of the economy, or particular groups of people, such as children 12 and under who use the Internet. Many of the most important federal privacy laws are sector-specific: the Fair Credit Reporting Act ("FCRA"), for example, focuses on companies that compile individual credit scores, the Health Insurance Portability and Accountability Act ("HIPAA") focuses on health care data, the Gramm-Leach-Bliley Act focuses on financial information, and so on.

---

30 McCullagh, *supra* note 18. For a more comprehensive look at the amendments to the CFAA and their impacts on the law, see Office of Legal Education, *Prosecuting Computer Crimes*, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS 2-3 (2010).

31 18 U.S.C. § 1030 *et seq*.

32 *Prosecuting Computer Crimes*, *supra note 28*, at 12-55; Andrew B. Serwin, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE VOL. 1 173-74 (2016).

There are advantages and drawbacks to this approach. Sector-specific regulation allows for greater context specificity and a more detailed approach to the privacy and data security issues that are problematic in a particular industry. However, on the whole, the sectoral approach can leave major gaps in the overall privacy scheme. For example, HIPAA is aimed at regulating the use of health information created by a health care provider (or their business associate) that relates to the condition, provision of care, or payment for care.[33] The particular focus of HIPAA has permitted regulators to address issues particular (such as those dealing with clinical laboratories and student vaccination records) to the health care field with specificity.[34] However, the law is not a comprehensive medical privacy law because it does not cover data when it isn't generated by the specific types of entities that are covered by HIPAA. As new technologies create and share health data outside HIPAA, it is likely that this phenomenon will increase.

Another sectoral federal privacy law, the Video Privacy Protection Act ("VPPA"), offers a good example of a law that is effective at regulating the conduct described, but it is narrowly tailored. The VPPA makes it a federal crime for a video tape service provider to knowingly disclose any personally identifiable information concerning a customer, and also offers civil remedies for people whose statutory rights have been violated.[35] This law was quickly enacted after a Washington, DC-

---

33 Andrew B. Serwin, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE VOL. 2 961-62 (2016).

34 Serwin, *supra* note 29, at 962.

35 Andrew B. Serwin, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE VOL. 2 656 (2016).

area newspaper obtained and published Supreme Court nominee Robert Bork's family's video rental records in the 1980s,[36] The VPPA requires law enforcement to obtain a warrant before obtaining protected records, and provides a civil cause of action for any person aggrieved by the knowing disclosure of protected records.[37] While the VPPA has proven effective in protecting access to customers' video rental records, it does not protect other datasets that are related, including some of those that might be described as implicating "intellectual privacy."[38] Many states protect reader privacy, however, often in the context of library records.[39]

III. THE FEDERAL TRADE COMMISSION

The U.S, government agency that has been most involved in privacy regulation across sectors at the national level has been the Federal Trade Commission ("FTC"). The Federal Trade Commission (FTC) sets the agenda for consumer protection in the United States, and privacy is a prominent part of this agenda. Despite its now central role in consumer protection, the FTC was established in the early 20th century focused on unfair competition by businesses These origins of the FTC, including its original jurisdictional scope, required Congress to significantly amend the Federal Trade Commission Act (FTCA) to provide the FTC with authority to address harms to consumers. This was achieved

---

36 Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 694-96 (2013).

37 *Id.*

38 *Id.* at 691. Included in the broader concept of intellectual privacy is that the media materials an individual consumes, whether it be in video, print, or audio form, should be protected from disclosure. See generally, Neil Richards, Intellectual Privacy (2015).

39 *Id.* at 693.

by giving the FTC expanded ability to act to stop "deceptive" and "unfair" acts or practices. Over time, both the courts and the FTC have clarified the FTC's jurisdiction to protect consumers, and the FTC has taken an increased role in privacy enforcement, first through cases alleging deception, and then through cases relying upon the FTC's unfairness authority.[40]

The FTC has become the lead privacy enforcer in the United States, ahd has expanded its portfolio in recent years to focus on international cooperation in privacy and consumer protection. International enforcement and policy cooperation also has become more important with the proliferation of complex cross-border data flows and cloud computing. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the OECD and the Asia-Pacific Economic Cooperation forum ("APEC"), as well as international cooperation between consumer protection regulators.

Within the OECD, the FTC has participated in the Working Party on Information Security and Privacy, which led the development of the 2007 OECD Council's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. In APEC, the FTC has been actively involved in an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region.

---

[40] Andrew B. Serwin, THE FEDERAL TRADE COMMISSION AND PRIVACY: DEFINING ENFORCEMENT AND ENCOURAGING THE ADOPTION OF BEST PRACTICES, 48 San Diego L. Rev. 809 (2011).

While Section 5, discussed below, is the main focus of the FTC's enforcement power, this was not its first foray into consumer privacy—in the 1970s the FTC was given authority to enforce under the FCRA. Now, while the FTC still enforces under the FCRA, Section 5 is the most common basis of enforcement.

The FTC's deception power was articulated in its 1983 "Policy Statement on Deception," and later discussed in the case of *In re Cliffdale Associates*. The FTC will find an act or practice deceptive if (1) "there is a representation, omission, or practice" that is (2) "likely to mislead the consumer acting reasonably in the circumstances" and (3) the representation, omission, or practice is material. In determining whether a practice is deceptive, the FTC will consider the statements from the perspective of a reasonable consumer. Moreover, in the FTC's view, it does not need to prove that the statement need not actually mislead consumers, but rather that it is likely to mislead consumers.

The FTC's unfairness authority was first addressed in *FTC v. Sperry & Hutchinson Co.*, and those principles have been refined over time. In response to a Congressional inquiry, the FTC issued a policy statement that is now known as its "Unfairness Statement." Congress also amended the FTC Act to address some of these issues, and ultimately the FTC's view of its unfairness authority can be boiled down to the following: an act or practice is unfair if the injury it causes, or is likely to cause, is (1) substantial, (2) not outweighed by other benefits, and (3) not reasonably avoidable.

The most prominent case addressing the scope of the FTC's unfairness and deception powers in the context of privacy and data security is the Third Circuit's decision in *Federal Trade Commission v. Wyndham Worldwide Corporation*.[41] In *Wyndham*, the FTC brought unfairness and deception charges against the Wyndham hotel chain based upon allegations related to alleged failures of data security. The Third Circuit held that the FTC's unfairness power did extend to cover data security issues, rejecting a challenge brought by the hotel chain which had suffered a series of data breaches.[42]

The FTC has traditionally relied more heavily on its deception power to regulate privacy and information security cases, although it has increasingly offered unfairness as an independent theory for regulation, particularly in data security cases.[43] Deception can be an easier route for the FTC because it avoids the harm analysis that is imbedded in the unfairness analysis; in a deception case, by contrast, a material false statement is sufficient to violate the FTC Act. The FTC has averaged about 10 such complaints per year for the last couple of decades, although that number seems to be increasing to some extent.[44]

The FTC cases are not published decisions from courts, but a few scholars view FTC consent decrees as the "new common law of privacy."[45] While this may overstate the effect that FTC orders and consent decrees play in regulating privacy,

---

41 799 F.3d 236 (2015).

42 *Id.* at 246.

43 Hoofnagle, *supra* note 31, at 160; *see also* Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 599 (2014).

44 Solove and Hartzog, *supra* note 42, at 599.

45 *See generally* Solove and Hartzog, *supra* note 42.

primarily because they are only binding on the parties named in the order, and frequently contain provisions expressly stating that the company does not admit any of the conduct or alleged violations, privacy lawyers advising companies in the U.S. certainly consider consent decrees at some level when advising clients. It should be noted that some have criticized the FTC's use of consent decrees to "fence in" companies that deal with consumer data as arbitrary and unpredictable.[46]

IV. PRIVACY FEDERALISM

In the United States, state law and state attorneys general play a major role in the development of privacy and data security law. While federal law has taken the lead in sector-specific laws relating to various segments of the economy (such as the Gramm-Leach Bliley law's focus on financial services and HIPAA's focus on healthcare), state legislatures and attorneys general have lead the way in other areas, particularly in the area of data breach notification. Data breach notification laws in various states make up a large component of the privacy regulatory burden that companies operating in the United States must face and California started this trend by enacting the first data breach law in the world. We now see this trend picked up in many countries, including in Europe. In order to give an overview of some of the elements of state data breach notification laws, it is helpful to look at three examples: California, Massachusetts, and Nevada.

---

46 *Id.* at 608.

In 2003, California became the first state to enact a data breach notification statute.[47] Today, 48 U.S. states and the District of Columbia have enacted some form of data breach notification law.[48] These state laws, not federal law, drive many of the obligations that companies operating in the U.S. must meet in the event of an inadvertent disclosure of personal data. Under California law, any person or entity who owns or licenses computer data must disclose the breach of their data systems to any consumer whose data the entity knows or reasonably believes has been compromised by the breach.[49] The disclosure must be made as soon as reasonably possible and must include the type(s) of information believed to be disclosed by the breach, the approximate date of the breach (if known), a general description of the incident that resulted in the breach, and the contact information of the person or entity that lost the data in question.[50] California's notification statute also includes a wide definition of personal information, including medical information and health insurance information, as well as username and password for certain accounts.[51] In addition, the California Department of Consumer Affairs' Office of Privacy Protection has distributed a list of best practices for companies to follow in the event that their databases have been breached and notification is required,

---

47 Serwin, *supra note 29*, at 432-33.

48 *Security Breach Notification Laws*, National Conference of State Legislatures (April 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

49 Serwin, *supra note 29*, at 432-33.

50 Serwin, *supra note 29*, at 435. Other types of disclosures may be required by statute depending on which types of information were exposed by the breach. For example, the entity issuing the notification is required to provide the phone numbers for the major credit reporting agencies if the breach involved the loss of Social Security, driver's license, or California identification numbers.

51 Serwin, *supra note 29*, at 434.

including adopting written procedures for documenting data security incidents, designating specific individuals to coordinate specific elements of a data breach response, and ensuring third parties that can access data adopt similar practices.[52] Any consumer who is harmed by a violation of the California breach notification statute is authorized to bring suit against the breaching entity for damages.[53]

Massachusetts is another example of a robust state data breach notification law. However, the requirements under the Massachusetts breach notification statute are different from California's. Under Massachusetts law, in the event of a qualifying breach, the entity that was breached must contact not only the affected consumers, but also the state Attorney General's office and the Office of Consumer Affairs and Business Regulation.[54] The timing requirements are similar to the California data breach notification laws. Unlike California, which requires a general description of the incident that lead to the data breach, Massachusetts prohibits companies from including this information in their notification.[55] The Massachusetts law also requires that the state Attorney General, not a private citizen, bring any suit authorized by the notification statute.[56]

The Nevada data breach notification statute is similar in scope to the California and Massachusetts laws with respect to the definitions of personal information and the timing requirements for notifying Nevada residents affected by

---

52 Serwin, *supra note 29*, at 439.
53 Serwin, *supra* note 29, at 437-38.
54 Serwin, *supra* note 29, at 506.
55 Serwin, *supra* note 29 at 508.
56 Serwin, *supra* note 29, at 511.

the breach.[57] The Nevada data breach notification law also requires that the entity holding the data provide notices to national consumer reporting agencies if at least 1,000 Nevada residents are affected by the breach.[58] Nevada also permits companies to maintain their own notification procedures as part of a comprehensive information security policy and holds that companies will be in compliance with the law as long as they follow their own notification procedures (and are otherwise in compliance with the statute's timing requirements).[59] Nevada permits both private citizens and the state Attorney General to bring suits in response to a violation of the data breach notification statute.[60]

California has led the way in other areas of privacy law as well. In 2003, California passed the Online Privacy Protection Act ("Cal OPPA").[61] Cal OPPA, among other important provisions, required websites that collect personal information on its users to display a privacy policy.[62] The privacy policy that Cal OPPA requires must include, at a minimum, the categories of information the site collects, the categories of third parties with whom the information will be shared, the process by which the operator allows consumers to review and request changes to the information held by the operator, the process by which consumers will be

---

57 Serwin, *supra* note 29, at 538-40.

58 Serwin, *supra* note 29, at 538.

59 Serwin, *supra* note 29, at 540.

60 Serwin, *supra* note 29, at 541.

61 Serwin, *supra* note 28, at 62.

62 Serwin, *supra* note 28, at 63. This is an important contribution to privacy and data security regulation for a number of reasons, not the least of which being that the FTC has based much of its privacy-based deceptive trade practice litigation on failing to live up to standards a company has announced in its privacy policies (*see generally* part III *supra*).

notified to any changes in the privacy policy, and the policy's effective date.[63] Another California-specific data security law, known as the "Shine the Light Law," requires companies that collect personal information provide an "opt-out" clause that allows consumers to prevent companies from sharing their data with third parties for the purposes of direct marketing.[64]

In addition to state statutes, state attorneys general play an important role both as independent policy makers and enforcement agencies and through the reinforcement of federal privacy standards. State attorneys general can use their "soft" powers to encourage companies to comply with privacy regulations and adopt sound privacy and data security practices, such as engaging business and community leaders on privacy issues, offering to review companies' privacy policies, and offering "best practices" documents, which provide companies with a list of procedures to follow while also keying them into the views and interpretations that the attorney general's office may take with respect to various provisions in their states' privacy laws.[65] Of course, the power of state attorneys general to bring enforcement actions against violators when gentler measures fail to provide adequate security or privacy is ever-present. In many cases, state attorneys general coordinate efforts by bringing multiple suits against a single target, then sharing information and engaging in joint negotiations.[66] The actions of various state

---

63 Serwin, *supra* note 28, at 63.

64 Serwin, *supra* note 28, at 77-80.

65 Danielle Keats Citron, *The Private Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 758-60 (2016).

66 Citron, *supra* note 60, at 761-62.

attorneys general have been critical in setting norms in a wide variety of privacy and data security areas, including transparency of data use, data breach notification, use restrictions, and others.[67] In addition to creating policy and norms through state statutes, policies, and enforcement actions, state attorneys general can use their positions to help reinforce federal privacy and data security norms. State attorneys general have brought actions against private entities for failing to comply with HIPAA, FCRA, COPPA, and other federal privacy statutes.[68] State attorneys general have also emulated the FTC's enforcement approach in their use of an enforcement tool known as an "assurance of voluntary compliance," similar to the FTC's use of settlements and consent decrees to address unfair and deceptive trade practices.[69]

Rather than engage in costly and time-consuming state-by-state analysis and compliance efforts, companies may simply choose to comply with the rules set by the most restrictive state (or states) and thereby ensure compliance with the rest. This gives large states immense power in setting privacy and data security regulations. Sometimes known as the "California effect," the power of these large marketplaces to set regulations and policies that companies then follow across the board can exert tremendous influence on privacy and data security behaviors both nationally and internationally.[70] All of these state-imposed obligations show that companies

---

67 *See generally* Citron, *supra* note 60, at 763-78.

68 Citron, *supra*, note 60, at 778-80.

69 Citron, *supra* note 60, at 761-2, 781.

70 Citron, *supra* note 60, at 762.

operating in the U.S. cannot afford to ignore the states' roles in creating and shaping American privacy and data security law. Entities who ignore the role of state legislatures and attorneys general do so at their own peril.

V. THE HARM PROBLEM

One final problem that data privacy advocates have encountered when attempting to enforce privacy standards in U.S. courts has been the problem of proving a legally recognizable harm. This is a significant problem for claimants that has both conceptual and practical dimensions. Conceptually, under Article III of the U.S. Constitution, the federal courts are limited to hearing matters that involve a "cases or controversies." Over time, this has given rise to the concept of "standing," or the idea that the plaintiff in a case must be the right person or entity to bring the case before the court – they must have legal "standing" to bring the claim against the defendant. At the most fundamental level, a plaintiff must prove three elements to show they have standing: (1) they must show an injury-in-fact that is either actual or imminent (in other words they must show "harm"), (2) they must show that injury is fairly traceable to the defendant's conduct, and (3) they must show that it is likely that their injury will be reduced or eliminated by a favorable court decision.[71] An injury-in-fact must be both "concrete" and "particularized."[72] For an injury to be concrete, it must be real, i.e. not an abstract injury.[73] To be

---

71 *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1993).

72 *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1548 (2015).

73 *Id*.

particularized, it must impact the plaintiff in a "personal and individual way."[74] While Congress has the power to create legally protected interests by statute that did not exist at common law, this does not mean that they can authorize a plaintiff to bring suit in federal court if they do not meet the minimum constitutional requirements for standing.[75] A "bare procedural violation," or the mere violation of a statute without proof of actual harm, is not enough.[76]

In practice, in the privacy and data security context, plaintiffs have struggled to meet the "injury in fact" requirement, the first element of this fundamental test. Traditionally, harm has been characterized as either economic harm or deprivation of fundamental rights, and absent a showing of economic harm courts have been reluctant to confer standing upon privacy plaintiffs. In *Clapper v. Amnesty International*,[77] for example, the Supreme Court held that the likelihood that the federal government would intercept the plaintiffs' communications, and the cost of implementing protective measures to defend against such interception, were insufficient to confer standing.[78] Another case that exemplifies the difficulties of showing privacy harm in the context of a data breach is *Bell v. Acxiom Corporation*.[79] In *Bell*, April Bell filed suit against Acxiom, a databank that stores

---

74 *Id.*

75 *Id.* at 1549

76 *Id.*

77 133 S.Ct. 1138 (2013).

78 In *Clapper*, the plaintiffs were a group of lawyers, human rights advocates, and other non-profit organizations that, in the course of their work, had contact with individuals overseas who they believed were targets of the National Security Agency's electronic surveillance programs. *Id.* at 1145-46.

79 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006).

personal information for corporate clients, after a gap in Acxiom's database security allowed a third party to access, download, and sell information located on multiple Acxiom-managed databases to a marketing company that used the illegally-downloaded information to advertise via direct mailings.[80] The plaintiff alleged as her harm that the theft of data from Acxiom (which held her personal information) created an increased risk of receiving unwanted direct mailings and an increased risk of identity theft.[81] In dismissing Ms. Bell's claim, the court stated that the mere risk of identity theft was "too speculative" to sustain standing.[82]

Even if plaintiffs can get past the harm requirement for standing in U.S. courts, the inability to prove the costs of inadequate data security may prevent plaintiffs from recovering. Plaintiffs will need to be able to prove damages in order to "win" privacy cases in any meaningful sense, and as long as courts remain hostile to recognizing noneconomic harm in privacy and data security cases.

While Article III standing is not a privacy-specific issue, it is one that is frequently litigated in privacy cases given the abstract and sometimes ephemeral harms that are alleged in most privacy cases. Ultimately, this issue is one that is embedded in the United States Constitution, and thus the burdens plaintiffs must meet are unlikely to change in the near term because changes to the United States

---

80 *Id.* at *1.

81 *Id.* at *2.

82 *Id.* In a case cited in the footnotes, the U.S. District Court for the District of Arizona stated that in order to obtain standing, a plaintiff must show "1) significant exposure of sensitive personal information, 2) a significantly increased risk of identity theft as a result of that exposure and 3) the necessity and effectiveness of credit monitoring in detecting, treating, and/or preventing identity fraud." *Stollenwerk v. Tri-West Healthcare Alliance, Inc.*, 2005 WL 2465906 at *4 (D. Ariz. Sept. 6, 2005).

Constitution are uncommon, whether by amendment or by changes in the interpretation given to the Constitution by the federal Courts.

CONCLUSION

The American law of privacy is not without its complexities or ambiguities, and it can at times be confusing or even bewildering to the uninitiated. Nevertheless, the idea that American law does not protect privacy is a fallacy. Much of the failure to appreciate American privacy can come from a failure to appreciate its key features – Bifurcation, Sectorization, the FTC, Privacy Federalism, and the importance of Privacy Harm. Some of these features are unique to American law, and others are unique (or have special resonance) in U.S. privacy law. Nevertheless, when these features are considered, we believe that the existence and nature of American privacy law can be better appreciated. This is not to say that American privacy law is perfect, or that it has no complexity, ambiguity, and even gaps. However, it would be false to maintain that American privacy law is nonexistent, or that, properly understood, it does not regulate the processing of personal data to a meaningful degree.