

Data Protection Law: An Overview

March 25, 2019

Congressional Research Service
https://crsreports.congress.gov
R45631

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Data Protection Law: An Overview

SUMMARY

R45631

March 25, 2019

Stephen P. Mulligan
Legislative Attorney

Wilson C. Freeman
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Recent high-profile data breaches and other concerns about how third parties protect the privacy of individuals in the digital age have raised national concerns over legal protections of Americans' electronic data. Intentional intrusions into government and private computer networks and inadequate corporate privacy and cybersecurity practices have exposed the personal information of millions of Americans to unwanted recipients. At the same time, internet connectivity has increased and varied in form in recent years. Americans now transmit their personal data on the internet at an exponentially higher rate than in the past, and their data are collected, cultivated, and maintained by a growing number of both "consumer facing" and "behind the scenes" actors such as data brokers. As a consequence, the privacy, cybersecurity and protection of personal data have emerged as a major issue for congressional consideration.

Despite the rise in interest in data protection, the legislative paradigms governing cybersecurity and data privacy are complex and technical, and lack uniformity at the federal level. The constitutional "right to privacy" developed over the course of the 20th century, but this right generally guards only against government intrusions and does little to shield the average internet user from private actors. At the federal statutory level, there are a number of statutes that protect individuals' personal data or concern cybersecurity, including the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, and others. And a number of different agencies, including the Federal Trade Commission (FTC), the Consumer Finance Protection Bureau (CFPB), and the Department of Health and Human Services (HHS), enforce these laws. But these statutes primarily regulate certain industries and subcategories of data. The FTC fills in some of the statutory gaps by enforcing a broad prohibition against unfair and deceptive data protection practices. But no single federal law comprehensively regulates the collection and use of consumers' personal data. Seeking a more fulsome data protection system, some governments—such as California and the European Union (EU)—have recently enacted privacy laws regulating nearly all forms of personal data within their jurisdictional reach. Some argue that Congress should consider creating similar protections in federal law, but others have criticized the EU and California approaches as being overly prescriptive and burdensome.

Should the 116th Congress consider a comprehensive federal data protection law, its legislative proposals may involve numerous decision points and legal considerations. Points of consideration may include the conceptual framework of the law (i.e., whether it is prescriptive or outcome-based), the scope of the law and its definition of protected information, and the role of the FTC or other federal enforcement agency. Further, if Congress wants to allow individuals to enforce data protection laws and seek remedies for the violations of such laws in court, it must account for standing requirements in Article III, Section 2 of the Constitution. Federal preemption also raises complex legal questions—not only of *whether* to preempt state law, but what form of preemption Congress should employ. Finally, from a First Amendment perspective, Supreme Court jurisprudence suggests that while some privacy, cybersecurity, or data security regulations are permissible, any federal law that restricts protected speech, particularly if it targets specific speakers or content, may be subject to more stringent review by a reviewing court.

Contents

Origins of American Privacy Protections 3
The Common Law and the Privacy Torts 3
Constitutional Protections and the Right to Privacy 5
Federal Data Protection Law 7
Gramm-Leach-Bliley Act (GLBA) 8
Health Insurance Portability and Accountability Act (HIPAA) 10
Fair Credit Reporting Act (FCRA) 12
The Communications Act 14
Common Carriers 14
Cable Operators and Satellite Carriers 17
Video Privacy Protection Act 19
Family Educational Rights and Privacy Act (FERPA) 20
Federal Securities Laws 21
Children's Online Privacy Protection Act (COPPA) 24
Electronic Communications Privacy Act (ECPA) 25
Computer Fraud and Abuse Act (CFAA) 29
Federal Trade Commission Act (FTC Act) 30
Consumer Financial Protection Act (CFPA) 35
State Data Protection Law 36
The California Consumer Privacy Act (CCPA) 38
The CCPA's Scope 38
The CCPA's Provisions and Requirements 38
Remedies, Liabilities, and Fines 39
The CCPA and the 116th Congress 39
The EU's General Data Protection Regulation (GDPR) 40
European Data Privacy Laws and the Lead-Up to the GDPR 41
GDPR Provisions and Requirements 42
Scope and Territorial Reach 42
Key Principles 43
Bases for Processing and Consent Requirements 43
Individual Rights and Corresponding Obligations 44
Data Governance and Security 46
Data Breach Notifications 47
Data Transfer Outside the EU 48
Remedies, Liability, and Fines 50
The GDPR and the 116th Congress 50
The Trump Administration's Proposed Data Privacy Policy Framework 51
Considerations for Congress 54
Prescriptive Versus Outcome-Based Approach 55
Defining Protected Information and Addressing Statutory Overlap 56
Agency Enforcement 57
Private Rights of Action and Standing 59
Preemption 62
First Amendment 64
Conclusion 69

Appendixes

Appendix. Summary of Federal Data Protection Laws 71

Contacts

Author Information 75

Recent high-profile data breaches and privacy violations have raised national concerns over the legal protections that apply to Americans' electronic data.[1] While some concern over data protection[2] stems from how the government might utilize such data, mounting worries have centered on how the private sector controls digital information,[3] the focus of this report. Inadequate corporate privacy practices[4] and intentional intrusions into private computer networks[5] have exposed the personal information of millions of Americans. At the same time, internet connectivity has increased and varied in form in recent years, expanding from personal computers and mobile phones to everyday objects such as home appliances, "smart" speakers, vehicles, and other internet-connected devices.[6]

Americans now transmit their personal data on the internet at an exponentially higher rate than the past.[7] Along with the increased connectivity, a growing number of "consumer facing" actors

[1] *See*, *e.g.*, Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ ("This survey finds that a majority of Americans have directly Experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse.").

[2] As discussed in more detail *infra* § Considerations for Congress, the term "data protection" in this report refers to both data privacy (i.e., how companies collect, use, and disseminate personal information) and data security (i.e., how companies protect personal information from unauthorized access or use and respond to such unauthorized access or use). Although data privacy and data security present distinct challenges and are discussed separately in this report when appropriate, legislation addressing these fields increasingly has been unified into the singular field of data protection. *See, e.g.,* ANDREW BURT & ANDREW E. GEER, JR., STANFORD UNIV., HOOVER INST., AEGIS SERIES PAPER NO. 1816, FLAT LIGHT: DATA PROTECTION FOR THE DISORIENTED, FROM POLICY TO PRACTICE 9 (2018) ("What we call 'privacy' and 'security' are now best and jointly described as 'data protection.'"); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2232 (2015) (referring to data privacy and security as "two related areas that together we will refer to as 'data protection.'").

[3] *See*, *e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 16-17 (2019) [hereinafter GAO-19-52] (discussing public opinion surveys related to public concerns over the protection of consumer data).

[4] *See*, *e.g.*, Paul Grewal, Deputy Vice President and General Counsel, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook*, FACEBOOK (last updated Mar. 17, 2017, 9:50 AM PT), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/ (reporting that the data analytics firm Cambridge Analytica exposed private user information by violating Facebook's privacy platform). In addition to violations of privacy protocols, Facebook recently reported that hackers have intentionally infiltrated its private networks. *See* Guy Rosen, Vice President of Product Management, Facebook, *Security Update*, FACEBOOK (Sept. 28, 2018), https://newsroom.fb.com/news/2018/09/security-update/ (reporting that hackers exploited a vulnerability in Facebook's code affecting nearly 50 million accounts).

[5] Large-scale intrusions into private networks have occurred at a variety of companies, including Equifax, Yahoo, Sony, Target, and Home Depot. *See* CRS Report R43496, *The Target and Other Financial Data Breaches: Frequently Asked Questions*, by N. Eric Weiss and Rena S. Miller; Anna Maria Andriotis, Robert McMillan and Christina Rexrode, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, WALL ST. J., Sept. 8, 2017, https://www.wsj.com/articles/equifax-hack-leaves-consumers-financial-firms-scrambling-1504906993.

[6] *See* Joshua D. Wright, Comm'r, Fed. Trade Comm'n, Remarks at the U.S. Chamber of Commerce 7–8 (May 21, 2015), https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf (stating that "[r]esearchers have estimated 900 million devices were connected to the Internet in 2009, increasing to 8.7 billion devices in 2012, and now up to 14 billion devices today," and describing predictions that between 25 billion and 50 billion devices will be connected to the "Internet of Things" by 2020). For background on the "Internet of Things" see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

[7] For statistics on the increasing use of computers and the internet in American homes, see CAMILLE RYAN, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2016, AMERICAN COMMUNITY SURVEY REPORTS 39 (Aug. 2018), https://www.census.gov/content/dam/Census/library/publications/2018/.../ACS-39.pdf and *Internet Broadband Fact Sheet*, PEW RESEARCH CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/internet-broadband/. *See also* GAO-19-52, *supra* note 3, at 5–6 (summarizing recent statistics on internet usage in the United States).

(such as websites) and "behind the scenes" actors (such as data brokers and advertising companies) collect, maintain, and use consumers' information.[8] While this data collection can benefit consumers—for instance, by allowing companies to offer them more tailored products—it also raises privacy concerns, as consumers often cannot control how these entities use their data.[9] As a consequence, the protection of personal data has emerged as a major issue for congressional consideration.[10]

Despite the increased interest in data protection, the legal paradigms governing the security and privacy of personal data are complex and technical, and lack uniformity at the federal level. The Supreme Court has recognized that the Constitution provides various rights protecting individual privacy, but these rights generally guard only against government intrusions and do little to prevent private actors from abusing personal data online.[11] At the federal statutory level, while there are a number of data protection statutes, they primarily regulate certain industries and subcategories of data.[12] The Federal Trade Commission (FTC) fills in some of the statutory gaps by enforcing the federal prohibition against unfair and deceptive data protection practices.[13] But no single federal law comprehensively regulates the collection and use of personal data.[14]

In contrast to the "patchwork" nature of federal law, some state and foreign governments have enacted more comprehensive data protection legislation.[15] Some analysts suggest these laws, which include the European Union's (EU's) General Data Protection Regulation (GDPR)[16] and state laws such as the California Consumer Privacy Act (CCPA),[17] will create increasingly

[8] Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Opening Remarks at PrivacyCon 2017 (Jan. 12, 2017), https://www.ftc.gov/system/files/documents/videos/privacycon-2017-part-1/ftc_privacycon_2017_-_transcript_segment_1.pdf (discussing the growing number of actors involved in compiling user data, including "consumer facing companies" and "behind the scenes" companies); FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 11–13 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter DATA BROKERS REPORT] (discussing how data brokers obtain consumer information).

[9] DATA BROKERS REPORT, *supra* note 8, at v–vi (discussing benefits and risk to data brokers' collection of consumer data).

[10] *See*, *e.g.*, *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing before the S. Comm. on Commerce, Science, and Transp.*, 116th Cong. (2019) [hereinafter *Policy Principles Hearing*]; *Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection and Commerce of the H. Comm. on Energy and Commerce*, 116th Cong. (2019) [hereinafter *Era of Big Data Hearing*]; *Consumer Data Privacy: Examining Lessons from the European Union's Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Science, and Transp.*, 115th Cong. (2018) [hereinafter *GDPR and CCPA Hearing*]; *Examining Safeguards for Consumer Data Privacy: Hearing Before the S. Comm. on Commerce, Science, and Transp.*, 115th Cong. (2018) [hereinafter *Examining Safeguards Hearing*]; *Examining the Current Data Security and Breach Regulatory Notification Regime: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs.*, 115th Cong. (2018) [hereinafter *Current Data Security Hearing*].

[11] *See infra* § Constitutional Protections and the Right to Privacy.

[12] *See infra* § Federal Trade Commission Act (FTC Act).

[13] *See id.*

[14] *See id.*

[15] Zachary S. Heck, *A Litigator's Primer on European Union and American Privacy Laws and Regulations*, 44 LITIG. 59, 59 (2018) ("[T]he United States has a patchwork of laws at both the federal and state levels relating to data protection and information sharing.").

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR].

[17] 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West) (codified in CAL. CIV. CODE §§ 1798.100—1798.198).

overlapping and uneven data protection regimes.[18] This fragmented legal landscape coupled with concerns that existing federal laws are inadequate has led many stakeholders to argue that the federal government should assume a larger role in data protection policy.[19] However, at present, there is no consensus as to what, if any, role the federal government should play, and any legislative efforts at data protection are likely to implicate unique legal concerns such as preemption, standing, and First Amendment rights, among other issues.[20]

This report examines the current U.S. legal landscape governing data protection, contrasting the current patchwork of federal data protection laws with the more comprehensive regulatory models in the CCPA and GDPR. The report also examines potential legal considerations for the 116th Congress should it consider crafting more comprehensive federal data protection legislation. The report lastly contains an **Appendix**, which contains a table summarizing the federal data protection laws discussed in the report.

Origins of American Privacy Protections

The Common Law and the Privacy Torts

Historically, the common law in the United States had little need to protect privacy—as one commentator has observed, "[s]olitude was readily available in colonial America."[21] Although common law had long protected against eavesdropping and trespass,[22] these protections said little to nothing about individual rights to privacy, per se. Over time, gradual changes in the technological and social environment caused a shift in the law. In 1890, Louis Brandeis and Samuel Warren published a groundbreaking article in the Harvard Law Review entitled *The Right to Privacy*.[23] Reacting to the proliferation of the press and advancements in technology such as more advanced cameras, the article argued that the law should protect individuals' "right to privacy" and shield them from intrusion from other individuals. The authors defined this

[18] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018) ("A growing number of foreign countries, and some U.S. states, have articulated distinct versions for how to address privacy concerns, leading to a nationally and globally fragmented regulatory landscape.").

[19] *See*, *e.g.*, *infra* § The Trump Administration's Proposed Data Privacy Policy Framework (discussing the Trump Administration's plans to develop a federal data privacy policy); Ben Kochman, *Tech Giants Want Uniform Privacy Law, But No GDPR,* LAW360 (Sept. 26, 2018), https://www.law360.com/articles/1086064 ("Representatives from Google LLC, Amazon.com Inc., Apple Inc., Twitter Inc., AT&T Inc. and Charter Communications Inc. all said they would support some sort of privacy law that would give consumers more control over the way in which their data is used."); Harper Neidig, *Advocates Draw Battle Lines over National Privacy Law*, THE HILL (Nov. 13, 2018), https://thehill.com/policy/technology/416341-advocates-draw-battle-lines-over-national-privacy-law (discussing statement of 34 public interest groups advocating for comprehensive federal data privacy legislation).

[20] *See infra* § Considerations for Congress.

[21] Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY § 1-4 (2006) (citing DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 1 (1972)).

[22] *See* 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769) ("Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to harken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance . . ."); 3 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 208–09 (1769) (discussing trespass).

[23] 4 HARV. L. REV. 193 (1890).

emergent right as the "right to be let alone."[24] Scholars have argued that this article created a "revolution" in the development of the common law.[25]

In the century that followed Brandeis's and Warren's seminal article, most states recognized the so-called "privacy torts"—intrusion upon seclusion, public disclosure of private facts, false light or "publicity," and appropriation.[26] These torts revolve around the central idea that individuals should be able to lead, "to some reasonable extent, a secluded and private life."[27] The Supreme Court described this evolution of privacy tort law as part of a "strong tide" in the twentieth century toward the "so-called right of privacy" in the states.[28]

Despite this "strong tide," some scholars have argued that these torts, which were developed largely in the mid-twentieth century, are inadequate to face the privacy and data protection problems of today.[29] Furthermore, some states do not accept all four of these torts or have narrowed and limited the applicability of the torts so as to reduce their effectiveness.[30] As discussed in greater detail below, state common law provides some other remedies and protections relevant to data protection, via tort and contract law.[31] However, while all of this state common law may have some influence on data protection, the impact of this judge-made doctrine is unlikely to be uniform, as courts' application of these laws will likely vary based on the particular facts of the cases in which they are applied and the precedents established in the various states.[32]

---

[24] *Id.* at 195–96.

[25] Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983). *See also* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979) (noting that the Brandeis and Warren article has done "nothing less than add a chapter to our law") (quoting Letter from Roscoe Pound to William Chilton (1916)).

[26] Solove, *supra* note 21, § 1-14.

[27] RESTATEMENT (SECOND) OF TORTS § 652A (Am. Law Inst. 2018).

[28] *See* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 487–88 (1975).

[29] *See, e.g.*, Neil M. Richards, *The Limits of Tort Privacy*, 9 J. on TELECOM & HIGH TECH L. 357, 359–60 (2011) ("For better or for worse, American law currently uses tools developed in the nineteenth and mid-twentieth centuries to deal with these problems of the twenty-first."); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889 (2010); Zimmerman, *supra* note 25, at 362 (arguing that the privacy torts have "failed to become a useable and effective means of redress for plaintiffs").

[30] *See* Richards, *supra* note 29 at 360.

[31] *See infra* § State Data Protection Law.

[32] *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 150–51 (3d Cir. 2015) (holding that plaintiffs stated a claim under California invasion of privacy law against Google for placement of tracking cookies on users' browsers); *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204 (C.D. Cal. 2017) (although acknowledging that "Courts have been hesitant to extend the tort of invasion of privacy to the routine collection of personally identifiable information as part of electronic communications," nonetheless concluding that plaintiffs stated a claim for invasion of privacy under California and Massachusetts law against "smart TV" company that collected information on consumer viewing habits); Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1078–80 (N.D. Cal. 2016) (holding that there was a triable question of fact in invasion of privacy claim under California law against software developer that allegedly improperly uploaded address book data without customers' consent). *But see* Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1024–25 (N.D. Cal. 2012) (dismissing claim for invasion of privacy under California law against social networking site that allegedly disclosed to third parties information about users browsing on LinkedIn); Dwyer v. American Express Co., 652 N.E.2d 1351, 1353–56 (Ill. App. Ct. 1995) (dismissing claims for invasion of privacy against credit card company for renting lists of consumer purchasing patterns for advertising purposes).

Constitutional Protections and the Right to Privacy

As reflected in the common law's limited remedies, at the time of the founding, concerns about privacy focused mainly on protecting private individuals from government intrusion rather than on protecting private individuals from intrusion by others.[33] Accordingly, the Constitution's Bill of Rights protects individual privacy from government intrusion in a handful of ways and does little to protect from non-governmental actors. Some provisions protect privacy in a relatively narrow sphere, such as the Third Amendment's protection against the quartering of soldiers in private homes[34] or the Fifth Amendment's protection against self-incrimination.[35] The most general and direct protection of individual privacy is contained in the Fourth Amendment, which states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ."[36]

For more than 100 years, the Fourth Amendment was generally read to prohibit only entry into private places rather than to provide general right to privacy.[37] However, alongside the developments in the common law, constitutional law evolved over time to place a greater emphasis on protecting an individual's personal privacy. In particular, in 1967, the Supreme Court in *Katz v. United States*[38] explained that the Fourth Amendment, while not creating a general "right to privacy," nonetheless protected "people, not places," and guarded individual privacy against certain types of governmental intrusion.[39] This principle has continued to evolve over time, and has come to protect, to some extent, individuals' interest in their digital privacy. For example, in the 2018 case of *Carpenter v. United States*,[40] the Supreme Court concluded that the Fourth Amendment's protection of privacy extended to protecting some information from government intrusion even where that information was shared with a third party. In *Carpenter*, the Court concluded that individuals maintain an expectation of privacy, protected by the Fourth Amendment, in the record of their movements as recorded by their cellular provider.[41] *Carpenter* distinguished earlier cases which had relied upon the principle that information shared with third parties was generally not subject to Fourth Amendment scrutiny, concluding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [his cellular phone]."[42] The Court's holding means that, in the future, the government

[33] Solove, *supra* note 21, at § 1-4.

[34] U.S. CONST. amend. III (forbidding the quartering of soldiers in private homes).

[35] *Id.* amend. V (in part, prohibiting the government from compelling persons toward self-incrimination in criminal cases).

[36] *Id.* amend. IV.

[37] *See e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (in rejecting claim that Fourth Amendment prohibited listening to private telephone calls, stating that "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

[38] 389 U.S. 347 (1967).

[39] *Id.* at 353 ("The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . .").

[40] 138 S. Ct. 2206 (2018).

[41] *Id.* at 2218–20.

[42] *Id.* at 2217 (citing United States v. Miller, 425 U.S. 435, 443 (1976) and Smith v. Maryland, 442 U.S. 735, 741 (1979)).

must obtain a warrant supported by probable cause to obtain this information.[43] The Fourth Amendment thus provides a limited bulwark against government intrusion into digital privacy.

In addition to the protection provided by the Fourth Amendment, in the 1960s and 1970s, the Court concluded that the Fourteenth Amendment's guarantee of "liberty"[44] implied the existence of a more general right of privacy, protecting individuals from government intrusion even outside the "search and seizure" context.[45] In the 1977 case *Whalen v. Roe*, the Supreme Court explained that this constitutional right of privacy "in fact involve[s] at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[46] The second of these interests relates primarily to individual rights concerning the "intimacies of [persons'] physical relationship,"[47] as well as the right to abortion,[48] and has little connection to data protection. However, the first of the interests listed in *Whalen* could potentially relate to data protection. This interest, the right to avoid certain disclosures, has come to be known as the right to "informational privacy."[49]

Despite its broad expression in *Whalen*, every Supreme Court case to consider the informational privacy right has rejected the constitutional claim and upheld the government program alleged to have infringed on the right.[50] In *Whalen* itself, physicians and patients challenged a New York law that required the recording of the names and addresses of all persons who had obtained certain drugs for which there was both a lawful and unlawful market.[51] Although the Court acknowledged that the statute "threaten[ed] to impair . . . [the plaintiffs'] interest in the nondisclosure of private information," the Court observed that the disclosures were an "essential part of modern medical practice" and the New York law had protections in place against unwarranted disclosure that showed a "proper concern" for the protection of privacy.[52] Together, the Court found these factors sufficient to uphold the law.[53] In the wake of *Whalen* and *Nixon v. Administrator of General Services*[54]—a case decided the same year as *Whalen* that also

[43] *Id.* at 2213–14.

[44] U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law."); *id*. amend. XIV ("[N]or shall any State deprive any person of life, liberty, or property, without due process of law . . . .").

[45] *See* Whalen v. Roe, 429 U.S. 589, 599–600, 599 n.23 (1977); Griswold v. Connecticut, 381 U.S. 479, 485 (1965) ("The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees.").

[46] *Whalen*, 429 U.S. at 600.

[47] *See* Lawrence v. Texas, 539 U.S. 558, 577–78 (2003). *See also* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) ("If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."); *Griswold*, 381 U.S. at 485.

[48] *See* Roe v. Wade, 410 U.S. 113, 152–53 (1973) ("This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.") (internal citations omitted).

[49] NASA v. Nelson, 562 U.S. 134, 159 (2011).

[50] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 564 (6th ed. 2018) ("Subsequent to *Whalen* and *Nixon* the Court did little to develop the right of information privacy . . .").

[51] *Whalen*, 429 U.S. at 591.

[52] *Id.* at 604–05.

[53] *Id.* at 605.

[54] 433 U.S. 425, 458–60 (1977) (rejecting constitutional privacy claim against Presidential Recordings and Materials Preservation Act; observing that Act had regulations aimed at preventing "undue dissemination of private materials"

considered the right to informational privacy—courts have struggled to articulate the precise contours of the right. The most recent Supreme Court case to consider the right to informational privacy, *NASA v. Nelson*,[55] went so far as to suggest that the right might not exist, "assuming without deciding" that the right existed in the course of rejecting the constitutional claim challenge to a government background check program for hiring.[56] Despite the Supreme Court's lack of clarity about the right to informational privacy, "most federal circuit courts" recognize the right to various extents.[57]

All of the constitutional rights involving privacy, like the common law privacy torts, focus on public disclosure of private facts. This focus limits their potential influence on modern data privacy debates, which extends beyond the disclosure issue to more broadly concern how data is collected, protected, and used.[58] Perhaps more importantly, whatever the reach of the constitutional right to privacy, the "state action doctrine" prevents it from being influential outside the realm of government action. Under this doctrine, only government action is subject to scrutiny under the Constitution, but purely private conduct is not proscribed, "no matter how unfair that conduct may be."[59] As a result, neither the common nor constitutional law provides a complete framework for considering many of the potential threats to digital privacy and consumer data. Rather, the most important data protection standards come from statutory law.

Federal Data Protection Law

Given the inherent limitations in common law and constitutional protections, Congress has enacted a number of federal laws designed to provide statutory protections of individuals' personal information. In contrast with the scheme prevalent in Europe and some other countries, rather than a single comprehensive law, the United States has a "patchwork" of federal laws that govern companies' data protection practices.[60]

These laws vary considerably in their purpose and scope. Most impose data protection obligations on specific industry participants—such as financial institutions, health care entities, and

and that any privacy intrusion must be weighed against "public interest").

[55] 562 U.S. 134 (2011).

[56] *See NASA*, 562 U.S. at 138 ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged portions of the Government's background check do not violate this right in the present case."). Justices Scalia and Thomas concurred in the judgment, expressing their view that "[a] federal constitutional right to 'informational privacy' does not exist." *Id.* at 159–60 (Scalia, J., concurring).

[57] *See* SOLOVE & SCHWARTZ, *supra* note 50, at 564 (citing cases). *See also* Hancock v. Cty. of Renssalaer, 882 F.3d 58, 65–68 (2d Cir. 2018) (articulating the test for balancing the interests in the disclosure of medical records to the government, concluding that general issues of material fact precluded summary judgment on claim that county jail had violated employees' Fourteenth Amendment rights); Big Ridge, Inc. v. Fed. Mine Safety and Health Review Comm'n, 715 F.3d 631, 649 (7th Cir. 2013) ("Whether the government can require banks, medical providers, or employers to turn over private medical records of customers, patients, or employees that are in their possession is a difficult question of balancing.").

[58] *See supra* notes 3, 10, 18–20 and accompanying text. *See also infra* § Considerations for Congress.

[59] National Collegiate Athletic Ass'n v. Tarkanian, 488 U.S. 179, 191 (1988).

[60] Heck, *supra* note 15, at 59; *see also* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 587 (2014) ("The statutory law is diffuse and discordant . . . . Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors. . . . This sectoral approach also leaves large areas unregulated . . . .").

communications common carriers—or specific types of data, such as children's data.[61] Other laws, however, supplement the Constitution's limited privacy protections and apply similar principles to private entities. The Stored Communications Act (SCA), for instance, generally prohibits the unauthorized access or disclosure of certain electronic communications stored by internet service providers.[62] Lastly, some laws prohibit broad categories of conduct that, while not confined to data protection, limit how companies may handle personal data. Most notably, the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices."[63] As some scholars have pointed out, the FTC has used its authority under the FTC Act to develop norms and principles that effectively fill in the gaps left by other privacy statutes.[64]

These laws are organized below, beginning with those most narrowly focused on discrete industries and moving toward more generally applicable laws. In light of its gap-filling function, this section lastly discusses the FTC Act—along with the Consumer Financial Protection Act (CFPA), which covers similar types of conduct.[65] The **Appendix** to this report contains a table summarizing the federal data protection laws discussed.[66]

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA)[67] imposes several data protection obligations on financial institutions.[68] These obligations are centered on a category of data called "consumer"[69] "nonpublic personal information"[70] (NPI), and generally relate to: (1) sharing NPI with third

[61] *See infra* §§ Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), The Communications Act, and Children's Online Privacy Protection Act (COPPA).

[62] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) ("The [SCA] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.").

[63] 15 U.S.C. § 45(a).

[64] Solove & Hartzog, *supra* note 60, at 587–88 ("It is fair to say that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States . . . . Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation."); Anna Karapetyan, *Developing a Balanced Privacy Framework*, 27 S. CAL REV. L. & SOC. JUST. 197, 213 ("The Federal Trade Commission ('FTC') . . . steps in to fill gaps in statutory protections. The FTC uses its broad authority to restrict 'unfair or deceptive acts or practices' to protect consumer privacy. Unlike federal statutory laws, the FTC is not limited to specific sectors of the economy and its authority applies to most companies acting in commerce.").

[65] This section focuses on federal laws applicable to companies that collect and maintain personal information. It does not cover federal laws primarily applicable to government agencies or government employees, such as the Privacy Act (5 U.S.C. § 552a) or the E-Government Act (44 U.S.C. § 3501 note).

[66] *See infra* § Summary of Federal Data Protection Laws.

[67] 15 U.S.C. §§ 6801–6809.

[68] Under GLBA, a "financial institution" is defined as "any institution the business of which is engaging in financial activities" as described in section 49(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)). 15 U.S.C. § 6809(3). This definition encompasses a broad range of entities, such as "banks; real estate appraisers and title companies; companies that provide consumer financing, insurance underwriters and agents; wire transfer, check cashing, and check printing companies; mortgage brokers; and travel agents that operate in connection with financial services." SARAH J. AUCHTERLONIE & ALEXANDRA E. SICKLER, CONSUMER FINANCE LAW AND COMPLIANCE 13–45 (2017).

[69] GBLA defines "consumer" as an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes" or "the legal representative of such an individual." 15 U.S.C. § 6809(9).

[70] GBLA defines "nonpublic personal information" as "personally identifiable financial information" that is not "publicly available" and is either is "provided by a consumer to a financial institution," "resulting from any transaction with the consumer or any service performed for the consumer," or "otherwise obtained by the financial institution." *Id.*

parties, (2) providing privacy notices to consumers, and (3) securing NPI from unauthorized access.

First, unless an exception applies, GLBA and its implementing regulations prohibit financial institutions from sharing NPI with non-affiliated third parties unless they first provide the consumers with notice and an opportunity to "opt-out."[71] Furthermore, financial institutions are prohibited altogether from sharing account numbers or credit card numbers to third parties for use in direct marketing.[72] Second, financial institutions must provide "clear and conspicuous" initial and annual notices to customers describing their privacy "policies and practices."[73] These notices must include, among other things, the categories of NPI collected and disclosed, the categories of third parties with which the financial institution shares NPI, and policies and practices with respect to protecting the confidentiality and security of NPI.[74] Third, GLBA and its implementing regulations (often referred to as the "Safeguards Rule"[75]) require financial institutions to maintain "administrative, technical, and physical safeguards" to "insure the security and confidentiality" of "customer"[76] (as opposed to "consumer") NPI, and to protect against "any anticipated threats or hazards" or "unauthorized access" to such information.[77] Financial institutions regulated by federal banking agencies[78] are further required to implement a program for responding to the unauthorized access of customer NPI.[79]

The Consumer Financial Protection Bureau (CFPB), FTC, and federal banking agencies share civil enforcement authority for GLBA's privacy provisions.[80] However, the CFPB has no

§ 6809(4).

[71] *Id.* § 6802; 12 C.F.R. § 1016.10(a). The opt-out notice must be "clear and conspicuous" and must provide a "reasonable means" to exercise the opt-out right, such as through "designate[d] check boxes" or providing a "toll-free telephone number" that consumers may call. 12 C.F.R. § 1016.7(a). The opt-out notice can be given in the same electronic or written form as the initial notice of the company's privacy policy. *Id.* § 1016.7(b). Exceptions to the opt-out requirement include situations where a financial institution shares NPI with a third party performing services on behalf of the financial institution, such as the marketing of the financial institution's own products, provided that the third party is contractually obligated to maintain the confidentiality of the information. 15 U.S.C. § 6802(b)(2); 12 C.F.R. § 1016.13. Exceptions further include situations where a financial institution shares NPI with third parties to "effect, administer, or enforce a transaction" requested by the consumer. 15 U.S.C. § 6802(e); 12 C.F.R. § 1016.14.

[72] Specifically, financial institutions are prohibited from disclosing such information to third parties, other than a consumer reporting agency, "for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." 15 U.S.C. § 6802(d); 16 C.F.R. § 313.12(a).

[73] 15 U.S.C. § 6803(a); 12 C.F.R. §§ 1016.4–1016.6.

[74] 12 C.F.R. § 1016.6(a).

[75] *See, e.g.*, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[76] Unlike the disclosure requirements, the safeguard requirements only apply to customers' NPI, rather than consumers' NPI. 15 U.S.C. § 6801(b); 16 C.F.R. § 314.3. A customer is defined as someone who has a "continuing relationship" with the financial institution, such as someone who has obtained a loan or who has opened a credit or investment account. 16 C.F.R. § 313.3(h)–(i); *see also* 12 C.F.R. § 1016.3(i)–(j).

[77] 15 U.S.C. § 6801(a); 16 C.F.R. § 314.3. Such safeguards must include, among other things, the designation of an information security program coordinator, a risk assessment process, and the implementation and testing of information safeguards designed to control risks identified through the risk assessment process. 16 C.F.R. § 314.4.

[78] Federal banking agencies include the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation. 12 U.S.C. § 1813.

[79] 70 Fed. Reg. 15736 (2005).

[80] 15 U.S.C. § 6805(a). The CFPB has exclusive enforcement authority over depository institutions (such as banks, thrifts, and credit unions) with over $10 billion in total assets, and federal banking agencies have exclusive enforcement authority over depository institutions and credit unions with $10 billion or less in total assets. *Id.* § 6805(a). The CFPB

enforcement authority over GLBA's data security provisions.[81] Under the data security provisions, federal banking regulators have exclusive enforcement authority for depository institutions, and the FTC has exclusive enforcement authority for all non-depository institutions.[82] GLBA does not specify any civil remedies for violations of the Act, but agencies can seek remedies based on the authorities provided in their enabling statutes, as discussed below.[83] GLBA also imposes criminal liability on those who "knowingly and intentionally" obtain or disclose "customer information" through false or fraudulent statements or representations.[84] Criminal liability can result in fines and up to five years' imprisonment.[85] GLBA does not contain a private right of action that would allow affected individuals to sue violators.[86]

Health Insurance Portability and Accountability Act (HIPAA)

Under the Health Insurance Portability and Accountability Act (HIPAA), the Department of Health and Human Services (HHS) has enacted regulations protecting a category of medical information called "protected health information" (PHI).[87] These regulations apply to health care providers, health plans, and health care clearinghouses (covered entities), as well as certain "business associates"[88] of such entities.[89] The HIPAA regulations generally speak to covered

and FTC share enforcement authority over the remaining non-depository financial institutions the GLBA covers. *Id.*

[81] *Id.* § 6805(a)(8) (excluding the CFPB from jurisdiction over the data security provisions).

[82] *Id.* § 6805(a)(1)–(7).

[83] *See, e.g.*, JOSEPH BECKMAN, LAW AND BUSINESS OF COMPUTER SOFTWARE § 13:3 (2018) ("The agency enforcing the GLBA will then typically proceed under its own grant of authority and general ability to impose fines."). For instance, under the CFPA, the CFPB can seek a broad range of remedies, including equitable relief and penalties, and under the FTC Act the FTC can seek equitable relief. *See infra* §§ Consumer Financial Protection Act (CFPA) and Federal Trade Commission Act (FTC Act).

[84] 15 U.S.C. §§ 6821, 6823.

[85] *Id.* § 6823.

[86] *See, e.g.*, Barroga-Hayes v. Settenbrino, P.C., No. 10-CV-5298, 2012 WL 1118194, at *6 n. 5 (E.D.N.Y. Mar. 30, 2012) (noting that "there is no private right of action under the GLBA").

[87] 45 C.F.R. part 164. HIPAA regulations define "protected health information" as "individually identifiable health information" transmitted or maintained in "electronic media" or "any other form or medium." *Id.* § 160.103. In turn, "individually identifiable health information" is defined as health information that: (1) "identifies" or can reasonably "be used to identify" an individual; (2) is "created or received by a health care provider, health plan, employer, or health care clearinghouse"; and (3) relates to an individual's physical or mental health, health care provision, or payment for provision of health care. *Id.* "Individually identifiable heath information" does not include data meeting certain "de-identification" requirements. *Id.* § 164.514. Under these requirements, information will not be considered individually identifiable if either: (1) an expert determines that "the risk is very small that the information could be used" to "identify an individual who is a subject of the information" and the expert "[d]ocuments the methods and results of the analysis that justify such determination"; or (2) the information excludes 18 listed identifiers—such as the individual's name, address information, Social Security number, and contact information—and the covered entity does not have "actual knowledge" that the information could be used to identify the individual. *Id.*

[88] A "business associate" is defined as "with respect to a covered entity, a person who: (i) [o]n behalf of such covered entity . . . , but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter . . . ; or (ii) [p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." *Id.* § 160.103.

[89] *Id.* §§ 164.104, 164.306, 164.502.

entities': (1) use or sharing of PHI, (2) disclosure of information to consumers, (3) safeguards for securing PHI, and (4) notification of consumers following a breach of PHI.

First, with respect to sharing, HIPAA's privacy regulations generally prohibit covered entities from using PHI or sharing it with third parties without patient consent,[90] unless such information is being used or shared for treatment, payment, or "health care operations"[91] purposes, or unless another exception applies.[92] Covered entities generally may not make treatment or services conditional on an individual providing consent.[93] Second, with respect to consumer disclosures, covered entities must provide individuals with "adequate notice of the uses and disclosures of [PHI] that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to [PHI]."[94] These notices must be provided upon consumer request, and covered entities maintaining websites discussing their services or benefits must "prominently post" the notices on their websites.[95] Furthermore, an individual has the right to request that a covered entity provide him with a copy of his PHI that is maintained by the covered entity.[96] In some cases, an individual may also request that the covered entity provide information regarding specific disclosures of the individual's PHI, including the dates, recipients, and purposes of the disclosures.[97] Third, with respect to data security, covered entities must maintain safeguards to prevent threats or hazards to the security of electronic PHI.[98] Lastly, HIPAA regulations contain a data breach notification requirement, requiring covered entities to, among other things, notify the affected individuals within 60 calendar days after discovering a breach of "unsecured"[99] PHI.[100]

---

[90] Valid consent must be accompanied by, among other things, a description of the information to be used or disclosed, and a description of the purpose of the requested use or disclosure, and the individual's signature. *Id.* § 164.508(c).

[91] "Health care operations" are defined as including a number of activities, such as: (1) "[c]onducting quality assessment and improvement activities," (2) evaluating health care professionals and health plan performance, (3) underwriting and "other activities related to the creation, renewal, or replacement" of health insurance or health benefits contracts; (4) "conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs"; (5) business planning and development such as "conducting cost-management and planning-related analyses related to managing and operating the entity," and (6) "business management and general administrative activities of the entity." *Id.* § 164.501.

[92] *Id.* §§ 164.506–508. Exceptions to the consent requirement include, among other things, when the use or disclosure is required by law, for public health activities, or for law enforcement purposes. *Id.* § 164.512.

[93] *Id.* § 164.508 (b)(4). Several exceptions apply to this rule, such as when the treatment is research-related or when "the authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations*." Id.*

[94] *Id.* § 164.520(a).

[95] *Id.* § 164.520(c). The regulations further contain specific requirements for certain categories of covered entities; in particular, health plans must provide notices at the time an individual enrolls in the plan and at least once every three years thereafter. *Id.* § 164.520(c)(1). Health care providers must provide the notice by the "date of the first service delivery," or, for emergency treatment situations, "as reasonably practicable" after the treatment; they must further make a "good faith effort" to obtain a written acknowledgement of receipt (except for emergency treatment situations), and they must post the notice in a "clear and prominent location" at any physical service delivery site and have the notices available for individuals to take with them upon request. *Id.* § 164.520(c)(2).

[96] *Id.* § 164.524(a). There are several exceptions to this right; in particular, individuals do not have a right to access: (1) psychotherapy notices or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding. *Id.* § 164.524(a)(1).

[97] *Id.* §164.528.

[98] *Id.* §§ 164.302–318.

[99] "Unsecured" PHI is defined as PHI that "is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary . . . ." *Id.* § 164.402.

[100] *Id.* §§ 164.400–414. HIPAA regulations define a "breach" as the "acquisition, access, use, or disclosure of protected

Violations of HIPAA's privacy requirements can result in criminal or civil enforcement. HHS possesses civil enforcement authority and may impose civil penalties, with the amount varying based on the level of culpability.[101] The Department of Justice has criminal enforcement authority and may seek fines or imprisonment against a person who, in violation of HIPAA's privacy requirements, "knowingly" obtains or discloses "individually identifiable health information" or "uses or causes to be used a unique health identifier."[102] HIPAA does not, however, contain a private right of action that would allow aggrieved individuals to sue alleged violators.[103]

Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA)[104] covers the collection and use of information bearing on a consumer's creditworthiness. FCRA and its implementing regulations govern the activities of three categories of entities: (1) credit reporting agencies (CRAs),[105] (2) entities furnishing information to CRAs (furnishers),[106] and (3) individuals who use credit reports issued by CRAs (users).[107] In contrast to HIPAA or GLBA, there are no privacy provisions in FCRA requiring entities to provide notice to a consumer or to obtain his opt-in or opt-out consent before collecting or disclosing the consumer's data to third parties. FCRA further has no data security provisions requiring entities to maintain safeguards to protect consumer information from unauthorized access. Rather, FCRA's requirements generally focus on ensuring that the consumer information reported by CRAs and furnishers is accurate and that it is used only for certain permissible purposes.[108]

---

health information in a manner not permitted under [HIPAA's privacy regulations] which compromises the security or privacy of the protected health information." *Id.* § 164.402. This definition contains several exclusions, including where the covered entity has a "good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information." *Id*

[101] 42 U.S.C. § 1320d-5; 45 C.F.R. § 160.404. The amounts range from $100 per violation (with a total maximum of $25,000 per year for identical violations) up to $50,000 per violation (with a total maximum of $1,500,000 per year for identical violations). 45 C.F.R. § 160.404(b). The low-end of the penalty spectrum applies when the offender "did not know and, by exercising reasonable diligence, would not have known" of the violation, and the high-end of the penalty spectrum applies when "it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred." *Id.*

[102] 42 U.S.C. § 1320d-6. *See also* Office of Civil Rights, *Enforcement Process*, HEALTH & HUMAN SERVICES (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html ("OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA."). Ordinary criminal violations can result in up to $50,000 in fines and up to one year imprisonment. 42 U.S.C. § 1320d-6(b)(1). However, if the offense is committed under false pretenses, then liability can result in up to $100,000 in fines and up to five years imprisonment. *Id.* § 1320d-6(b)(2). If the offense is committed with an intent to "sell, transfer, or use" individually identifiable health information for commercial advantage, personal gain, or malicious harm, then liability can result in up to $250,000 in fines and up to ten years imprisonment. *Id.* § 1320d-6(b)(3).

[103] *See, e.g.*, Univ. of Colo. Hosp. v. Denver Pub. Co., 340 F. Supp. 2d 1142, 1143 (D. Colo. 2004) (holding that no private right of action exists under HIPAA).

[104] 15 U.S.C. §§ 1681–1681x.

[105] A CRA is any entity that, for a fee or on a cooperative nonprofit basis, regularly assembles or evaluates "consumer credit information" or "other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." *Id.* § 1681a(f).

[106] FCRA regulations define a "furnisher" as any entity that provides a CRA with information "relating to consumers" for inclusion in a consumer report. 12 C.F.R. § 1022.41(c).

[107] AUCHTERLONIE & SICKLER, *supra* note 68, at 13-39.

[108] *See, e.g.*, CHI CHI WU, FAIR CREDIT REPORTING § 1.3.1 (2013) ("The FCRA attempts to protect consumers' privacy

With respect to accuracy, CRAs must maintain reasonable procedures to ensure the accuracy of information used in "consumer reports."[109] CRAs must further exclude adverse information, such as "accounts placed in collection" or civil judgements, from consumer reports after a certain amount of time has elapsed.[110] Furnishers must similarly establish reasonable policies and procedures to ensure the accuracy of the information reported to CRAs and may not furnish to a CRA any consumer information if they have reasonable cause to believe that information is inaccurate.[111] Consumers also have the right to review the information CRAs have collected on them to ensure such information is accurate. CRAs must disclose information contained in a consumer's file upon the consumer's request, as well as the sources of the information and the identity of those who have recently procured consumer reports on the consumer.[112] Should a consumer dispute the accuracy of any information in his file, CRAs and furnishers must reinvestigate the accuracy of the contested information.[113]

In addition to the accuracy requirements, under FCRA consumer reports may be used only for certain permissible purposes such as credit transactions.[114] Accordingly, a CRA may generally furnish consumer reports to a user only if it "has a reason to believe" the user intends to use it for a permissible purpose.[115] Likewise, users may "use or obtain a consumer report" only for a permissible purpose.[116] Along with the permissible purpose requirement, users must further notify consumers of any "adverse action" taken against the consumer based on the report.[117] Adverse actions include refusing to grant credit on substantially the terms requested, reducing insurance coverage, and denying employment.[118]

and reputations by placing various obligations on persons who use or disseminate credit information about consumers. Consumer reporting agencies must adopt reasonable procedures to ensure that the information they disseminate is accurate and up-to-date and that it is furnished only to users with certain permissible purposes.").

[109] 15 U.S.C. § 1681e(b). "Consumer reports" are defined as communications by a CRA about a consumer, which are "used or expected to be used" to evaluate the consumer for credit, insurance, employment or another permissible purpose under the Act. *Id.* § 1681a(d).

[110] *Id.* § 1681c(a). Generally, adverse information may not be reported once the information "antedates the report by more than seven years." *Id.* There are certain exceptions, however, to this general rule. For instance, bankruptcy cases may be reported for up to ten years. *Id.* § 1681c(a)(1).

[111] *Id.* § 1681s-2(a)(1)(A); 12 C.F.R. § 1022.42.

[112] 15 U.S.C. § 1681g(a). If the report was procured for employment purposes, then CRAs must identify each procuring individual in the past two years. *Id.* § 1681g(a)(3)(A)(i). For any other purpose, CRAs need only identify any individual who has procured a consumer report in the past year. *Id.* § 1681g(a)(3)(A)(ii).

[113] 15 U.S.C. §§ 1681i(a), 1681s-2(b); 12 C.F.R. § 1022.43.

[114] Other permissible purposes include, among other things, using the information for (1) employment purposes, (2) insurance underwriting involving the consumer, (3) evaluating a consumer's eligibility for a "license or benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status," or (4) a "legitimate business need" in connection with a business transaction initiated by the consumer or the review of an account to determine whether the consumer continues to meet the terms of the account. 15 U.S.C. § 1681b(a).

[115] *Id.* at § 1681b(a)(3).

[116] *Id.* § 1681m(f).

[117] *Id.* § 1681m(a).

[118] *Id.* §§ 1681a(k)(1), 1691(d)(6).

The FTC and the CFPB share civil enforcement authority over FCRA,[119] with each agency possessing enforcement authority over entities subject to their respective jurisdictions.[120] In addition to government enforcement, FCRA provides a private right of action for consumers injured by willful or negligent violations of the Act.[121] Consumers bringing such actions for negligent violations of the Act may recover actual damages, attorney's fees, and other litigation costs.[122] For willful violations, consumers may recover either actual damages or statutory damages ranging from $100 to $1,000, attorney's fees, other litigation costs, and "such amount of punitive damages as the court may allow."[123] FCRA also imposes criminal liability on any individual who knowingly and willfully obtains consumer information from a CRA under false pretenses and on any officer or employee of a CRA who knowingly and willfully provides consumer information to a person not authorized to receive that information.[124]

The Communications Act

The Communications Act of 1934 (Communications Act or Act), as amended,[125] established the Federal Communications Commission (FCC) and provides a "comprehensive scheme" for the regulation of interstate communication.[126] Most relevant to this report, the Communications Act includes data protection provisions applicable to common carriers, cable operators, and satellite carriers.

Common Carriers

The Telecommunications Act of 1996[127] amended the Communications Act to impose data privacy and data security requirements on entities acting as common carriers.[128] Generally, common carrier activities include telephone and telegraph services but exclude radio broadcasting, television broadcasting, provision of cable television, and provision of broadband

[119] *Id.* § 1681s; *see also* ROBERT BROWNSTONE & TYLER NEWBY, FAIR CREDIT REPORTING ACT GENERALLY, DATA SECURITY & PRIVACY LAW § 9:139 (2018) ("[T]he Consumer Financial Protection Bureau (CFPB) assumed concurrent jurisdiction, and now rulemaking and enforcement duties for the FCRA are shared by the CFPB and the FTC."). Because the two agencies' jurisdiction overlaps, the FTC and CFPB have executed a Memorandum of Understanding (MOU) in which they agreed to coordinate enforcement activities. *See* Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission (2012), https://www.ftc.gov/system/files/120123ftc-cfpb-mou.pdf.

[120] 15 U.S.C. §§ 1681s(a), (b)(H).

[121] *Id.* §§ 1681n–1681o. *But see infra* § Private Rights of Action and Standing (discussing limitations on this private right of action).

[122] 15 U.S.C. § 1681o(a).

[123] *Id.* § 1681n(a).

[124] *Id.* §§ 1681q–1681r. Criminal liability can result in fines and up to two years imprisonment. *Id.*

[125] 47 U.S.C. ch. 5.

[126] Benanti v. United States, 355 U.S. 96, 104 (1957).

[127] Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified throughout 47 U.S.C.).

[128] Specifically, the act uses the term "telecommunications carrier," which the FCC has interpreted as synonymous with a "common carrier." In the Matter of AT&T Submarine Systems, Inc., 13 FCC Rcd. 21585, 21587–21588 (F.T.C. 1998) ("As the Commission has previously held, the term 'telecommunications carrier' means essentially the same as common carrier."). The term "telecommunications carrier" is defined as "any provider of telecommunications services." 47 U.S.C. § 153(51). "Telecommunication service" is further defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." *Id.* § 153(53).

internet.[129] The privacy and security requirements imposed on entities acting as common carriers[130] are primarily centered on a category of information referred to as "customer proprietary network information (CPNI)."[131] CPNI is defined as information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier," and is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[132]

Section 222(c) of the Communications Act and the FCC's implementing regulations set forth carriers' obligations regarding CPNI. These provisions cover three main issues. First, carriers must comply with certain use and disclosure rules. Section 222(c) imposes a general rule that carriers may not "use, disclose, or permit access to" "individually identifiable"[133] CPNI without customer approval,[134] unless a particular exception applies.[135] Before a carrier may solicit a customer for approval to use or disclose their CPNI, it must notify customers of their legal rights regarding CPNI and provide information regarding the carrier's use and disclosure of CPNI.[136] Second, carriers must implement certain safeguards to ensure the proper use and disclosure of CPNI.[137] These safeguards must include, among other things, a system by which the "status of a customer's CPNI approval can be clearly established" prior to its use, employee training on the authorized use of CPNI, and "reasonable measures" to discover and protect against attempts to

[129] *See, e.g.*, *id.* § 153(11) ("a person engaged in radio broadcasting shall not . . . be deemed a common carrier"); United States v. Radio Corp. of Am., 358 U.S. 334, 349 (1959) ("In contradistinction to communication by telephone and telegraph, which the Communications Act recognizes as a common carrier activity . . . the Act recognizes that broadcasters are not common carriers and are not to be dealt with as such.") (internal quotations omitted); FCC v. Midwest Video Corp., 440 U.S. 689, 708–9 (1979) ("The Commission may not regulate cable systems as common carriers, just as it may not impose such obligations on television broadcasters."); FCC Order, Restoring Internet Freedom, FCC 17-166 (Jan. 4, 2018) (reversing a 2015 order classifying broadband internet access service as a common-carriage service and instead classifying it as an "information service").

[130] As a recent decision by the U.S. Court of Appeals for the Ninth Circuit clarified, common carrier classification is activity-based rather than status-based. FTC v. AT&T Mobility LLC, 883 F.3d 848, 850 (9th Cir. 2018) ("[W]e conclude that the [common carrier exemption under the FTC Act] is activity-based. The phrase 'common carriers subject to the Acts to regulate commerce' thus provides immunity from FTC regulation only to the extent that a common carrier is engaging in common-carrier services."); *see also* Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC, 533 F.2d 601, 608 (D.C. Cir. 1976) ("[O]ne can be a common carrier with regard to some activities but not to others.").

[131] 47 U.S.C. § 222(h)(1).

[132] *Id.* § 222(h)(1). The Act further states that CPNI includes "information contained in the bills pertaining to telephone exchange service or telephone service received by a customer of a carrier" but does not include "subscriber list information." *Id.*

[133] "Individually identifiable" is not defined in the statute or regulations. *See id.* §§ 153, 222(h); 47 C.F.R. § 64.2003.

[134] The regulations provide that, generally, customer approval must be "opt-in" approval. 47 C.F.R. §§ 64.2007(b). "Opt-in approval" requires that "the carrier obtain from the customer "affirmative, express consent allowing the requested CPNI usage, disclosure, or access . . . ." *Id.* § 64.2003(k). However, carriers only need to obtain "opt-out approval" to use or disclose individually identifiable CPNI to its agents and affiliates for marketing communications-related service. *Id.* § 64.2007(b). Under "opt-out approval," a customer is deemed to have consented if he has "failed to object" within a specified waiting period after being provided the "appropriate notification of the carrier's request for consent." *Id.* § 64.2003(l).

[135] 47 U.S.C. § 222(c); 47 C.F.R. § 64.2007. Exceptions include, among other things, using or disclosing individually identifiable CPNI to disclose "aggregate customer information," provide or market service offerings for services to which the customer already subscribes, or provide "inside wiring installation, maintenance, and repair services." 47 U.S.C. §§ 222(c)–(d); 47 C.F.R. § 64.2005.

[136] 47 C.F.R. § 64.2008.

[137] *Id.* §§ 64.2009–64.2010.

gain unauthorized access to CPNI."[138] Lastly, carriers must comply with data breach requirements. Following a "breach"[139] of customers' CPNI, a carrier must disclose such a breach to law enforcement authorities no later than seven days following a "reasonable determination of the breach."[140] After it has "completed the process of notifying law enforcement," it must notify customers whose CPNI has been breached.[141]

In addition to the CPNI requirements, the Communications Act contains three other potentially relevant data privacy and security provisions pertaining to common carriers. First, Section 222(a) of the Act states that carriers must "protect the confidentiality of proprietary information" of "customers."[142] Second, Section 201(b) of the Act declares unlawful "any charge, practice, classification, and regulation" in connection with a carrier's communication service that is "unjust or unreasonable."[143] Lastly, Section 202(a) provides that it shall "be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classification, regulations, facilities, or services . . . ."[144]

In a 2016 rule,[145] which was subsequently overturned pursuant to the Congressional Review Act,[146] the FCC attempted to rely on these three provisions to regulate a broad category of data called "customer proprietary information" (customer PI).[147] While customer PI is not defined in the statute, the FCC's 2016 rule defined it broadly to include CPNI, as well as other "personally identifiable information" and the "content of communications." The FCC reasoned that Section 222(a) imposes a general duty, independent from Section 222(c), on carriers to protect the confidentiality of customer PI.[148] It further maintained that Sections 201(b) and 202(a) provide independent "backstop authority" to ensure that no gaps are formed in commercial data privacy and security practices, similar to the FTC's authority under the FTC Act.[149] However, given that Congress overturned the 2016 rule, the FCC may be prohibited under the CRA from relying on these three provisions to regulate data privacy and security. Under the CRA, the FCC may not reissue the rule in "substantially the same form" or issue a "new rule that is substantially the

[138] *Id.*

[139] The regulations provide that a "breach" occurs "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." *Id.* § 64.2011(e).

[140] *Id.* § 64.2011(b).

[141] *Id.* § 64.2011(c). The regulations do not specify a timeline for notifying customers of a breach following the notification of law enforcement. *See id.*

[142] 47 U.S.C. § 222(a).

[143] *Id.* § 201(b).

[144] *Id.* § 202(a).

[145] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274 (Dec. 2, 2016).

[146] S.J. Res. 34, 115th Cong. (2017) (enacted). Senator Jeff Flake, who introduced the joint resolution, criticized the FCC's rule as "restricting the free speech of its regulatory target" and creating a "dual track regulatory environment where some consumer data is regulated one way if a company is using it under the FCC's jurisdiction and an entirely different way if its use falls under the FTC . . . ." 163 Cong Rec. S. 1,925 (2017). He further stated that overturning the rules would "restor[e] a single, uniform set of privacy rules for the internet" and "send a powerful message that Federal agencies can't unilaterally restrict constitutional rights and expect to get away with it." *Id.*

[147] The FCC rule defined "customer proprietary information" to include "individually identifiable CPNI," "personally identifiable information," and "content of communications." 81 Fed. Reg. 87274, 87275.

[148] *Id.* at 87323–87327.

[149] *Id.* at 87328. See § Federal Trade Commission Act (FTC Act), *infra*, for more information on the FTC's authority.

same" as the overturned rule "unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule."[150]

The FCC is empowered to enforce civil violations of the Communications Act's provisions, including its common carrier provisions.[151] The FCC may impose a "forfeiture penalty" against any person who "willfully or repeatedly" violates the Act or the FCC's implementing regulations.[152] The Communications Act further imposes criminal penalties on those who "willfully and knowingly" violate the statute or the FCC's implementing regulations.[153] Along with its general civil and criminal provisions, the Communications Act provides a private right of action for those aggrieved by violations of its common carrier provisions; in such actions, plaintiffs may seek actual damages and reasonable attorney's fees.[154]

Cable Operators and Satellite Carriers

In addition to common carriers, the Communications Act imposes a number of data privacy and security requirements on how "cable operators"[155] and "satellite carriers"[156] (i.e., covered entities)

[150] 5 U.S.C. § 801(b)(2). The CRA does not define "substantially the same." *See id.* § 804. Further, the CRA may preclude courts from determining whether a rule is "substantially the same," as it states that "no determination, finding, action, or omission under this chapter shall be subject to judicial review." *Id.* § 805. Some courts have suggested this provision prevents them from reviewing all actions alleging noncompliance with the CRA. *See, e.g.*, Montanans for Multiple Use v. Barbouletos, 568 F.3d 225, 229 (D.C. Cir. 2009) ("The [CRA] provision denies courts the power to void rules on the basis of agency noncompliance with the Act. The language of § 805 is unequivocal and precludes review of this claim—even assuming that the plan amendments qualify as rules subject to the Act in the first place."); *but see* Ctr. for Biological Diversity v. Zinke, 313 F. Supp. 3d 976, 991 n.89 (D. Alaska 2018) ("CBD is not seeking review of action taken under the CRA. Instead, CBD is claiming that DOI, at the behest of Congress, acted *ultra vires* in taking action beyond the authority provided by the CRA. Therefore, § 805's restriction on judicial review does not apply."). For more information on the CRA, see CRS Report R45248, *The Congressional Review Act: Determining Which "Rules" Must Be Submitted to Congress*, by Valerie C. Brannon and Maeve P. Carey, and CRS Insight IN10660, *What Is the Effect of Enacting a Congressional Review Act Resolution of Disapproval?*, by Maeve P. Carey.

[151] 47 U.S.C. §§ 151, 503(b). In recent years the FCC has brought several data privacy enforcement actions against common carriers. For instance, in 2015, in what the FCC called its "largest data security enforcement action," AT&T settled allegations that it violated the Communications Act's common carrier privacy provisions. Press Release, Fed. Commc'ns Comm'n, AT&T to Pay $25 Million to Settle Consumer Privacy Investigation (Apr. 8, 2015), https://docs.fcc.gov/public/attachments/DOC-332911A1.pdf. In that case, the FCC alleged that employees at AT&T call centers in Mexico, Colombia, and the Philippines accessed customer CPNI without authorization and also disclosed other non-CPNI sensitive customer information, such as names and full or partial Social Security numbers. AT&T Services, Inc., 30 FCC Rcd. 2808 (Apr. 8, 2015) (order and consent decree).

[152] 47 U.S.C. § 503(b)(1). For common carriers, forfeiture penalties may be up to $160,000 for each violation or each day of a continuing violation but may not exceed $1,575,000 for any "single act or failure to act." *Id.* § 503(b)(2)(B); 47 C.F.R. § 1.80(b)(2).

[153] Any person who "willfully and knowingly" violates the Act's requirements may be fined up to $10,000 and imprisoned up to one year, and anyone who "willfully and knowingly" violates any FCC "rule, regulation, restriction or condition" made under the authority of the Act shall be fined up to $500 for "each and every day during which such offense occurs." 47 U.S.C. §§ 501–502.

[154] Common carriers violating the Act "shall be liable to the person or persons injured thereby for the full amount of damages," along with reasonable attorney fees. *Id.* § 206.

[155] "Cable operators" are defined to include anyone who uses the "cable system" to provide any video or other programming service. *Id.* §§ 522(5)–(6).

[156] "Satellite carriers" are defined as any "entity that uses the facilities of a satellite or satellite service . . . to establish and operate a channel of communications for point-to-multipoint distribution of television station signals . . . ." *Id.*§ 338(k)(7); 17 U.S.C. § 119(d)(6).

treat their subscribers'[157] "personally identifiable information" (PII).[158] These requirements relate to: (1) data collection and disclosure; (2) subscribers' access to, and correction of, their data; (3) data destruction; (4) privacy policy notification; and (5) data security.

First, covered entities must obtain the "prior written or electronic consent" of a subscriber before collecting the subscriber's PII or disclosing it to third parties.[159] There are several exceptions to this consent requirement. Among other things, covered entities may collect a subscriber's PII in order to obtain information necessary to render service to the subscriber,[160] and they may disclose a subscriber's PII if the disclosure is necessary to "render or conduct a legitimate business activity" related to the service they provide.[161] Second, covered entities must provide subscribers, at "reasonable times and a convenient place," with access to all of their PII "collected and maintained," and they must further provide subscribers a reasonable opportunity to correct any error in such information.[162] Third, covered entities are obligated to destroy PII if it is "no longer necessary for the purpose for which it is was collected" and there are "no pending requests or orders for access to such information."[163] Fourth, covered entities must provide subscribers with a privacy policy notice at the "time of entering into an agreement" for services and "at least once a year thereafter."[164] These notices must describe, among other things: (1) the nature of the subscriber's PII that has been, or will be, collected, (2) the nature, frequency, and purpose of any disclosure of such information and the types of persons to whom the disclosure is made, and (3) the times and place at which the subscriber may have access to such information.[165] Lastly, the Communications Act imposes a general data security requirement on covered entities; they must "take such actions as are necessary to prevent unauthorized access to [PII] by a person other than the subscriber" or the covered entity.[166]

---

[157] FCC regulations define a "subscriber" in the "context of cable of service" as "a member of the general public who receives broadcast programming distributed by a cable television system and does not further distribute it." 47 C.F.R. § 76.5(ee)(1). FCC regulations further define a "subscriber" in the "context of satellite service" as "a person who receives a secondary transmission service from a satellite carrier and pays a fee for the service, directly or indirectly, to the satellite carrier or to a distributor." *Id.* § 76.5(ee)(2).

[158] The Communications Act only defines PII as information that "does not include any record of aggregate data which does not identify particular persons." 47 U.S.C. §§ 338(i)(2)(A), 551(a)(2)(A). *See also* Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 275 (6th Cir. 2006) ("The phrase 'personally identifiable information' is not defined in the statute except in the negative. The term 'does not include any record of aggregate data which does not identify particular persons.'").

[159] 47 U.S.C. §§ 338(i)(3)–(4), 551(b)–(c).

[160] *Id.* §§ 338(i)(3)(B), 551(b)(2)(A). Cable operators are also allowed to collect PII without the prior written or electronic consent in order to "detect unauthorized reception of cable communications," and satellite carriers may similarly collect PII in order to "detect unauthorized reception of satellite communications." *Id.* §§ 338(i)(3)(B), 551(b)(2)(B).

[161] *Id.* §§ 338(i)(4)(B), 551(c)(2)(B). Covered entities may also disclose PII without consent include situations where: (1) the disclosure is made pursuant to a court order; (2) the disclosure (i) only consists of a subscriber's name and address, (ii) the covered entity has given the subscriber the "opportunity to prohibit or limit such disclosure," and (iii) the disclosure does not reveal the "extent of any viewing or other use by the subscriber" of the service provided or "the nature of any transaction made by the subscriber"; or (3) the disclosure is authorized by a government entity and the disclosure does not include records revealing the subscriber's selection of video programming. *Id.* §§ 338(i)(4)(B), 553(c)(2).

[162] *Id.* §§ 338(i)(5), 551(d).

[163] *Id.* §§ 338(i)(6), 551(e).

[164] *Id.* §§ 338(i)(1), 551(a)(1).

[165] *Id.*

[166] *Id.* §§ 338(i)(4)(A), 551(c)(1).

The Communications Act provides a private right of action for "[a]ny person aggrieved by any act" of a covered entity in violation of these requirements.[167] In such actions, a court may award actual damages, punitive damages, and reasonable attorneys' fees and other litigation costs.[168] Additionally, covered entities violating these provisions may be subject to FCC civil enforcement and criminal penalties that, as previously noted, are generally applicable to violations of the Communications Act.[169]

Video Privacy Protection Act

The Video Privacy Protection Act (VPPA)[170] was enacted in 1988 in order to "preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials."[171] The VPPA does not have any data security provisions requiring entities to maintain safeguards to protect consumer information from unauthorized access. However, it does have privacy provisions restricting when covered entities can share certain consumer information. Specifically, the VPPA prohibits "video tape service providers"[172]—a term that includes both digital video streaming services and brick-and-mortar video rental stores[173]—from knowingly disclosing PII[174] concerning any "consumer"[175] without that consumer's opt-in consent.[176] The VPPA provides several exceptions to this general rule. In particular, video tape service providers may disclose PII to "any person if the disclosure is incident to the ordinary course of business."[177] Providers may also disclose PII if the disclosure solely includes a consumer's name and address and does not identify the "title, description, or subject matter of any video tapes or other audio visual material,"[178] and the consumer has been provided with an opportunity to opt out of such disclosure.[179] The VPPA does not empower any federal agency to enforce violations of the Act

[167] *Id.* §§ 338(i)(7), 551(f)(1).

[168] *Id.* §§ 338(i)(7), 551(f)(2).

[169] *Id.* §§ 501–503.

[170] Video Privacy Protection Act of 1988, Pub. L. No. 100-619, 102 Stat. 3195 (1988) (codified at 18 U.S.C. § 2710).

[171] *Id.* ("An Act . . . to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials.").

[172] "Videotape service provider" is defined as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale or delivery of prerecorded video cassette tapes or similar audio visual materials . . ." *See* 18 U.S.C. § 2710(a)(4).

[173] *See, e.g.*, *In re* Hulu Privacy Litigation, No. C 11-0374, 2012 WL 3282960, at *5–*6 (N.D. Cal. Aug. 10, 2012) (holding that Hulu, a video-streaming business, is a "video tape service provider" under VPPA); Mollett v. Netflix, Inc., No. 5:11–CV–01629, 2012 WL 3731542, at *2 (N.D. Cal., Aug. 17, 2012) ("Netflix does not challenge the allegations that it is a 'video tape service provider" and a 'person providing video recording . . . rental services . . .'").

[174] "[T]he term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider . . . ." 18 U.S.C. § 2710(a)(3).

[175] "Consumer" is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." *Id.* § 2710(a)(1).

[176] *Id.* § 2710(b). The statute specifies that the consumer must provide "informed, written consent (including through an electronic means using the Internet)" that is "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and includes an opportunity, provided in a "clear and conspicuous manner," for the "consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." *Id.* § 2710(b)(2)(B).

[177] *Id*. § 2710(b)(2)(E).

[178] The subject matter of such materials may be disclosed, however, if the disclosure is "for the exclusive use of marketing goods and services directly to the consumer." *Id.* § 2710(b)(2)(D).

[179] *Id.* Other exceptions include disclosures to a law enforcement agency pursuant to a warrant and disclosure pursuant to a court order in a civil proceeding. *Id.* §§ 2710(b)(2)(C), (F).

and there are no criminal penalties for violations, but it does provide for a private right of action for persons aggrieved by the Act.[180] In such actions, courts may award actual damages, punitive damages, preliminary and equitable relief, and reasonable attorneys' fees and other litigation costs.[181]

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act of 1974 (FERPA)[182] creates privacy protections for student education records. "Education records" are defined broadly to generally include any "materials which contain information directly related to a student" and are "maintained by an educational agency or institution."[183] FERPA defines an "educational agency or institution" to include "any public or private agency or institution which is the recipient of funds under any applicable program."[184] FERPA generally requires that any "educational agency or institution" (i.e., covered entities) give parents or, depending on their age, the student[185] (1) control over the disclosure of the student's educational records, (2) an opportunity to review those records, and (3) an opportunity to challenge them as inaccurate.

First, with respect to disclosure, covered entities must not have a "policy or practice" of permitting the release of education records or "personally identifiable information contained therein" without the consent of the parent or the adult student.[186] This consent requirement is subject to certain exceptions. Among other things, covered entities may disclose educational records to (1) certain "authorized representatives,"[187] (2) school officials with a "legitimate educational interest,"[188] or (3) "organizations conducting studies" for covered entities "for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instructions."[189] Covered entities may also disclose the information

[180] *Id.* § 2710(c)(1).

[181] *Id.* § 2710(c)(2).

[182] Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–74 (1974) (codified at 20 U.S.C. § 1232g).

[183] *Id.* § 1232g(a)(4)(A). However, FERPA excludes certain things from the "education records" definition, specifically: (1) records made by "instructional, supervisory, and administrative personnel" that are kept "in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute"; (2) "records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement"; and (3) records made or maintained by a "physician, psychiatrist, psychologist or other recognized professional or paraprofessional" on a student who is "eighteen years of age or older, or is attending an institution of postsecondary education," that are only used "in connection with the provision of treatment" and are "not available to anyone other than the person providing such treatment," except for a "physician or other appropriate professional of the student's choice." *Id.* § 1232g(a)(4)(B).

[184] *Id.* § 1232g(a)(3).

[185] FERPA rights transfer from the parent to the student once the student turns 18 years old or attends a postsecondary institution. *Id.* § 1232g(d).

[186] *Id.* § 1232g(b).

[187] Specifically, this exemption applies to "authorized representatives" of "the Comptroller General of the United States," "the Secretary [of Education]," "State educational authorities," or "authorized representatives of the Attorney General for law enforcement purposes." *Id.* § 1232g(b)(C). Department of Education regulations further define the term "authorized representative" as meaning "any entity or individual designated by a State or local educational authority or an agency headed by [the Comptroller General, Attorney General, or the Secretary of Education] to conduct—with respect to Federal- or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs." 34 C.F.R. § 99.3(b).

[188] 20 U.S.C. § 1232g(b)(1)(A).

[189] *Id.* § 1232g(b)(1)(F). These studies must be conducted in "such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations," and the

without consent if it constitutes "directory information"[190] and the entity has given notice and a "reasonable period of time" to opt out of the disclosure.[191] Second, in addition to the disclosure obligations, covered entities must not have a "policy of denying" or "effectively prevent[ing]" parents or an adult student from inspecting and reviewing the underlying educational records.[192] Covered entities must further "establish appropriate procedures" to grant parents' review requests "within a reasonable period of time, but in no case more than forty-five days after the request has been made."[193] Lastly, covered entities must provide an "opportunity for a hearing" to challenge the contents of the student's education records as "inaccurate, misleading, or otherwise in violation of the privacy rights of students."[194] Covered entities must further "provide an opportunity for the correction or deletion of any such inaccurate, misleading or otherwise inappropriate data contained therein and to insert into such records a written explanation of the parents respecting the content of such records."[195]

Parents or adult students who believe that their rights under FERPA have been violated may file a complaint with the Department of Education.[196] FERPA authorizes the Secretary of Education to "take appropriate actions," which may include withholding federal education funds, issuing a "cease and desist order," or terminating eligibility to receive any federal education funding.[197] FERPA does not, however, contain any criminal provisions or a private right of action.[198]

Federal Securities Laws

While federal securities statutes and regulations do not explicitly address data protection, two requirements under these laws have implications for how companies prevent and respond to data breaches.

First, federal securities laws may require companies to adopt controls designed to protect against data breaches. Under Section 13(b)(2)(B) of the Securities and Exchange Act of 1934 (Exchange

information must be "destroyed when no longer needed for the purpose which it is conducted." *Id.* Other exceptions to the consent requirement include the disclosure of educational records: (1) to "officials of other schools or school systems in which the student seeks or intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record"; (2) "in connection with a student's application for, or receipt of, financial aid"; (3) to "appropriate persons" necessary to "protect the health or safety of the student or other person" in connection with an "emergency"; (4) to "accrediting organizations in order to carry out their accrediting functions"; (5) to parents of a student who is a "dependent" as defined in the Internal Revenue Code; or (6) to comply with a subpoena. *Id*. § 1232g(b*)*.

[190] FERPA defines "directory information" as "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most previous educational agency or institution attended by the student." *Id.* § 1232g(5)(A).

[191] *Id.* § 1232g(a)(5)(B).

[192] *Id.* § 1232g(a)(1)(A).

[193] *Id.* § 1232g(a)(1)(A).

[194] *Id.* § 1232g(a)(2).

[195] *Id.*

[196] 34 C.F.R. § 99.63.

[197] 20 U.S.C. § 1232g(f); 34 C.F.R. § 99.67.

[198] *See* Gonzaga University v. Doe, 536 U.S. 273, 290 (2002) ("FERPA's nondisclosure provisions contain no rights-creating language, they have an aggregate, not individual, focus, and they serve primarily to direct the Secretary of Education's distribution of public funds to educational institutions.").

Act),[199] public companies and certain other companies[200] are required to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances" that "transactions are executed in accordance with management's general or specific authorization," and that "access to assets is permitted only in accordance with management's general or specific authorization."[201] In a recent report, the Securities and Exchange Commission (SEC) suggested that, in order to comply with this requirement, companies should consider "cyber-related threats" when formulating accounting controls.[202] The report discussed the SEC's investigation of companies that wrongly transferred millions of dollars in response to fraudulent emails, generally noting that "companies should pay particular attention to the obligations imposed by Section 13(b)(2)(B)" in light of the "risks associated with today's ever expanding digital interconnectedness."[203]

Second, federal securities laws may require companies to discuss data breaches when making required disclosures under securities laws. The Exchange Act, Securities Act of 1933 (Securities Act),[204] and their implementing regulations[205] require certain companies to file a number of disclosures with the SEC. Specifically, the Securities Act requires companies issuing securities in a public offering to file detailed statements registering the offering (registration statements),[206] and the Exchange Act requires public companies to file periodic reports on an annual, quarterly, and ongoing basis.[207] These filings must contain certain categories of information, such as a description of the most significant factors that make investing in the company speculative or risky (known as "risk factors")[208] and a description of any "events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition . . . ."[209] Further, when making these filings, or any other statements in connection with the purchase or sale of a security, companies are required to include any "material"[210] information necessary to make the statements made therein "not misleading."[211] In interpretive guidance

[199] 15 U.S.C. §§ 78a–78qq.

[200] Companies are subject to these obligations if they have a class of securities registered with the Securities and Exchange Commission (SEC) under Section 12 of the Exchange Act or if they must file reports with the SEC under Section 15(d) of the Exchange Act. *Id.* § 78m(b)(2). Such companies include all companies with securities traded on a national securities exchange, such as the New York Stock Exchange or the Nasdaq Stock Market. *Id.* § 78*l*.

[201] *Id.* §§ 78m(b)(2)(B)(i), (iii).

[202] SEC. EXCHANGE COMM'N, SEC RELEASE NO. 34-84429, REPORT OF INVESTIGATION PURSUANT TO 21(A) OF THE SECURITIES AND EXCHANGE ACT OF 1934 REGARDING CERTAIN CYBER-RELATED FRAUDS PERPETRATED AGAINST PUBLIC COMPANIES AND RELATED INTERNAL ACCOUNTING CONTROLS REQUIREMENTS (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

[203] *Id*. at 5.

[204] 15 U.S.C. §§ 77a–77aa.

[205] 17 C.F.R. Pts. 200–301.

[206] 15 U.S.C. §§ 77f–77g.

[207] *Id.* § 78m; 17 C.F.R. §§ 240.13a-1, 240.13a-11, 240.13a-13.

[208] 17 C.F.R. § 229.503(c).

[209] Commission Statement on Guidance on Public Company Cybersecurity Disclosures, 83 Fed Reg. 8166, 8170 (Feb. 26, 2018).

[210] The Supreme Court has explained that for an omitted fact to be "material" there "must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." Basic Inc. v. Levinson, 485 U.S. 224, 231–232 (1988) (quoting TSC Industries v. Northway, Inc., 426 U.S. 438, 449 (1976)).

[211] 15 U.S.C. § 77k (imposing liability where "any part of the registration statement . . . contained an untrue statement of material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading . . . "); *id.* § 77*l* (imposing liability on "[a]ny person who . . . offers or sells a security . . . by

issued in February 2018, the SEC indicated that, pursuant to these obligations, companies may be required to disclose in their filings cyber incidents such as data breaches.[212]

The SEC can enforce violations of the Securities Act and the Exchange Act, including the accounting controls requirement and the disclosure requirements, through civil actions filed in court[213] or administrative "cease and desist" proceedings.[214] The SEC may seek civil penalties, disgorgement, and injunctive relief (in civil actions) or a cease and desist order (in administrative proceedings).[215] Furthermore, under both the Exchange Act and the Securities Act, individuals aggrieved by a company's misrepresentation or omission of a material fact in connection with the purchase or sale of a security may sue the company for actual damages incurred by the individual.[216] There is not, however, a private right of action for violations of the Exchange Act's accounting controls requirement.[217] Lastly, in addition to civil enforcement, both the Securities Act and the Exchange Act impose criminal liability; any person who "willfully" violates the acts or their implementing regulations may be subject to fines and imprisonment.[218]

means of a prospectus or oral communication, which includes an untrue statement of material fact or omits to state a material fact necessary in order to make the statements, in light of the circumstances under which they were made, not misleading . . ."); *id.* § 78j ("It shall be unlawful for any person . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe . . . ."); 17 C.F.R. § 240.10b-5 ("It shall be unlawful for any person . . . to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading . . . .").

[212] 83 Fed Reg. 8166. The SEC guidance does not provide a bright-line approach defining when companies must report cyber incidents. Rather, it generally directs companies to consider whether they are required to discuss such incidents as part of the required categories of disclosure, such as the risk factors or the description of events impacting the company's operations. *Id.* at 8169–8171. It further directs companies to consider whether cyber incidents are "material" and whether disclosure is required to make the filings "not misleading." *Id.* at 8168–8169. When evaluating materiality, the guidance explains that relevant factors include the nature of the compromised information, potential magnitude of the breach, and range of harm caused by the breach. *Id.* at 8169.

[213] 15 U.S.C. §§ 77t(d), 78u(d).

[214] *Id.* §§ 77h-1, 78u-3.

[215] *Id.* §§ 77h-1, 77t, 78u, 78u-2, 78u-3.

[216] *Id.* § 77*l* (providing a private right of action to investors who purchased a security from someone who offered or sold a security by means of a prospectus or oral communication containing an untrue statement of a material fact or omission of a material fact); Halliburton Co. v. Erica P. John Fund, Inc., 573 U.S. 258, 267 (2014) ("Although section 10(b) does not create an express private cause of action, we have long recognized an implied private cause of action to enforce the provision and its implementing regulation."); Pelletier v. Stuart-James Co., Inc., 863 F.2d 1550, 1557 (11th Cir. 1989) ("In securities fraud cases, therefore, damages are determined in accordance with the extent to which a plaintiff is actually damaged as a result of the defendant's fraudulent conduct.").

[217] *See, e.g.*, *In re* Remec Inc. Sec. Litig., 388 F. Supp. 2d. 1170, 1177 (S.D. Cal. 2005) ("The parties recognize that there is no private right of action under § 78m(b)(2) . . . ."); Eisenberger v. Spectex Indus., Inc., 644 F. Supp. 48, 51 (E.D.N.Y. 1986) ("The court holds that no private cause of action exists under section 78m(b)(2)."); Lewis v. Sporck, 612 F. Supp. 1316, 1333 (N.D. Cal. 1985) ("I conclude that Section 13(b)(2) was not enacted to provide private litigants another cause of action . . . .").

[218] 15 U.S.C. §§ 77x, 78ff(a).

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA)[219] and the FTC's implementing regulations[220] regulate the online collection and use of children's information.[221] Specifically, COPPA's requirements apply to: (1) any "operator"[222] of a website or online service that is "directed to children," or (2) any operator that has any "actual knowledge that it is collecting personal information from a child" (i.e., covered operators).[223] Covered operators must comply with various requirements regarding data collection and use, privacy policy notifications, and data security.

First, COPPA and the FTC's implementing regulations prohibit covered operators from collecting or using "personal information"[224] from children under the age of thirteen without first obtaining parental consent.[225] Such consent must be "verifiable" and must occur before the information is collected.[226] Second, covered operators must provide parents with direct notice of their privacy policies, describing their data collection and sharing policies.[227] Covered operators must further post a "prominent and clearly labeled link" to an online notice of its privacy policies at the home page of its website and at each area of the website in which it collects personal information from children.[228] Lastly, covered operators that have collected information from children must establish and maintain "reasonable procedures" to protect the "confidentiality, security, and integrity" of the information, including ensuring that the information is provided only to third parties that will similarly protect the information.[229] They must also comply with certain data retention and deletion requirements.[230] Under COPPA's safe harbor provisions, covered operators will be

[219] *Id.* §§ 6501–6506.

[220] 16 C.F.R. pt. 312.

[221] *Id.* §§ 6501–6506.

[222] "Operator" is defined as "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service," but does not include any "nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act." 16 C.F.R. § 312.2.

[223] 15 U.S.C. § 6502; 16 C.F.R. § 312.3.

[224] "Personal information" is defined as "individually identifiable information about an individual collected online, including—(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or parents of that child that the website collects online from the child and combines with an identifier described in this paragraph." 15 U.S.C. § 6501(8). FTC regulations further define "personal information" as including (1) a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services," such as "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier"; (2) a "photograph, video, or audio file where such file contains a child's image or voice"; or (3) "[g]eolocation information sufficient to identify street name and name of a city or town." 16 C.F.R. § 312.2.

[225] 15 U.S.C. §§ 6502(a)–(b).

[226] *Id.* § 6502(b)(1)(A)(ii); 16 C.F.R. § 312.5(a)(1). *See also* United States v. UMG, No. cv-04-1050 (C.D. Cal. 2004) (settlement decree), https://www.ftc.gov/sites/default/files/documents/cases/2004/02/040217cagumgrecordings.pdf (settling charges that website operator violated COPPA by notifying parents after it collected the children's information).

[227] 15 U.S.C. § 6502(b)(1)(A)(i); 16 C.F.R. §§ 312.4(a), (c).

[228] 16 C.F.R § 312.4(d).

[229] *Id.* § 312.8.

[230] Operators may only retain children's personal information for "as long as is reasonably necessary to fulfill the

deemed to have satisfied these requirements if they follow self-regulatory guidelines the FTC has approved.[231]

COPPA provides that violations of the FTC's implementing regulations will be treated as "a violation of a rule defining an unfair or deceptive act or practice" under the FTC Act.[232] Under the FTC Act, as discussed in more detail below, the FTC has authority to enforce violations of such rules by seeking penalties or equitable relief.[233] COPPA also authorizes state attorneys general to enforce violations affecting residents of their states.[234] COPPA does not contain any criminal penalties[235] or any provision expressly providing a private right of action.[236]

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) was enacted in 1986,[237] and is composed of three acts: the Wiretap Act,[238] the Stored Communications Act (SCA),[239] and the Pen Register Act.[240] Much of ECPA is directed at law enforcement, providing "Fourth Amendment like privacy protections" to electronic communications.[241] However, ECPA's three acts also contain privacy obligations relevant to non-governmental actors. ECPA is perhaps the most comprehensive federal law on electronic privacy, as it is not sector-specific, and many of its provisions apply to a wide range of private and public actors. Nevertheless, its impact on online privacy practices has been limited. As some commentators have observed, ECPA "was designed to regulate wiretapping and electronic snooping rather than commercial data gathering," and litigants attempting to apply ECPA to online data collection have generally been unsuccessful.[242]

---

purpose for which the information was collected" and must "delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion." *Id.* § 312.10.

[231] 15 U.S.C. § 6503; 16 C.F.R. § 312.11.

[232] 15 U.S.C. § 6502(c).

[233] *Id*. § 45(m)(1)(A). For further discussion of the FTC's enforcement authority under the FTC Act, see § Federal Trade Commission Act (FTC Act), *infra*.

[234] *Id.* § 6504.

[235] *See, e.g.*, John Soma, J. Zachary Courson, & John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J. L. & TECH. 11, 30 (2009) ("COPPA does not carry criminal penalties").

[236] Moreover, no court appears to have considered whether an implied right of action can be read into COPPA. However, the Supreme Court has explained that Congress must create private rights of action in "clear and unambiguous terms," Gonzaga University v. Doe, 536 U.S. 273, 290 (2002) ("In sum, if Congress wishes to create new rights enforceable under § 1983, it must do so in clear and unambiguous terms—no less and no more than what is required for Congress to create new rights enforceable under an implied private right of action."), suggesting that Congress did not create a private cause of action under COPPA. *See* Dorothy Hertzel, *Don't Talk to Strangers: an Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L. J. 429, 439 (2000) ("The COPPA does not provide parents or children with a private right of action . . .").

[237] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–3127).

[238] 18 U.S.C. §§ 2510–2523.

[239] *Id.* §§ 2701–2713.

[240] *Id.* §§ 3121–3127.

[241] Kerr, *supra* note 62, at 1212 ("[T]he [SCA] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."); *see also* Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 730 (9th Cir. 2011) (noting that "ECPA was intended to shore up Fourth Amendment rights").

[242] Solove & Hartzog, *supra* note 60, at 592 ("An attempt was made early on to apply existing statutory law to online

The Wiretap Act applies to the interception of a communication in transit. A person violates the Act if, among other acts,[243] he "intentionally intercepts . . . any wire, oral, or electronic communication."[244] The Wiretap Act defines an "electronic communication" broadly, and courts have held that the term includes information conveyed over the internet.[245] Several thresholds must be met for an act to qualify as an unlawful "interception." Of particular relevance are three threshold issues.[246] First, the communication must be acquired contemporaneously with the transmission of the communication.[247] Consequently, there is no "interception" where the communication in question is in storage.[248] Furthermore, the acquired information must relate to the "contents" of the communication, defined as information concerning the "substance, purport, or meaning of that communication."[249] As a result, while the Act applies to information like the header or body of an email,[250] the Act does not apply to non-substantive information automatically generated about the characteristics of the communication, such as IP addresses.[251]

---

data gathering practices. . . . ECPA was indeed a poor fit, as it was designed to regulate wiretapping and electronic snooping rather than commercial data gathering. . . . These rare attempts to apply existing law nearly all failed . . . .").

[243] The Wiretap Act also prohibits: (1) any person from intentionally disclosing or using of the contents of a communication obtained through an unlawful interception; (2) any person from disclosing information obtained through a lawful interception in connection with a criminal investigation, where the disclosure is made with the intent to "improperly obstruct, impede, or interfere with a duly authorized criminal investigation"; and (3) electronic service providers from "intentionally divulging the contents of any communication" in transmission to anyone other than the sender or intended recipient. 18 U.S.C. §§ 2511(1)(c)–(e), (3)(a).

[244] *Id.* § 2511(1)(a).

[245] The Wiretap Act defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo electronic or photooptical system that affects interstate or foreign commerce . . ." *Id.* § 2510(12). Courts have held that this definition encompasses information transmitted via the internet, such as emails or computer viruses. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) ("Here, the source penetrated Steiger's computer by using a 'Trojan Horse' virus that enabled him to discover and download files stored on Steiger's hard drive. That information was transferred from Steiger's computer to the source over one of the specified media and thus falls within the Wiretap Act's definition of 'electronic communications.'"); United States v. Councilman, 418 F.3d 67, 84 (1st Cir. 2005) ("The simplest reading of the statute is that the e-mail messages were 'electronic communications' under the statute at the point where they were intercepted.").

[246] There are a number of other exceptions to the Wiretap Act not discussed here. For instance, the Act allows law enforcement to intercept communications pursuant to a court order. 18 U.S.C. §§ 2516–2518.

[247] *See, e.g.*, Luis v. Zang, 833 F.3d 619, 629 (6th Cir. 2016) ("We therefore hold that, in order for an 'intercept' to occur for purposes of the Wiretap Act, the electronic communication at issue must be acquired contemporaneously with the transmission of that communication.").

[248] Communications in storage are generally covered by the SCA, rather than the Wiretap Act. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878–879 (9th Cir. 2002) ("We therefore hold that for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage. . . . [This conclusion] is consistent with the structure of ECPA, which created the SCA for the express purpose of addressing 'access to stored . . . electronic communications and transactional records.'") (emphasis in original).

[249] 18 U.S.C. §§ 2510(4), (8).

[250] Optiver Australia Pty. Ltd. & Anor. v. Tibra Trading Pty. Ltd. & Ors., No. C12-80242 EJD (PSG), 2013 WL 256771, *2 (N.D. Cal. 2013) ("The subject lines of emails and other electronic communications serve to convey a substantive message about the body of the email. In the sense that they communicate information concerning the 'substance, purport, or meaning' of the topic of the email, subject lines are no different from the body of the email.").

[251] *See, e.g.*, *In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014) ("[W]e hold that under ECPA, the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."). Courts have noted that IP address information, identifying the server or device with which an internet user communicated, does not reveal "contents" of a communication. *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 97 (2nd Cir. 2017) ("We therefore join the other circuits that have considered this narrow question and hold that collecting IP address information devoid of content is 'constitutionally indistinguishable from the use of a pen register.'"). However, uniform resource locators

Third, individuals do not violate the Wiretap Act if they are a "party to the communication" or received "prior consent" from one of the parties to the communication.[252] The party-to-the-communication and consent exceptions have been subject to significant litigation; in particular, courts have often relied on the exceptions to dismiss suits alleging Wiretap Act violations due to online tracking, holding that websites or third-party advertisers who tracked users' online activity were either parties to the communication or received consent from a party to the communication.[253]

The SCA prohibits the improper access or disclosure of certain electronic communications in storage. With respect to improper access, a person violates the SCA if he obtains an "electronic communication"[254] in "electronic storage"[255] from "a facility through which an electronic communication service is provided" by either: (1) "intentionally access[ing] [the facility] without authorization" or (2) "intentionally exceed[ing] an authorization."[256] Although the statute does not define the term "facility," most courts have held that the term is limited to a location where network service providers store communications.[257] However, courts have differed over whether a personal computer is a "facility." Most courts have excluded personal computers from the reach of the SCA,[258] but some have disagreed.[259]

(URLs), which reveal more information than IP addresses, may, in some cases, reveal "contents" of a communication and be excluded from the reach of the Pen Register Act. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 n. 6 (9th Cir. 2008) ("A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity."). For instance, if a URL contains a search term entered by the user, then it may reveal "content." *See, e.g.*, *In re* Application of U.S. for an Order Authorizing use of A Pen Register and Trap, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

[252] 18 U.S.C. § 2511(2)(d).

[253] *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (holding that third-party advertising company's placement of cookies on users' computers that track their activities on affiliated websites did not violate the Wiretap Act because the affiliated sites were "parties to the communication" and had consented to the interception); *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F. 3d 125, 139–142 (3d Cir. 2015) (holding that third-party advertising companies were parties to the communications because the users' servers sent a request to their servers asking them to populate the websites with ads, and in response to these requests the advertising companies either placed a cookie on the users' browsers or collected information from an existing cookie). *But see In re* Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003) (reversing district court's dismissal of plaintiffs' Wiretap Act claim and holding that defendants' actions constituted an "interception" and defendants did not have "consent").

[254] For the Wiretap Act's definition of "electronic communication," see *supra* note 245. This definition also applies to the SCA. 18 U.S.C. § 2711(1) ("the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section").

[255] "Electronic storage" means: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17).

[256] *Id.* § 2701(a).

[257] *See, e.g.*, *Google*, 806 F. 3d at 147 ("'[F]acility' is a term of art denoting where network service providers store private communications.").

[258] *See, e.g.,* Morgan v. Preston, No. 13–cv–0403, 2013 WL 5963563, at *5 (M.D. Tenn. Nov. 7, 2013) ("[T]he overwhelming body of law" supports the conclusion that "an individual's personal computer is not a 'facility through which an electronic communication service is provided.'").

[259] *See, e.g.*, Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) ("Viewing this factual dispute in the light most favorable to the nonmovant, as is required on summary judgment, it is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act.").

With respect to improper disclosure, the SCA generally prohibits[260] entities providing "electronic communication services"[261] or "remote computing services"[262] from knowingly divulging the contents of a communication while holding the communication in electronic storage.[263] Similar to the Wiretap Act, the SCA's access and disclosure prohibitions are subject to certain exceptions. In particular, individuals do not violate the SCA if they are the sender or intended recipient of the communication or when a party to the communication consents to the access or disclosure.[264] As with the Wiretap Act, courts have relied on these two exceptions to dismiss suits under the SCA related to online tracking.[265]

The Pen Register Act prohibits the installation of a "pen register" or "trap and trace device" without a court order.[266] A pen register is a "device or process" that "records or decodes" outgoing "dialing, routing, addressing, or signaling information," and a trap and trace device is a "device or process" that "captures the incoming . . . dialing, routing, addressing, and signaling information."[267] In contrast to the Wiretap Act, the Pen Register Act applies to the capture of non-content information, as the definitions of pen registers and trap and trace devices both exclude any device or process that captures the "contents of any communication."[268] Furthermore, the Pen Register Act prohibits only the use of a pen register or trap and trace device and does not separately prohibit the disclosure of non-content information obtained through such use.[269] The statute does, however, have several exceptions similar to those contained in the Wiretap Act and SCA. Among other things, providers of an electronic or wire communication service will not violate the Act when they use a pen register or trap and trace device in order to "protect their rights or property" or "where the consent of the user of that service has been obtained."[270]

The Wiretap Act and the SCA both provide for private rights of action. Persons aggrieved by violations of either act may bring a civil action for damages, equitable relief, and reasonable attorney's fees.[271] For actions under the Wiretap Act, damages are the greater of: (1) actual damages suffered by the plaintiff, or (2) "statutory damages of whichever is the greater of $100 a

[260] This disclosure prohibition applies to remote computing service providers only when they maintain the communication: (A) on behalf of "a subscriber or customer of such service"; and (B) "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." 18 U.S.C. § 2702(a)(2).

[261] The SCA incorporates the Wiretap Act's definition of an "electronic communication service." *Id.* § 2711(1) ("[T]he terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section."). Under the Wiretap Act's definition, an "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

[262] "Remote computing service" means the "provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2).

[263] *Id.* § 2702(a).

[264] *Id.* §§ 2701(c), 2702(b). There are a number of other exceptions to the SCA. For instance, service providers may disclose the contents of a communication when the disclosure is "necessarily incident" to the "rendition of the service" or the "protection of [the provider's] rights or property" of the provider. *Id.* at § 2702(b).

[265] *See, e.g.*, *DoubleClick*, 154 F. Supp. 2d at 507–511 (holding that, under the SCA, website was a party to the communications and consented to a third-party advertiser's access to the communications.).

[266] 18 U.S.C. § 3121(a).

[267] *Id.* §§ 3127(3)–(4).

[268] *Id.*

[269] *Id*. § 3121.

[270] *Id.* § 3121(b).

[271] *Id.* §§ 2520(a)–(b), 2707(a)–(b).

day for each day of violation or $10,000."[272] For actions under the SCA, damages are "the sum of the actual damages suffered by the plaintiff and the profits made by the violator," provided that all successful plaintiffs are entitled to receive at least $1,000.[273] Violations of the Wiretap Act and SCA are also subject to criminal prosecution and can result in fines and imprisonment.[274] In contrast, the Pen Register Act does not provide for a private right of action, but knowing violations can result in criminal fines and imprisonment.[275]

Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA)[276] was originally intended as a computer hacking statute and is centrally concerned with prohibiting unauthorized intrusions into computers, rather than addressing other data protection issues such as the collection or use of data.[277] Specifically, the CFAA imposes liability when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[278] A "protected computer" is broadly defined as any computer used in or affecting interstate commerce or communications, functionally allowing the statute to apply to any computer that is connected to the internet.[279]

Violations of the CFAA are subject to criminal prosecution and can result in fines and imprisonment.[280] The CFAA also allows for a private right of action, allowing aggrieved individuals to seek actual damages and equitable relief, such as an injunction against the defendant. [281] As with ECPA, internet users have attempted to use this private right of action to sue companies tracking their online activity, arguing that companies' use of tracking devices constitutes an unauthorized access of their computers.[282] In this vein, CFAA is theoretically a more generous statute than ECPA for such claims because it requires authorization from the owner of the computer (i.e., the user), rather than allowing any party to a communication (i.e., either the user or the website visited by the user) to give consent to the access.[283] In practice,

[272] *Id.* § 2520(c)(2).

[273] 18 U.S.C. § 2707(c). Courts may also assess punitive damages where the SCA violation is willful or intentional. *Id.*

[274] *Id.* §§ 2511(4), 2701(b).

[275] *Id.* § 3121(d).

[276] *Id.* § 1030.

[277] *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009) ("The [CFAA] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives.") (internal quotations omitted).

[278] *Id.* § 1030(a)(2)(c).

[279] *Id.* § 1030(e)(2).

[280] *Id.* § 1030(c).

[281] *Id.* § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[282] *See, e.g.*, Complaint at ¶¶ 92–96, *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) No. 00-Civ-0641 (BRB), 2000 WL 34326002 (alleging that third-party advertiser, which placed cookies on users' computers that tracked their activities on affiliated websites, violated CFAA because plaintiffs' computers are "protected computers" and the third-party advertiser intentionally accessed them "without authorization or by exceeding authorized access and thereby obtained information from such protected computers").

[283] *See, e.g.*, Craiglist Inc. v. 3Taps Inc., 964 F.Supp. 2d 1178, 1183 (N.D. Cal. 2013) ("[T]he Ninth Circuit's interpretation of the CFAA's phrase 'without authorization' confirms that computer owners have the power to revoke the authorizations they grant."); Sargeant v. Maroil Trading Inc., No. 17-81070, 2018 WL 3031841, *6 (S.D. Fla. 2018) ("[U]nder the CFAA, the person who can 'authorize' access to the protected computer is the person who retains

however, such claims have typically been dismissed due to plaintiffs' failure to meet CFAA's damages threshold.[284] Specifically, as a threshold to bring a private right of action, a plaintiff must show damages in excess of $5,000 or another specific type of damages such as physical injury or impairment to medical care.[285]

Federal Trade Commission Act (FTC Act)

The FTC Act has emerged as a critical law relevant to data privacy and security. As some commentators have noted, the FTC has used its authority under the Act to become the "go-to agency for privacy," effectively filling in gaps left by the aforementioned federal statutes.[286] While the FTC Act was originally enacted in 1914 to strengthen competition law, the 1938 Wheeler-Lea amendment revised Section 5 of the Act to prohibit a broad range of unscrupulous or misleading practices harmful to consumers.[287] The Act gives the FTC jurisdiction over most individuals and entities, although there are several exemptions.[288] For instance, the FTC Act exempts common carriers,[289] nonprofits,[290] and financial institutions such as banks, savings and loan institutions, and federal credit unions.[291]

The key provision of the FTC Act, Section 5, declares unlawful "unfair or deceptive acts or practices" (UDAP) "in or affecting commerce."[292] The statute provides that an act or practice is

dominion and control over that computer and/or the relevant information contained on that computer."). For a discussion of ECPA's scope, see § Electronic Communications Privacy Act (ECPA), *supra*.

[284] *See, e.g.*, *Double Click*, 154 F. Supp. 2d at 520–526 (holding that plaintiffs could not meet CFAA's $5,000 threshold by aggregating their damages, as damages could only be aggregated across multiple victims for a "single act" against a "particular computer"); *Google*, 806 F.3d at 148–149 (holding that plaintiffs failed to meet damages threshold because they failed to show they suffered any concrete harm); Mount v. Pulse Point, No. 13-6592-CV, 2016 WL 5080131, at *7–*9 (S.D.N.Y. Aug. 17, 2016) (same); *but see In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *9 –*12 (N.D. Cal. Oct. 9, 2001) (rejecting defendants' motion to dismiss CFAA action based on defendants' use of web bugs and cookies to track plaintiffs' online activities and holding that plaintiffs adequately pleaded damages under CFAA). Relatedly, plaintiffs' failure to allege concrete harm through the use of cookies has led some courts to conclude that the standing requirements under Article III of the Constitution were not met. *See, e.g.*, LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW, 2011 WL 1661532, *3–*6, *8 (C.D. Cal., Apr. 28, 2011) (dismissing, with leave to amend, CFAA action for failure to allege harm giving rise to Article III standing). *See also infra* § Private Rights of Action and Standing (discussing constitutional limitations on private rights of action).

[285] 18 U.S.C. §§ 1030(c)(4)(A)(i), (g).

[286] Solove & Hartzog, *supra* note 60, at 588, 604 ("Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation. . . . [P]artly due to the FTC's embrace of the self-regulatory approach, its impeccable timing, a large void in U.S. privacy law, and lack of existing alternatives, the FTC became the go-to agency for privacy.").

[287] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1228 (11th Cir. 2018) ("[A]t the time of the FTC Act's inception, the FTC's primary mission was understood to be the enforcement of antitrust law. In 1938, the Act was amended to provide that the FTC had authority to prohibit 'unfair . . . acts or practices.' This amendment sought to clarify that the FTC's authority applied not only to competitors but, importantly, also to consumers.").

[288] 15 U.S.C. § 45(a)(2) (providing the FTC with jurisdiction over all "persons, partnerships, or corporations" except certain exempted entities).

[289] *Id.* For a discussion of common carriers regulated under the Communications Act, see *supra* § Common Carriers.

[290] *See, e.g.*, Nat'l Fed'n of the Blind v. Fed. Trade Comm'n, 420 F.3d 331, 334 (4th Cir. 2005) ("[A]ccording to the FTC's organic statute, non-profit organizations fall outside the scope of the agency's jurisdiction.").

[291] 15 U.S.C. § 45(a)(2).

[292] *Id.* § 45(a)(1); *see also* FED. TRADE COMM'N, REPORT ON PRIVACY & DATA SECURITY 1 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (noting that the FTC's "primary legal authority comes from Section 5 of the [FTC] Act").

"unfair" only if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[293] While the statute does not define "deceptive," the FTC has clarified in guidance that an act or practice is to be considered deceptive if it involves a material "representation, omission, or practice that is likely to mislead [a] consumer" who is "acting reasonably in the circumstances."[294] Under the FTC Act, the agency may enact rules defining specific acts or practices as UDAPs,[295] often referred to as "trade regulation rules" (TRRs)[296] or "Magnuson-Moss" rulemaking.[297] However, to enact TRRs the FTC must comply with several procedures that are not required under the notice-and-comment rulemaking procedures set forth in Section 553 of the Administrative Procedure Act (APA), which are the default rulemaking procedures for federal agencies.[298] Among other things, these additional procedures require the FTC to publish an advance notice of proposed rulemaking (ANPRM), give interested persons an opportunity for an informal hearing, and issue a statement accompanying the rule regarding the "prevalence of the acts or practices treated by the rule."[299] Consequently, the FTC rarely uses its TRR rulemaking authority[300] and has not enacted any TRRs regarding data protection.[301] Rather,

[293] 15 U.S.C. § 45(n).

[294] FED. TRADE COMM'N, POLICY STATEMENT ON DECEPTION 1–2 (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf; *see also*, *In re* International Harvester, 104 F.T.C. 949, 1984 WL 565290, *85 (1984) ("Our approach to deception cases was described in a policy statement that the Commission issued in 1983. . . . In brief, a deception case requires a showing of three elements: (1) there must be a representation, practice, or omission likely to mislead consumers; (2) the consumers must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be 'material,' that is, likely to affect consumers' conduct or decision with regard to a product.").

[295] 15 U.S.C. § 57a(a)(1)(B) ("[T]he Commission may prescribe . . . rules which define with specificity acts or practices which are unfair or deceptive . . .").

[296] FED. TRADE COMM'N, OPERATING MANUAL: CHAPTER SEVEN 2, https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf (last visited Jan. 3, 2019) (stating that rules promulgated under the FTC Act are "referred to as 'trade regulation rules' (TRRs).").

[297] The Magnuson-Moss Warranty—Federal Trade Commission Improvements Act amended the FTC Act to include this rulemaking authority. Pub. L. No. 93-637 § 202(d), 88 Stat. 2183, 2198 (1975) (codified at 15 U.S.C. § 57a).

[298] 15 U.S.C. § 57a (providing that the FTC "shall proceed in accordance with section 553 of [the APA]" as well as the other specified procedures); see also Auchterlonie & Sickler, supra note 68, at 1-28 ("The [rulemaking procedures under the FTC Act] exceed the notice-and-comment procedures mandated in Section 553 of the APA which otherwise typically apply to agency rulemakings."). For an overview of the notice-and-comment procedures under Section 553 of the APA, see CRS Report R41546, A Brief Overview of Rulemaking and Judicial Review, by Todd Garvey.

[299] 15 U.S.C. § 57a(b)–(d).

[300] *See, e.g.*, Jeffrey S. Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1989–1990 (2015) (explaining that "no new rule makings under the Magnuson-Moss Procedures have been initiated since 1980, when the procedures were made more complex by that year's FTC Improvements Act," other than the FTC amending some if its "original trade regulation rules . . . after conducting period reviews of their effectiveness"); *see also* Hartzog & Solove, supra note 2, at 2300 n.160 ("[Under Section 5] the FTC has only Magnuson-Moss rulemaking which is so procedural burdensome that it is largely ineffective . . . . These rules require the FTC Staff to engage in an industry-wide investigation, prepare draft staff reports, propose a rule, and engage in a series of public hearings, including cross-examination opportunities prior to issuing a final rule in any area. These processes are so burdensome that the FTC has not engaged in a Magnuson-Moss rule-making in 32 years.") (internal citations omitted).

[301] *See* 16 C.F.R. pts. 408–460; *see also* Lubbers, *supra* note 300, at 1985–1989 (describing FTC rulemakings before and under the Magnuson-Moss rulemaking procedures).

as discussed further below, the agency largely uses enforcement actions to signal the types of acts and practices it considers to be impermissible UDAPs.[302]

The FTC has brought hundreds of enforcement actions against companies alleging deceptive or unfair data protection practices.[303] Most of these actions result in companies entering into consent decrees requiring the companies to take certain measures to prevent any further violations.[304] While these consent decrees are not legally binding on those who are not a party to them, they are significant because they reflect the type of practices that the FTC views as "unfair" or "deceptive."[305] Indeed, some scholars view the principles arising from them as a type of "common law of privacy."[306] Given the uniquely important role FTC enforcement plays in the U.S. data protection landscape, it is worth noting the types of data protection practices the FTC has viewed as "unfair" or "deceptive."

Perhaps the most settled principle of the FTC's "common law of privacy" is that companies are bound by their data privacy and data security promises.[307] The FTC has taken the position that companies act deceptively when they gather, use, or disclose personal information in a way that contradicts their posted privacy policy or other statements,[308] or when they fail to adequately protect personal information from unauthorized access despite promises that that they would do so.[309] In addition to broken promises, the FTC has alleged that companies act deceptively when they make false representations in order to induce disclosure of personal information.[310] For example, in *FTC v. Sun Spectrum Commc'ns Org., Inc.*, the FTC alleged that several telemarketers acted "deceptively" by misrepresenting themselves as a credit card company and

[302] Solove & Harzog, *supra* note 60, at 620–621 ("[F]or Section 5 enforcement . . . the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective. The FTC must rely heavily on its settlements to signal the basic rules that it wants companies to follow.").

[303] FED. TRADE COMM'N, REPORT ON PRIVACY & DATA SECURITY 2 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf ("The Commission has brought over 500 enforcement actions protecting the privacy of consumer information.").

[304] Solove & Hartzog, *supra* note 60, at 610 ("[V]irtually every [privacy-related] complaint has either been dropped or settled.").

[305] *Id.* at 621 ("[FTC settlements] have a kind of precedential value, and they serve as a useful way to predict future FTC activity.").

[306] *Id.* at 619 ("Although the FTC's privacy cases nearly all consist of complaints and settlements, they are in many respects the functional equivalent of common law."). FTC commissioners have similarly referred to the FTC's enforcement as a common law approach. *See, e.g.*, Justin Hurwitz, *Data Security and the FTC's Uncommon Law*, 101 IOWA L. REV. 955, 966–967 (2016) (describing various statements from FTC commissioners regarding the FTC's common law approach).

[307] *Id.* at 628 ("Much of the FTC's privacy jurisprudence is based on a deception theory of broken promises.").

[308] *See, e.g.*, Complaint, In the Matter of Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) (alleging Myspace provided advertisers with users' personally identifiable information, despite promises in its privacy policy that it would not share such information); Complaint, In the Matter of Liberty Financial Companies, Inc., No. C-3891 (F.T.C. Aug. 12, 1999); Press Release, Fed. Trade Comm'n, Online Auction Site Settles FTC Privacy Charges (Jan. 6, 2000), https://www.ftc.gov/news-events/press-releases/2000/01/online-auction-site-settles-ftc-privacy-charges (describing settlement of allegations that an online operator used personal identifying information to generate spam, despite agreeing to a privacy policy stating it would only gather personal identifying information from users for certain authorized purposes).

[309] *See, e.g.*, Complaint, Fed. Trade Comm'n v. Ruby Corp., No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016) (alleging that operators of dating site AshleyMadison.com deceived consumers by assuring them personal information would be protected but failing to implement the necessary security to prevent a data breach).

[310] Solove & Hartzog, *supra* note 60, at 630 ("The FTC has also developed a general theory of deception in its complaints based upon a company's deceptive actions taken in order to induce disclosure of personal information.").

requesting personal information from individuals, ostensibly for the purpose of providing non-existent credit cards to the individuals.[311] The FTC has further maintained that companies act deceptively when their privacy policies or other statements provide insufficient notice of their privacy practices. For instance, in *In the Matter of Sears Holdings Management Co.*, the FTC alleged that Sears acted deceptively by failing to disclose the extent to which downloadable software would monitor users' internet activity, merely telling users that it would track their "online browsing."[312]

Along with "deceptive claims," the FTC has also alleged that certain data privacy or data security practices may be "unfair." Specifically, the FTC has maintained that it is unfair for a company to retroactively apply a materially revised privacy policy to personal data that it collected under a previous policy.[313] The FTC has also taken the position that certain default privacy settings are unfair. In the case *FTC v. Frostwire*, for example, the FTC alleged that a peer-to-peer file sharing application had unfair privacy settings because, immediately upon installation, the application would share the personal files stored on users' devices unless the users went through a burdensome process of unchecking many pre-checked boxes.[314] With respect to data security, the FTC has more recently maintained that a company's failure to safeguard personal data may be "unfair," even if the company did not contradict its privacy policy or other statements.[315] While at least one court has agreed that such conduct may be "unfair" under the FTC Act,[316] a recent U.S. Court of Appeals for the Eleventh Circuit[317] case, *LabMD v. FTC*, suggests that any FTC cease and desist order based on a company's "unfair" data security measures must allege specific data failures and specific remedies.[318] In *LabMD*, the court noted that the FTC's order "contain[ed] no prohibitions" but "command[ed] [the company] to overhaul and replace its data-security program

[311] Complaint, Fed. Trade Comm'n v. Sun Spectrum Commc'ns Org., Inc., No. 03-8110 (S.D.N.Y. Dec. 2, 2003); Press Release, Fed. Trade Comm'n, U.S. and Canadian Telemarketers Pay $415,000 to Settle FTC Charges (Oct. 24, 2005), https://www.ftc.gov/news-events/press-releases/2005/10/us-and-canadian-telemarketers-pay-415000-settle-ftc-charges.

[312] *See, e.g.*, Complaint, In the Matter of Sears Holdings Management Co., No. C-4264 (F.T.C. Aug. 31, 2009), (alleging that Sears failed to disclose the extent to which downloadable software would monitor users' internet activity, merely telling users that it would track their "online browsing"); *see also* Complaint, In the Matter of Lenovo, No. C-4636 (F.T.C. Dec. 20, 2017) (alleging that Lenovo acted deceptively by installing third-party software on consumers' computers that collected extensive personal data and simply telling consumers that the software would let them "discover visually similar products and best prices while [they] shop").

[313] *See, e.g.*, Complaint at 9, In the Matter of Facebook, FTC File No. 0923184 (F.T.C. Nov. 9, 2011) (alleging that Facebook acted unfairly by materially changing its privacy policy regarding what information users could keep private and retroactively applying these changes to previously collected information); Complaint at 5, *In re* Gateway Learning Corp., FTC File No. 0423047 (F.T.C. Sept. 17, 2004) (alleging that Gateway Learning acted unfairly by changing its privacy policy to allow it to share personal information with third parties and retroactively applying this new policy to previously collected data).

[314] Complaint, Fed. Trade Comm'n v. Frostwire LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.

[315] *See, e.g.*, Complaint at 8, United States v. Rental Research Services, Inc., No. 0:09-cv-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf (alleging that defendant's failure to employ reasonable and appropriate security measures to protect consumers' personal information was an unfair act or practice).

[316] Fed. Trade Comm'n v. Wyndham, 10 F. Supp. 3d 602 (D.N.J. 2014) (declining to dismiss the FTC's action alleging that defendant violated both the unfairness and deceptiveness prongs of Section 5(a) of the FTC Act by failing to maintain reasonable and appropriate data security for consumers' personal information), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[317] This report references a significant number of decisions by federal appellate courts of various regional circuits. For purposes of brevity, references to a particular circuit in the body of this report (e.g., the Eleventh Circuit) refer to the U.S. Court of Appeals for that particular circuit.

[318] 894 F.3d 1221.

to meet an indeterminable standard of reasonableness."[319] The court concluded that such an order was unenforceable, reasoning that the order "effectually charge[d] the district court [enforcing the order] with managing the overhaul."[320] The court further suggested that penalizing a company for failing to comply with an imprecise standard "may constitute a denial of due process" because it would not give the company fair notice of the prohibited conduct.[321] Ultimately, while *LabMD* did not decide whether inadequate data security measures may be "unfair" under the FTC Act,[322] the decision is nevertheless a potentially significant limitation on the FTC's ability to remedy such violations of the statute.

LabMD is also a notable case because it adds to the relatively sparse case law on the FTC Act's "unfair or deceptive" prohibition. As mentioned, the large majority of the FTC enforcement actions are settled, with parties entering into consent decrees.[323] To the extent FTC allegations are contested, the FTC may either commence administrative enforcement proceedings or civil litigation against alleged violators.[324] In an administrative enforcement proceeding, an Administrative Law Judge (ALJ) hears the FTC's complaint and may issue a cease and desist order prohibiting the respondent from engaging in wrongful conduct.[325] In civil litigation, the FTC may seek equitable relief, such as injunctions or disgorgement,[326] when a party "is violating, or is about to violate," the FTC Act.[327] The FTC may only seek civil penalties, however, if the party has violated a cease and desist order, consent decree, or a TRR.[328] The FTC Act does not

[319] *Id.* at 1236.

[320] *Id.* at 1237.

[321] *Id.* at 1235–1236.

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

[323] Solove & Hartzog, *supra* note 60, at 610 ("[V]irtually every [privacy-related] complaint has either been dropped or settled.").

[324] 15 U.S.C. §§ 45(a)(2), 45(b), 53(b).

[325] *Id.* § 45(b); *see also*, FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority ("Upon conclusion of the hearing, the ALJ issues an 'initial decision' setting forth his findings of fact and conclusions of law, and recommending either entry of an order to cease and deist or dismissal of the complaint.").

[326] Civil actions are brought under Section 13(b) of the FTC Act, codified at 15 U.S.C. § 53(b). Although Section 13(b) explicitly references only injunctive relief, courts have held that the FTC may seek all forms of equitable remedies in civil actions brought under the provision, including injunctive relief and disgorgement of profits. *See, e.g.*, FTC v. Sw. Sunsites, Inc., 665 F.2d 711, 717–18 (5th Cir. 1982) ("Although the plain language of the statute speaks only of enjoining an allegedly unlawful act of practice . . . . [t]hese cases make indisputably clear that a grant of jurisdiction such as that contained in Section 13(b) carries with it the authorization for the district court to exercise the full range of equitable remedies traditionally available to it.").

[327] In light of a recent decision by the Third Circuit, the FTC may be unable to bring civil suits based on past UDAP violations that are no longer ongoing. In *Fed Trade Comm'n v. Shire ViroPharma,* the Third Circuit held that, in civil actions under Section 13(b) of the FTC Act, the FTC must show the defendant "is violating, or is about to violate" the law and that this standard requires more than simply showing that the conduct is "likely to recur." No. 1-17-cv-00131, 2019 WL 908577, at *9 (3d Cir. Feb. 25, 2019) ("In short, we reject the FTC's contention that Section 13(b)'s 'is violating' or 'is about to violate' language can be satisfied by showing a violation in the distant past and a vague and generalized likelihood of recurrent conduct. Instead, 'is' or 'is about to violate' means what it says—the FTC must make a showing that a defendant is violating or is about to violate the law."). For additional background on this issue, see CRS Legal Sidebar LSB10232, *UPDATE: Will the FTC Need to Rethink its Enforcement Playbook? Third Circuit Considers FTC's Ability to Sue Based on Past Conduct*, by Chris D. Linebaugh.

[328] 15 U.S.C. §§ 45(l)–(m).

provide a private right of action,[329] and it does not impose any criminal penalties for violations of Section 5.[330]

Consumer Financial Protection Act (CFPA)

Similar to the FTC Act, the CFPA prohibits covered entities from engaging in certain unfair, deceptive, or abusive acts. Enacted in 2010 as Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPA created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System.[331] The Act gives the CFPB certain "organic" authorities, including the authority to take any action to prevent any "covered person" from "committing or engaging in an unfair, deceptive, or abusive act or practice" (UDAAP) in connection with offering or providing a "consumer financial product or service."[332]

The CFPB's UDAAP authority under the CFPA is very similar to the FTC's UDAP authority under the FTC Act; indeed, the CFPA contains the same definition of "unfair" as in the FTC Act,[333] and the CFPB has adopted the FTC's definition of "deceptive" acts or practices.[334] However, there are several important differences. First, the CFPA's UDAAP prohibition includes "abusive" practices, as well as unfair or deceptive ones. An act or practice is abusive if it either (1) "materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service" or (2) "takes unreasonable advantage of" a consumer's (a) lack of understanding, (b) inability to protect her own interest in selecting or using a consumer financial product or service, or (c) reasonable reliance on a covered person to act in her interest.[335] While abusive conduct may also be unfair or deceptive, abusiveness is a separate standard that may cover additional conduct.[336] Second, the CFPA prohibits UDAAPs only in connection with offering or providing a "consumer financial product or service."[337] A product or service meets this standard if it is one of the specific financial product or services listed in the CFPA[338] and is offered or provided to consumers primarily for personal, family, or household purposes.[339] Lastly, the CFPA applies only to "covered persons" or "service providers."[340] The statute defines

[329] *See, e.g.*, Wisniewski v. Rodale, Inc., 406 F. Supp. 2d 550, 557 (E.D.Pa. 2005) ("[N]o private right of action exists under the FTC Act.").

[330] *See* 15 U.S.C. §§ 45, 50.

[331] Consumer Financial Protection Act of 2010, Pub. L. No. 111-203, tit. X, 124 Stat. 1376, 1955–2113 (2010) (codified at 12 U.S.C. §§ 5491–5603).

[332] 12 U.S.C. § 5531(a).

[333] *See id.* § 5531(c); 15 U.S.C. § 45(n).

[334] CONSUMER FIN. PROT. BUREAU, SUPERVISION AND EXAMINATIONS MANUAL, UDAAP Section at 5, n. 10 (2012), https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102012_cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures.pdf [hereinafter EXAMINATION MANUAL] (citing to the FTC Policy Statement on Deception and stating that "[e]xaminers should be informed by the FTC's standard for deception").

[335] 12 U.S.C. § 5531(d).

[336] EXAMINATION MANUAL, *supra* note 334, 13-99 ("Although abusive acts also may be unfair or deceptive, examiners should be aware that the legal standards for abusive, unfair, and deceptive each are separate.").

[337] 12 U.S.C. § 5531(a).

[338] The CFPA contains an extensive list of activities constituting "financial products or services," such as extending credit, providing payments or financial data processing products or services, and debt collection. *Id.* § 5481(15).

[339] *Id.* § 5481(5)(A). A product or service will also meet this standard if it involves a certain subset of the defined "financial products or services" and is "delivered, offered, or provided in connection with a consumer financial product or service." *Id.* § 5481(5)(B).

[340] *Id.*

"covered persons" as persons who offer or provide a consumer financial product or service, and it defines "service providers" as those who provide a "material service" to a "covered person" in connection with offering or providing a consumer financial product or service.[341]

As some commentators have noted, the CFPB could follow in the FTC's footsteps and use its UDAAP authority to regulate data protection.[342] However, the CFPB has generally been inactive in the data privacy and security space. Indeed, to date, it has brought only one such enforcement action, which involved allegations that an online payment platform, Dwolla, Inc., made deceptive statements regarding its data security practices and the safety of its online payments system.[343] To the extent it does use its authority, the CFPB has some powerful procedural advantages in comparison with the FTC. In particular, the CFPB can enact rules identifying and prohibiting particular UDAAP violations through the standard APA rulemaking process, whereas the FTC must follow the more burdensome Magnuson-Moss rulemaking procedures.[344] Regarding enforcement, the CFPA authorizes the CFPB to bring civil or administrative enforcement actions against entities engaging in UDAAPs.[345] Unlike the FTC, the CFPB can seek civil penalties in all such enforcement actions, as well as equitable relief such as disgorgement or injunctions.[346] However, as with the FTC Act, the CFPA does not provide a private right of action that would allow adversely affected individuals to sue companies violating the Act.[347] The statute also does not impose any criminal penalties for UDAAP violations.[348]

State Data Protection Law

Adding to the complex federal patchwork of data protection statutes are the laws of the fifty states. First and foremost, major regulators of privacy and data protection in the states include the courts, via tort and contract law.[349] With respect to tort law, in addition to the "privacy" causes of action that developed at the state level during the early 20th century (discussed above),[350] negligence and other state tort law claims serve as a means to regulate businesses that are injured from data security issues or otherwise fail to protect their customers from foreseeable harm.[351]

---

[341] *Id.* § 5481(6).

[342] *See, e.g.*, Thomas Pahl, *The CFPB is a Sleeping Giant on Data Security. Let's Not Wake It.*, THE HILL (Dec. 28, 2016), https://thehill.com/blogs/pundits-blog/finance/311974-the-cfpb-is-a-sleeping-giant-on-data-security-lets-not-wake-it; Joanathan G. Cedarbaum, *The Consumer Financial Protection Bureau as a Privacy & Data Security Regulator*, 17 FINTECH L. REPT. 1 (2014).

[343] Press Release, Consumer Fin. Prot. Bureau, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/; Pahl, *supra* note 342 ("[T]he CFPB's sole foray into data security has been a single case earlier this year alleging that Dwola, an online payment platform, violated the Dodd-Frank Act by making deceptive claims to consumers about its data security practices and the safety of its online payment system.").

[344] *See supra* § Federal Trade Commission Act (FTC Act).

[345] 12 U.S.C. §§ 5563–5564.

[346] *Id.* § 5565. In contrast, the FTC can seek penalties only when an entity violates a cease and desist order, consent decree, or TRR. *See infra* § Federal Trade Commission Act (FTC Act).

[347] *See, e.g.*, Johnson v. J.P. Morgan Chase Nat. Corporate Services, Inc., No. 3:13-CV-678, 2014 WL 4384023, at *5 (W.D.N.C. Aug. 5, 2014) ("[T]here is no private right of action under the CFPA.").

[348] *See* 12 U.S.C. §§ 5531, 5565.

[349] *See, e.g.*, SOLOVE AND SCHWARTZ, *supra* note 50 at 821–842.

[350] *See supra* § Origins of American Privacy Protection.

[351] *See, e.g.*, Resnick v. AvMed, Inc, 693 F.3d 1317, 1327–28 (11th Cir. 2012) (concluding that plaintiffs had adequately pleaded claims for negligence, as well as other state law claims, in suit against health plan operator relating to identity theft incidents); Anderson v. Hannaford Bros. Co., 659 F.3d 151, 161–62 (1st Cir. 2011) (concluding that

Contracts, implied contracts, and other commercial causes of action can also form important bulwarks for privacy.[352] The common law, however, is not perfect: it is subject to variability from state to state, and within states, from judge to judge and jury to jury.

In addition to the common law, most states have their own statutory framework which may affect data protection and the use of data by private entities. For example, many states have a consumer protection law, sometimes prohibiting unfair or deceptive practices, often referred to as "little FTC Acts."[353] These laws, like the FTC Act, are increasingly being used to address privacy matters.[354] In addition, each state[355] has passed a data breach response law, requiring some form of response or imposing liability on companies in the event of a breach of their data security. [356]

While an examination of every state data security law is beyond the scope of this report,[357] at least one state has undertaken a general and ambitious effort to regulate data security. Specifically, the California Consumer Privacy Act (CCPA), enacted in 2018, has captured significant attention.[358]

---

plaintiffs had adequately stated claim for negligence against grocer when payment data was allegedly stolen by third-party wrongdoer); Brush v. Miami Beach Healthcare Group Ltd., 238 F. Supp. 3d 1359, 1366 (S.D. Fla. 2017) (concluding that plaintiff had adequately pleaded claim for negligence for data breach that allegedly caused plaintiff's identity to be stolen); Bohannan v. Innovak Int'l, Inc., 318 F.R.D. 525, 530 (M.D. Ala. 2016) (concluding that plaintiffs had adequately pleaded claim for negligence against information technology company that allegedly suffered data breach and failed to inform its customers); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (allowing some of the plaintiffs' negligence claim against retail store chain for data breach to go forward). *But see* USAA Federal Savings Bank v. PLS Financial Services, Inc., 260 F. Supp. 3d 965, 969–70 (N.D. Ill. 2017) (holding that Illinois law did not recognize a common law duty to safeguard personal information); *Target*, 66 F. Supp. 3d at 1176 (concluding that "economic loss rule" barred negligence claims under the laws of several states); SOLOVE AND SCHWARTZ, *supra* note 50 at 822-29 (discussing obstacles to using tort law to remedy privacy harms).

[352] *See, e.g.*, Hutton v. National Board of Examiners in Optometry, Inc., 892 F.3d 613, 623–24 (4th Cir. 2018) (concluding that plaintiffs had standing to assert claims arising out of breach of personal information database, including breach of contract); Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1246–48 (D. Colo. 2018) (concluding that plaintiffs had adequately pleaded claim for breach of implied contract in case involving data breach and theft of personally identifiable information); Google, 58 F. Supp. 3d at 986–87 (N.D. Cal. 2014) (concluding that plaintiffs had adequately stated a claim for breach of contract against Google for Google's alleged misrepresentations in their privacy policies). *See also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1057–61 (2000) (discussing how, in general, contract law involving promises not to reveal information can be used to protect privacy rights).

[353] *See* Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little-FTC Acts?*, 63 FLA. L. REV. 163, 165 (2011).

[354] Cary Silverman & Jonathan L. Wilson, *State Attorney General Enforcement of Unfair or Deceptive Trade Acts and Practices Laws: Emerging Concerns and Solutions*, 65 KAN. L. REV. 209, 257 (2016) ("Historically, the FTC has taken the lead in privacy law enforcement. Now, with increased storage of consumer data and a rise in security breaches, state attorneys general and class action lawyers are increasingly bringing actions under state UDAP laws and other legal theories.").

[355] Hunton Andrews Kurth, *Alabama Becomes Final State to Enact Data Breach Notification Law*, PRIVACY & INFO. SEC. LAW BLOG (Apr. 3, 2018), https://www.huntonprivacyblog.com/2018/04/03/alabama-becomes-final-state-enact-data-breach-notification-law/; *see also* CRS Legal Sidebar LSB10232, *UPDATE: Will the FTC Need to Rethink its Enforcement Playbook? Third Circuit Considers FTC's Ability to Sue Based on Past Conduct*, by Chris D. Linebaugh.

[356] Silverman & Wilson, *supra* note 354 at 257–59 (describing various recent state attorney general actions in the privacy sphere); National Conference of State Legislatures, *State Laws Related to Internet Privacy* (Sept. 24, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (collecting various state laws impacting areas of privacy and data protection). These laws, however, are not uniform—exacerbating the sense that data protection law is a patchwork at best.

[357] For more information on state laws, see National Conference of State Legislatures, *supra* note 356.

[358] 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375). See also CRS Legal Sidebar LSB10213, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, by Wilson C. Freeman.

The California Consumer Privacy Act (CCPA)

The CCPA's Scope

Unlike the federal patchwork provisions, neither the method of data collection nor the industry that the business operates in limits the potential application of the CCPA. Instead, the CCPA applies to any company that collects the personal information of Californians, is for-profit, does business in California, and satisfies a basic set of thresholds.[359] Analysts have suggested that these thresholds are low enough that the law could reach a considerable number of even "relatively small" businesses with websites accessible in California.[360]

The CCPA also does not distinguish between the sources of the data that comes within its scope. Rather, the CCPA regulates all "personal information," which, by the CCPA's definition, covers nearly any information a business would collect from a consumer.[361] The law does not require the presence of any individual identifier, such as a name or address, for data to fall within the meaning of personal information. Rather, the CCPA broadly defines personal information as "information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[362] Following this definition, the CCPA provides some telling illustrations of what constitutes personal information, including any "electronic network activity [such as] browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement" and "inferences drawn from any of" this information.[363]

The CCPA's Provisions and Requirements

The CCPA provides consumers with three main "rights." The first of these is a "*right to know*" the information that businesses have collected or sold about them. This right requires that businesses must, in advance of any collection, "inform [by mail or electronically] consumers as to the categories of personal information to be collected and the purposes" to which the information will be put.[364] Second, the CCPA provides consumers with the "*right to opt out*" of the sale of a consumer's information. Under the new law, businesses must inform consumers of this right, and if a consumer so affirmatively opts out, the business cannot again sell the consumer's information

[359] CAL CIV. CODE § 1798.140(c)(1) (defining "business" as any company with more than $25 million in annual gross revenues, or that engages in the buying, selling, or receipt of the personal information of 50,000 or more California residents, or that derives more than 50% of its annual revenues from the sale of California residents' personal information).

[360] Christopher A. Ott, *Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018*, PRIVACY & SECURITY LAW BLOG (Aug. 6, 2018), https://www.privsecblog.com/2018/08/articles/marketing-and-consumer-privacy/qa-privacy-and-security-partner-christopher-ott-on-the-california-consumer-privacy-act-of-2018/.

[361] *Id.* ("The CCPA applies to broadly defined personal information of California residents collected by businesses, regardless of how the collection is done, or the type of industry in which the business operates.").

[362] CAL CIV. CODE § 1798.140(O)(1).

[363] *Id.* § 1798.140(O)(1)(A)–(K). The CCPA does exempt some categories of information from its definition of personal information. For example, personal information generally does not include "publicly available information," meaning information lawfully made available from government records. *Id.* § 1798.140(o)(2). Similarly, the CCPA does not restrict a business's ability to collect "deidentified" or "aggregate consumer information," generally meaning information that cannot be linked in any way with particular consumers. *Id.* § 1798.145(a)(5) ("The obligations imposed on businesses by this title shall not restrict a business's ability to . . . . Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.").

[364] *See id.* § 1798.100.

unless the consumer subsequently provides the business express authorization.[365] Finally, the CCPA gives consumers the right, in certain circumstances, to request that a business delete any information collected about the consumer (i.e., "*right to delete*"). Under the law, a business that receives such a request must delete the information collected and direct its "service providers" to do the same.[366]

Remedies, Liabilities, and Fines

The primary means to enforce the CCPA are actions brought by the California Attorney General.[367] According to the statute, businesses that fail to provide the protections required by the CCPA and fail to cure those violations within 30 days are liable for civil penalties of up to $7,500 per violation.[368] Penalties or settlements collected under the CCPA are to be deposited with the newly created Consumer Privacy Fund, the funds for which are used only to offset costs incurred in connection with the administration of the CCPA.[369] While the CCPA provides for a private cause of action, allowing for individual and class action lawsuits against businesses, this cause of action is only available in the case of a consumer whose "nonencrypted or nonredacted personal information" is subject to "unauthorized access and exfiltration, theft, or disclosure" as a result of a failure to "implement and maintain reasonable security procedures."[370] Further, such actions can be brought only if a consumer provides a business with 30 days' written notice and provides the business with opportunity to cure the violation, unless the consumer suffered actual pecuniary damages.[371] The statute does not specify how a business could "cure" a violation of this type. Consumers may obtain damages under this section of no less than $100 and no more than $750 "per incident," or actual damages, whichever is greater, as well as injunctive relief.[372]

The CCPA and the 116th Congress

Statements by some Members of Congress during Congressional hearings have already noted the CCPA's likely importance to future federal legislative efforts.[373] Further, some outside commentators have argued explicitly that the CCPA should be preempted by a future federal law.[374] These statements may be motivated by the likely fact that, if left intact, the California law

[365] *See generally id.* § 1798.120.

[366] *See id.* § 1798.105.

[367] *See id.* § 1798.115.

[368] *Id.* § 1798.115(b).

[369] *Id.* § 1798.115(c).

[370] *Id.* § 1798.150(a)(1).

[371] *Id.* § 1798.150(b)(1).

[372] *Id.* §§ 1798.150(a)(1)(A)–(B).

[373] *See Examining Safeguards for Consumer Data Privacy Before the S. Comm. on Commerce, Science & Transp.*, 115th Cong. (2018) (statement of Sen. John Thune) ("Like GDPR, the new California law—which will take effect on January 1, 2020—contains many privacy mandates and severe penalties for violators. These developments have all combined to put the issue of consumer data privacy squarely on Congress' doorstep. The question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape that law should take.").

[374] *See, e.g.*, Jessica Guynn, *Amazon, AT&T, Google Push Congress to Pass Online Privacy Bill to Preempt Stronger California Law*, USA TODAY (Sept. 26, 2018), https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/; Harper Neidig, *Chamber of Commerce calls for Congress to Block State Privacy Laws*, THE HILL (Sept. 9, 2018), https://thehill.com/policy/technology/405433-chamber-of-commerce-calls-for-congress-to-block-state-privacy-laws. *See also infra* § Preemption.

could shape industry and consumer concerns both inside and outside California. First, the law is likely to be the "first in a long line of similar pieces of legislation," all of which may model themselves after the CCPA, or will have to respond to its impact.[375] Second, even though the statute is the product of a single state, its broad jurisdictional reach would bring companies throughout the United States and from around the world into its sweep.[376] These factors combined are likely to make the CCPA important to federal legislators. Furthermore, some of the provisions of the California law could form a model for future federal regulation—although along those lines, another potential model it has to compete with is Europe's GDPR.[377]

The EU's General Data Protection Regulation (GDPR)

In addition to U.S. states like California, some foreign nations have enacted comprehensive data protection legislation.[378] The EU, in particular, has long applied a more wide-ranging data protection regulatory scheme.[379] Whereas privacy principles in the U.S. Constitution focus on government intrusions into private life[380] and U.S. data privacy statutes generally are sector-specific,[381] European privacy regulations have generally concerned *any* entity's accumulation of large amounts of data.[382] As a result, foundational EU treaties provide individuals with a general right to "protection of personal data" from all potential interferences.[383] The objective of the EU's most recent data privacy legislation—the GDPR—is to safeguard this right to personal data protection, while ensuring that data moves freely within the EU.[384]

[375] *See* Forbes Technology Council, *How Will California's Consumer Privacy Law Impact the Data Privacy Landscape*, FORBES (AUG. 20, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape.

[376] *See, e.g.*, *Is California's Consumer Privacy Act of 2018 Going to be GDPR Version 2?*, NAT'L L. REV. (Sept. 6, 2018), https://www.natlawreview.com/article/california-s-consumer-privacy-act-2018-going-to-be-gdpr-version-2.

[377] *See* Covington & Burling LLP, *Senate Examines Potential for Federal Data Privacy Legislation*, INSIDE PRIVACY, October 1, 2018, https://www.insideprivacy.com/uncategorized/senate-examines-potential-for-federal-data-privacy-legislation/ (discussing legislative responses and legislator views on using the CCPA and the GDPR as a model for future federal legislation).

[378] For a survey of data protection legislation in the EU and in "twelve individual countries with highly developed digital infrastructures," see LAW LIBRARY OF CONGRESS, ONLINE PRIVACY LAW (2017 UPDATE) (Dec. 2017), https://www.loc.gov/law/help/online-privacy-law/online-privacy-law-2017.pdf. *See also infra* note 490 (discussing countries that have modeled data privacy legislation on the GDPR).

[379] For additional background on EU data protection initiatives and their implications for Congress, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[380] *See supra* § Constitutional Protections and the Right to Privacy.

[381] *See supra* § Federal Data Protection Law.

[382] *See*, *e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1219 (2004); Jeffrey Rosen, *Continental Divide*, LEGAL AFFAIRS, Sept.–Oct. 2004, at 49–50.

[383] Consolidated Version of the Treaty on the Functioning of the European Union, art. 16(1), Oct. 26, 2012, 2012 O.J. C 326/47 [hereinafter TFEU] ("Everyone has the right to the protection of personal data concerning them."); Charter of Fundamental Rights of the European Union, art. 8, Dec. 18, 2000, 2000 O.J. C 364/1 [hereinafter EU Human Rights Charter] ("Everyone has the right to the protection of personal data concerning him or her.").

[384] GDPR, art. 1.

European Data Privacy Laws and the Lead-Up to the GDPR

Beginning in the 1970s, individual European countries began enacting broad, omnibus national statutes concerning data protection, privacy, and information practices.[385] Although these domestic laws shared certain features, their differing data privacy and protection standards occasionally impeded the free flow of information between European countries.[386] As a consequence, the EU attempted to harmonize its various national privacy laws by adopting an EU-wide data privacy and protection initiative—the 1995 Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive).[387]

While the Data Protection Directive applied on an EU-wide basis, EU law authorized each member-nation to implement the directive's requirements into the country's national law.[388] By 2012, the European Commission—the executive body of the EU[389]—came to view differing implementations of the Data Protection Directive at the national level as problematic.[390] The Commission concluded that a single regulation should be developed in order to eliminate the fragmentation and administrative burdens created by the directive-based system.[391] The Commission also sought to bring EU law up to date with developments in technology and globalization that changed the way data is collected, accessed, and used.[392] In pursuit of these goals, the EU developed and adopted the GDPR, which replaced the 1995 Data Protection Directive and went into effect on May 25, 2018.[393]

---

[385] Sweden enacted the first national statute aimed at data protection in 1973. IAN J. LLOYD, INFORMATION TECHNOLOGY LAW 27 (7th ed. 2014). Similar omnibus data protection laws soon followed in Germany, France, Spain, the United Kingdom and the Netherlands. Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/ec: Does U.S. Data Protection Meet This Standard?,* 21 FORDHAM INT'L L.J. 932, 1018 (1998).

[386] *See* Murray, *supra* note 385, at 934–35.

[387] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 1995 O.J. 95 (L281) [hereinafter Data Protection Directive].

[388] Among other legal actions authorized under the EU system, EU-wide legislative acts generally take one of two forms: *directives* or *regulations*. *See*, *e.g.*, ALEX SAMUEL, 2 DATA SECURITY & PRIVACY LAW § 11:1 (2018); Nadia E. Nedzel, *The International Rule of Law and Economic Development*, 17 WASH. U. GLOBAL STUD. L. REV. 447, 466 (2018). Directives apply to all EU countries, but EU law authorizes each nation to determine the "form and methods" by which the directive is implemented into its national law. TFEU, *supra* note 383, art. 288. Regulations, by contrast, are binding as written and apply directly to all member states. TFEU, *supra* note 383, art. 288. Because the 1995 Data Protection Directive was a directive rather than a regulation, EU member states implemented its requirements somewhat differently. European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale_en [hereinafter European Commission Press Release IP/12/46] ("EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement.").

[389] For further background on the division of authority between EU institutions, see CRS Report RS21372, *The European Union: Questions and Answers*, by Kristin Archick.

[390] *See* European Commission Press Release IP/12/46, *supra*, note 388, ("Member States have implemented the 1995 rules differently, resulting in divergences in enforcement.").

[391] *Id.* ("A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.").

[392] *Id. See also* GDPR, recital 10 ("The objectives and principles of [the 1995 Data Protection Directive] remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union . . .").

[393] GDPR, arts. 94, 99(2).

GDPR Provisions and Requirements

Scope and Territorial Reach

The GDPR regulates the *processing* of *personal data* that meet its territoriality requirements, discussed below.[394] Processing includes collection, use, storage, organization, disclosure or any other operation or set of operations performed on personal data,[395] unless an exception applies.[396] Personal data is defined as any information relating to an identified or identifiable person, [397] and it can include names, identification numbers, location data, IP addresses, cookies, and any other information through which an individual can be directly or indirectly identified.[398] The GDPR applies different requirements for *controllers* and *processors* of personal data.[399] In general, a controller determines the purposes and means of processing personal data,[400] and a processor is responsible for processing data on behalf of a controller.[401]

From a territorial perspective, the GDPR applies to organizations that have an "establishment" in the EU and that process personal data in the context of the activities of that establishment.[402] The GDPR does not define "establishment," but states that it "implies the effective and real exercise of activity through stable arrangements."[403] In a pre-GDPR case, the Court of Justice of the European Union stated that the concept of establishment under the 1995 Data Protection Directive extended "to any real and effective activity—even a minimal one—exercised through stable arrangements."[404] Entities that meet the establishment requirement are subject to the GDPR even if their data processing activities take place outside the EU.[405] The GDPR also applies to non-EU-established entities that offer goods or services to individuals in the EU or monitor

[394] *Id.* art. 3.

[395] *Id.* art. 4(2).

[396] The GDPR does not apply to the processing of personal data: (1) in the course of an activity that "falls outside the scope of [EU] law"; (2) by EU nations carrying out certain EU-wide foreign policy and national security objectives; (3) by an individual in the course of a purely personal or household activity; and (4) by "competent authorities" conducting criminal investigations and prosecutions, including safeguarding against preventing threats to public security. *Id.* art. 2(2).

[397] *Id.* art. 4(1).

[398] *See* U.K. INFO. COMM'RS OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) 10 (2018) [hereinafter ICO GUIDE].

[399] The GDPR imposes significantly greater obligations on data controllers than data processors. For example, controllers are responsible for obtaining consent from individuals, providing access to data processing information, and responding to objections to data processing and requests for rectification, erasure, restriction, and receipt of personal data. GDPR, arts. 7, 12-21.

[400] *Id.* art. 4(7).

[401] *Id.* art. 4(2).

[402] GDPR, art. 3(1).

[403] *Id.* recital 22.

[404] Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14 ¶ 31, http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.381.01.0006.01.ENG.

[405] GDPR, art. 3(1) ("This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.").

individuals' behavior in the EU.[406] Because many businesses with an online presence offer goods and services to EU individuals, the GDPR applies to many businesses outside the EU.[407]

Key Principles

The GDPR lays out seven guiding principles for the processing of personal data. While these principles are not "hard and fast rules" themselves, they inform the interpretation of the GDPR and its more concrete requirements, discussed below.[408]

1. **Lawfulness, fairness, and transparency**
   Personal data must be processed lawfully, fairly, and in a transparent manner in relation to individuals.
2. **Purpose limitation**
   Personal data should be collected only for specified, explicit, and legitimate purposes, but processing for archiving purposes in the public interest, scientific or historical research, or statistical purposes may comply with this principle.
3. **Data minimization**
   Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.
4. **Accuracy**
   Personal data held by processors and controllers should be accurate, up-to-date, and erased or rectified without delay.
5. **Storage limitation**
   Personal data must be kept in a form that permits identification of the data subjects for no longer than is necessary, but it may be archived when in the public interest or for scientific and historical research or statistical purposes.
6. **Integrity and confidentiality (i.e., data security)**
   Personal data must be processed in a manner that ensures security and protects against unauthorized processing, accidental loss, destruction, or damage.
7. **Accountability**
   Data controllers must be responsible for and able to demonstrate compliance with the GDPR's principles.[409]

Bases for Processing and Consent Requirements

The GDPR requires data controllers and processors to have a lawful basis to process personal data.[410] The regulation delineates six possible legal bases: (1) consent; (2) performance of contract; (3) compliance with a legal obligations;[411] (4) protection of the "vital interests" (i.e., the life) of the data subject or another individual;[412] (5) tasks carried out in the public interest (e.g.,

[406] *Id.* art. 3(2).

[407] SAMUEL, *supra* note 388, § 11.2. Entitles with no EU establishment that are subject to the GDPR must designate a representative within the Union. GDPR, art 27.

[408] ICO GUIDE, *supra* note 398, at 16.

[409] GDPR, art. 5.

[410] *Id.* art. 6.

[411] Examples of circumstances when compliance with a legal obligation could serve as a basis for processing include a financial institution reporting suspicious activity as mandated by law or a court order requiring the processing of personal data. ICO GUIDE, *supra* note 398, at 69.

[412] GDPR, recital 46. The vital interests basis for processing may arise, for example, when data processing is necessary

by a government entity);[413] and (6) the "legitimate interests"[414] of the controller or a third party, unless the fundamental rights and freedom of the data subject override those interests.[415] Commentators describe the "legitimate interests" category as the most flexible[416] and as the potential basis for a host of common activities, such as processing carried out in the normal course of business,[417] provided that the processing is not unethical, unlawful, or otherwise illegitimate.[418] When data processing is premised on consent, the consent must be freely given, specific, informed, and unambiguous,[419] and it can be withdrawn at any time.[420] Additional consent requirements and restrictions apply to especially sensitive data, such as children's information and data that reveals ethnic origins, political opinions, religious beliefs, union status, sexual orientation, health information, and criminal histories.[421]

Individual Rights and Corresponding Obligations

The GDPR provides a series of rights to individuals and corresponding obligations for data controllers, unless an exception applies.[422]

for humanitarian purposes such as monitoring for epidemics or in responding to a natural disaster. *Id.*

[413] The public task basis applies when, for example, a governmental body exercises its official authority or performs a task that has a legal basis. ICO GUIDE, *supra* note 398, at 75.

[414] Legitimate interests for data processing include, among other things, processing for direct marketing purposes, transmission within a group of affiliated entities for internal administrative purposes, ensuring network and information security, and reporting of possible criminal acts or threats to public security. GDPR, recitals 47–50.

[415] *Id.* art. 6(1).

[416] *See When Can We Rely on Legitimate Interests*, U.K. INFO. COMM'RS OFFICE (last visited Jan. 3, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/.

[417] *See e.g.*, Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L.J. 287, 311 & n.103 (2018) (discussing the legal basis for online search providers such as Google to operate under the GDPR); *What is the 'Legitimate Interests' Basis?*, U.K. INFO. COMM'RS OFFICE (last visited Feb. 29, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ ("Legitimate interests . . . could in principle apply to any type of processing for any reasonable purpose.").

[418] *What is the 'Legitimate Interests' Basis?*, *supra* note 417 ("Whilst any purpose could potentially be relevant, that purpose must be 'legitimate'. Anything illegitimate, unethical or unlawful is not a legitimate interest. For example, although marketing may in general be a legitimate purpose, sending spam emails in breach of electronic marketing rules is not legitimate.").

[419] GDPR, art. 4(11).

[420] *Id.* art 7(3). Recitals to the GDPR state controllers must be able to demonstrate that individuals have provided consent; that pre-formulated consent forms should be provided an in "intelligible and easily accessible form" that uses clear and plain language and does not include unfair terms; and that consent should not be regarded as freely given if the individual has "no genuine or free choice or is unable to refuse or withdraw consent without detriment." *Id.*, recital 42.

[421] *Id.* arts. 8–10.

[422] Exceptions to individual rights, which are outside the scope of this report, are defined on a right-by-right basis. *See id.* arts. 12–22.

1. **Right to be informed**

   Individuals have a right to be informed about the collection and use of their personal data.[423] Controllers must provide individuals with certain information, including the purposes for processing, retention periods, and with whom the data will be shared.[424] The information must be concise, transparent, intelligible, easily accessible, and presented in plain language.[425]

2. **Right of access (i.e., right to a copy)**

   Individuals have a right to access and obtain copies of their personal data, and controllers must respond to a request for access within one month.[426]

3. **Right to rectification**

   The GDPR provides individuals with a right to require personal data controllers to correct inaccurate information or complete incomplete data.[427]

4. **Right to erasure (also known as the "right to be forgotten")**

   Individuals have the right to have their personal data erased in some cases.[428] Controllers must comply with an erasure request when, among other circumstances: (1) the data is no longer necessary for the purposes for which it was collected; (2) the controller relied on consent as its legal basis for processing and the individual subsequently withdrew consent; or (3) the controller relied on the "legitimate interests" basis for processing, the individual objected to processing, and there was no overriding legitimate interest.[429]

5. **Right to restrict processing**

   The GDPR provides individuals the right to restrict data processing in certain circumstances, often during a limited period of time while the controller evaluates a broader objection to its data processing activities.[430]

6. **Right to data portability**

   The right to data portability allows individuals to obtain the personal data that they provided to a controller in a commonly used, machine-readable format that can be transmitted to another controller without affecting the data's usability.[431] This right is intended to allow individuals to take advantage of alternative programs and services that can use their data, even when a different controller originally collected or compiled the data.[432]

7. **Right to object**

   The GDPR gives individuals the right to object to the processing of their personal data in several circumstances.[433] Individuals have an absolute right to object to data processing for direct marketing

[423] *Id.* arts. 12–14.

[424] *Id.*

[425] *Id*. art. 12.

[426] *Id*. arts. 12(3), 15.

[427] *Id.* art. 16.

[428] *Id*. art. 17.

[429] *Id*. art. 17. Absent an exception, the right of erasure also applies when: (1) the controller is processing personal data for direct marketing purposes and the individual objects to the processing; (2) the data was processed unlawfully; (3) EU law or the law of an EU member nation requires the data to be erased; or (4) the data was collected in connection with the offering of internet services to a child. *Id.*

[430] *Id.* art. 18(1). The right to restriction applies when: (1) the accuracy of personal data is contested and controller is in the process of verifying whether the data is accurate; (2) the processing is unlawful, but the data subject prefers restriction instead of erasure; (3) the controller no longer needs the personal data, but the data subject requires the data to be maintained in relation to its legal claims; or (4) the controller is considering whether the data subject's objection to processing overrides the legitimate interests in the processing. *Id.*

[431] *Id*. art. 20.

[432] *See* ICO GUIDE, *supra* note 398, at 128 (explaining that data portability "enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.").

[433] GDPR, art. 21.

purposes; once the individual objects the data may no longer be processed for direct marketing.[434] In other circumstances, the right to object is less complete, and controllers may be able to continue processing if they demonstrate compelling legitimate grounds that override an objector's claims or that the processing is necessary for legal claims or defenses.[435] Controllers must respond to an objection within one month.[436]

8. **Rights regarding automated decision making and profiling**

Individuals have the right to object to data processing that involves automated decision making without human involvement.[437] Individuals may also object to profiling, which is defined as the automated processing of personal data to evaluate certain personal aspects of an individual, in particular to analyze or predict aspects about the individual's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. [438] Automated decision making and profiling are permissible when necessary for a contract, authorized by EU law or the law of an EU member state, or based on an individual's explicit consent.[439]

Data Governance and Security

The GDPR requires organizations to implement a range of measures designed to ensure and demonstrate that they are in compliance with the regulation.[440] When proportionate in relation to the processing activities, such measures may include adopting and implementing data protection policies[441] and taking a "data protection by design and default" approach whereby the organization implements compliance measures into all stages of data processing.[442] Measures may also include the following:

- establishing GDPR-conforming contracts with data processors;[443]
- maintaining records of processing activities;[444]
- conducting impact assessments on personal data use that is likely to risk individual rights and freedoms;[445]
- appointing a data protection officer;[446] and
- adhering to relevant codes of conduct and compliance certification schemes.[447]

The GDPR also requires controllers and processors to implement technical and organizational measures to ensure a level of data security that is "appropriate to the risk" presented by the data

[434] *Id.* art. 21(2-3).

[435] *Id.* art. 21(1).

[436] *Id.* art. 12(3).

[437] *Id.* art. 22(1).

[438] *Id.* art. 4(4).

[439] *Id.* art. 22(2).

[440] *Id.* arts. 24–43.

[441] *Id.* art. 24(2).

[442] *Id.* art. 25.

[443] *Id.* art. 28(3).

[444] *Id*. art. 30.

[445] *Id.* art. 35.

[446] *Id.* arts. 37–39. Any personal data controller whose core activities include large-scale processing of especially sensitive data or regular and systematic monitoring of data subjects on a large scale must designate a data protection officer. *Id.* art. 37(1). With the exception of courts acting their judicial capacity, all public authorities or bodies also must designate a data protection officer. *Id.*

[447] *Id.* arts. 40–43.

processing.[448] In implementing data security measures, organizations must consider the "state of the art, the costs of implementation," the nature, scope, and context, and purposes of processing, and the likelihood and potential severity of an infringement on individual rights if data security were to be violated.[449] The GDPR does not impose a "one-size-fits-all" requirement for data security, and security measures that are "appropriate" (and therefore mandatory) will depend on the specific circumstances and risks.[450] For example, a company with an extensive network system that holds a large amount of sensitive or confidential information presents greater risk, and therefore must install more rigorous data security protections than an entity that holds less data.[451]

When appropriate, organizations should consider encryption and *pseudonymization*[452]—the processing of personal data such that the data can no longer be attributed to a specific individual.[453] Security measures should ensure the confidentiality, integrity, and resilience of processing systems; be able to restore access to personal data in the event of an incident; and include a process for testing security effectiveness.[454]

Data Breach Notifications

In the event of a personal data breach,[455] the GDPR requires controllers to notify the designated EU government authority "without undue delay" and no later than 72 hours after learning of the breach, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[456] For example, whereas a company must report the theft of a customer database that contains information that could be used for future identity fraud given the high level of risk to individuals, it may not need to report the loss of more innocuous data, such as a directory of staff office phone numbers.[457] When notification to the government is required, the notification must describe the nature and likely consequences of the breach, identify measures to address the breach, and identify the employee responding to the incident.[458] When data processors experience a breach, they must notify the controller without undue delay.[459]

In addition to governmental notification, controllers must notify the individuals whose data has been compromised if the breach is likely to result in a "high risk to the rights and freedoms" of individuals.[460] The "high risk" threshold is higher than the threshold for notifying the government

[448] *Id.* art. 32(1).

[449] *Id*.

[450] *Security*, U.K. INFO. COMM'RS OFFICE (last visited Feb. 21, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/.

[451] *See id*.

[452] GDPR, art. 32(1)(a).

[453] *Id*. art. 4(5).

[454] *Id*. art 32(1)(b–c).

[455] Personal data breach is defined as the "breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed . . . ." *Id*. art. 4(11).

[456] *Id.* art. 33(1).

[457] *See Personal Data Breaches*, U.K. INFO. COMM'RS OFFICE (last visited Feb. 21, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

[458] GDPR, art. 33(2).

[459] *Id.* art. 33(3).

[460] *Id.* art. 34(1).

authority, but it could met in circumstances when individuals may need to take steps to protect themselves from the effects of a data breach.[461] According to the United Kingdom's data protection regulatory authority, for example, a hospital that disclosed patient medical records as a result of a data breach may present a "high risk" to individuals, but a university that accidentally deleted, but was able to re-create, an alumni contact information database may not meet the mandatory individual reporting threshold.[462]

Notification to the individual must describe the breach in clear and plain language and contain at least the same information as provided in the governmental notifications.[463] Notification to the individual is not required in the following cases:

- the controller implemented appropriate technical and organizational protection measures, such as encryption, that will render the data unintelligible;
- the controller took subsequent measures that will ensure that the high risk to individual rights and freedom are no longer likely to materialize; or
- individual notifications would involve disproportionate efforts, in which case the controller must provide public notice of the breach.[464]

Regardless of whether notification is required, controllers must document all data breaches so that government supervisory authorities can verify compliance at a later date.[465]

Data Transfer Outside the EU

The EU has long regulated the transfer of data from EU member states to foreign countries, and the GDPR continues to restrict such international data transfers.[466] Like the 1995 Data Protection Directive, the GDPR authorizes data transfer from within the EU to a non-EU country if the receiving country ensures an *adequate level of protection* for personal data.[467] To meet this requirement, the non-EU country must offer a level of protection that is "essentially equivalent to that ensured" by the GDPR.[468] If the European Commission previously made an adequacy decision under the Data Protection Directive's legal framework, that decision remains in force under the GDPR.[469]

U.S. and EU officials previously developed a legal framework—the U.S.-EU Privacy Shield—for protecting transatlantic data flow into the United States.[470] Under the Privacy Shield framework,

[461] *See Personal Data Breaches*, *supra* note 457.

[462] *See id*.

[463] GDPR, art. 34(2).

[464] *Id.* art. 34(3).

[465] *Id.* art. 33(5). For additional background on cross-border data flows, see CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

[466] *Id.* arts. 44–50.

[467] *Compare* GDPR, art. 45(1) ("A transfer of personal data to a third country . . . may take place where the Commission has decided that the third country . . . ensures an adequate level of protection."), *with* Data Protection Directive, *supra* note 387, art. 25(6) ("The Commission may find . . . that a third country ensures an adequate level of protection . . . by reason of its domestic law or of the international commitments it has entered into . . .").

[468] GDPR, recital 104.

[469] *Id.* art. 45(9).

[470] For background on data transfers from the EU to the U.S., see CRS Report R44257, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, by Martin A. Weiss and Kristin Archick.

U.S.-based organizations self-certify to the International Trade Administration in the Department of Commerce that they will comply with the framework's requirements for protecting personal data by complying with, among other provisions, notice requirements, data retention limits, security requirements, and data processing purpose principles.[471] In 2016, the European Commission concluded that the Privacy Shield framework provided adequate protections under the Data Protection Directive.[472] That adequacy determination continues to apply under the GDPR,[473] although the European Commission annually reviews whether the Privacy Shield framework continues to provide an adequate level of protection.[474]

In the absence of an adequacy decision from the European Commission, the GDPR permits data transfers outside the EU when (1) the recipient of the data has itself established *appropriate safeguards*,[475] and (2) effective legal remedies exist for individuals to enforce their data privacy and protection rights.[476] Appropriate safeguards include: a legally binding agreement between public authorities or bodies; binding corporate rules; standard contract clauses adopted by the European Commission; and approved codes of conduct and certification mechanisms.[477] U.S. companies that do not participate in Privacy Shield often must rely on standard contract clauses to be able to receive data from the EU.[478]

The GDPR also identifies a list of circumstances in which data may be transferred outside the EU even without appropriate safeguards or an adequacy decision.[479] These circumstances include, among other reasons, when: an individual has provided informed consent; transfer is necessary for the performance of certain contracts involving the data subject; or the transfer is necessary for important reasons of public interests.[480]

---

[471] *See id.* at 9–11.

[472] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Jan. 1, 2016, O.J. L. 207, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

[473] *See* GDPR, art. 45(9). *See also Adequacy of the Protection of Personal Data in Non-EU Countries*, EUROPEAN COMM'N (last visited Feb. 21, 2019), https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en ("The European Commission has so far recognised . . . the United States of America (limited to the Privacy Shield framework) as providing adequate protection.").

[474] *See* EUROPEAN COMM'N, REPORT FROM THE COMMISSION TO EUROPEAN PARLIAMENT AND THE COUNCIL ON THE SECOND ANNUAL REVIEW OF THE FUNCTIONING OF THE U.S.-E.U. PRIVACY SHIELD (2018), https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf. Although the Privacy Shield enables participating companies to meet the GDPR's requirements for the transfer of personal data outside the EU, participation in the program does not ensure that a U.S. company is compliant with all GDPR requirements. *See*, *e.g.*, Int'l Trade Adm', Dep't of Commerce, *Privacy Shield Program, FAQs-General*, Privacy Shield.gov (last visited Feb. 21, 2019), https://www.privacyshield.gov/article?id=General-FAQs ("It is important to note that Privacy Shield is not a GDPR compliance mechanism, but rather is a mechanism that enables participating companies to meet the EU requirements for transferring personal data to third countries, discussed in Chapter V of the GDPR.").

[475] GDPR, art. 46.

[476] *Id.* art. 46(1).

[477] *Id.* art. 46(2).

[478] *See* Phillip Bantz, *As More Countries Seek Adequacy Decisions, Will US Get Left Behind*, CORPORATE COUNSEL (Feb. 26, 2019), https://www.law.com/corpcounsel/2019/02/26/as-more-countries-seek-adequacy-decisions-with-eu-will-us-get-left-behind/.

[479] GDPR, art. 49.

[480] *Id*. art. 49. Transfers may also be permitted when necessary for a legal claim; necessary to protect the vital interest of a data subject and the data subject is physically or legally incapable of giving consent; and the transfer is made from a register that, according to EU law or the national law of an EU country, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a

Remedies, Liability, and Fines

One of the most commented-upon aspects of the GDPR is its high ceiling for administrative fines.[481] For the most serious infractions of the GDPR, regulatory bodies within individual EU countries may impose fines up to 20 million euro (approximately $22 million) or 4% of global revenue, whichever is higher, for certain violations of the GDPR.[482] The GDPR also provides tools for individuals to enforce compliance with its terms. Individuals whose personal data is processed in a way that does not comport with the GDPR may lodge a complaint with regulatory authorities.[483] Individuals also have the right to an "effective judicial remedy" (i.e., to pursue a lawsuit) against the responsible data processor or controller, and individuals may obtain compensation for their damages from data processors or controllers.[484]

The GDPR and the 116th Congress

The GDPR may be relevant to the 116th Congress' consideration of data protection initiatives in several ways. Because the GDPR applies to U.S. companies that offer goods and services to individuals in the EU, many U.S. companies have developed new data protection practices in an effort to comply with its requirements.[485] Other businesses reported that they withdrew from the European market rather than attempt to obtain compliance GDPR.[486] For those companies that remained in the European market, some have stated that they will apply their GDPR-compliant practices on a company-wide basis rather than changing their model only when doing business in the EU.[487] Consequently, the GDPR already directly impacts the data protection practices of some U.S. companies.

The GDPR also has served as a prototype for comprehensive data protection legislation in other governments. For example, commentators have described China's Personal Information Security Specification, which defines technical standards related to the collection, storage, use, transfer, and disclosure of personal information, as modeled on the GDPR.[488] And the CCPA includes

---

legitimate interest in inspecting the register. Id. art. 49(1).

[481] *See e.g.*, Bernard Marr, *GDPR: The Biggest Data Breaches and the Shocking Fines (That Would Have Been)*, FORBES (June 11, 2018), https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#28cbc336c109; Andrea O'Sullivan, *The EU's New Privacy Rules are Already Causing International Headaches*, REASON (June 12, 2018), https://reason.com/archives/2018/06/12/the-eus-new-privacy-rules-are-already-ca.

[482] GDPR, art. 83(5).

[483] *Id.* art. 77.

[484] *Id.* arts. 79, 82. Individuals also may authorize a nonprofit entity to lodge complaints and seek judicial remedies on their behalf. *Id.* art. 80.

[485] *See supra* § Scope and Territorial Reach.

[486] *See*, *e.g.*, Hannah Kuchler, *US Small Businesses Drop EU Customers over New Data Rule*, FIN. TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04 (identifying small businesses that stated that they will no longer do business in the EU due to risk of GDPR non-compliance); Roslyn Layton & Julian Mclendon, *The GDPR: What It Really Does and How the U.S. Can Chart A Better Course*, 19 FEDERALIST SOC'Y REV. 234, 244-45 (2018) (discussing the "[m]any American retailers, game companies, and service providers [that] no longer operate in the EU" as a result of the GDPR).

[487] *See*, *e.g.*, Josh Constine, *Zuckerberg Says Facebook Will Offer GDPR Privacy Controls Everywhere*, TECHCRUNCH (Mar. 22, 2018), https://techcrunch.com/2018/04/04/zuckerberg-gdpr/ (discussing Facebook's "plans to comply with GDPR's data privacy rules around the world").

[488] *See* Samm Sacks, *China's Emerging Data Privacy System and GPDR*, CTR. FOR STRATEGIC AND INT'L STUDIES (Mar. 9, 2018), https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr; *Where Are We Now With Data Protection in China?*, FRESHFIELDS BRUCKHAUS DERINGER (Sept. 13, 2018),

elements similar to the GDPR, such as an enumeration of individual rights related to data privacy.[489] If this trend continues, GDPR-like data protection laws may become more commonplace internationally.[490]

Finally, some argue that Congress should consider enacting comprehensive federal data protection legislation similar to the GDPR.[491] As discussed below, however, other observers[492] and some officials in the Trump Administration[493] have criticized the GDPR, describing the regulation as overly prescriptive and likely to result in negative unintended consequences. Regardless of the merits of these positions, the GDPR may remain a focal point of discussion in the debate over whether the United States should develop a more comprehensive data protection policy.

The Trump Administration's Proposed Data Privacy Policy Framework

Although some commentators argue that the federal government should supplement the current patchwork of federal data protection laws with more comprehensive legislation modeled on the CCPA or GDPR,[494] some Trump Administration officials have criticized these legislative

http://knowledge.freshfields.com/m/Global/r/3824/where_are_we_now_with_data_protection_law_in_china_.

[489] *Compare* § The CCPA's Provisions and Requirements *with* § Individual Rights and Corresponding Obligations.

[490] *See*, *e.g.*, Adam Satariano, *G.D.R.P., A New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html ("Brazil, Japan and South Korea are set to follow Europe's lead, with some having already passed similar data protection laws. European officials are encouraging copycats by tying data protection to some trade deals and arguing that a unified global approach is the only way to crimp Silicon Valley's power."); Melanie Ramey, *Brazil's New General Data Privacy Law Follows GDPR Provisions*, INSIDE PRIVACY (Aug. 20, 2018), https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/ ("The [Brazilian General Data Privacy Law's] key provisions closely mirror the European Union's General Data Privacy Regulation . . . ."); Gopal Rantam, *Data Privacy Bill Faces Long Odds, EU Moves Ahead*, CQ (Mar. 11, 2019), https://plus.cq.com/shareExternal/doc/news-5481061/gVGqdMK17H9EZfgmaRVAdltAhE4?0 ("India, Singapore, Brazil, and Japan have or are writing laws that would comply with the EU's GDPR.").

[491] *See*, *e.g.*, *America Should Borrow from Europe's Data Privacy Law*, THE ECONOMIST (Apr. 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law; Max Read, *The E.U.'s New Privacy Law Might Actually Create a Better Internet*, N.Y. MAG (May 15, 2018), http://nymag.com/intelligencer/2018/05/can-gdpr-create-a-better-internet.html; Trevor Butterworth, *Europe's Tough New Digital Privacy Law Should be a Model for U.S. Policymakers*, VOX (May 23, 2018); https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge.

[492] *See*, *e.g.*, Layton & Mclendon, *supra* note 486, at 248 ("The GDPR's unintended consequences include violations of the freedom of speech, closures of startups, blocked foreign news outlets, the disruption of online ad markets, the compromising of the WHOIS database, and the hampering of innovation."); Niam Yaraghl, *A Case Against the General Data Protection Regulation*, BROOKINGS (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/ (arguing that GDPR could increase the cost of services that consumers are used to receiving on the internet free of charge and lead to lower quality online services and products).

[493] *See infra* § The Trump Administration's Proposed Data Privacy Policy Framework (discussing the Trump Administration's criticism of the GDPR).

[494] *See supra* note 491.

approaches[495] and questioned whether they will improve data privacy outcomes.[496] The Administration has argued that many comprehensive data privacy models have resulted in "long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users[.]"[497] Rather than pursuing a *prescriptive* model in which the government defines (or prescribes) data protection rules, the Trump Administration advocates for what it describes as an *outcome-based* approach whereby the government focuses on the "outcomes of organizational practices, rather than on dictating what those practices should be."[498]

In September 2018, the National Telecommunications and Information Administration (NTIA) in the Department of Commerce issued a request for public comments on the Trump Administration's efforts to develop an outcome-based approach to advancing consumer privacy that also protects prosperity and innovation.[499] According to NTIA, changes in technology have led consumers to conclude that they are losing control over their personal information, while at the same time that foreign and state privacy laws have led to a fragmented regulatory landscape that disincentives innovation.[500] Accordingly, NTIA is attempting to develop a set of "user-centric" privacy outcomes and goals that would underpin the protections that should be produced by any federal actions related to consumer privacy.[501]

NTIA's proposed policy focuses on a set of outcomes that the Trump Administration seeks to achieve:[502]

1. **Transparency**

   Users should be able to easily understand how organizations collect, store, use, and share personal information. Organizations should take into account how the average user interacts with their services and should avoid lengthy privacy notices.

2. **Control**

   Users should be able to exercise reasonable control over organizations' collection, use, storage, and disclosure of their personal information. Users' ability to withdraw or limit consent to data use should be as readily accessible.

[495] *See* Wilbur Ross, U.S. Sec'y of Commerce, *EU Data Privacy Laws are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c ("GDPR's implementation could significantly interrupt transatlantic co-operation and create unnecessary barriers to trade, not only for the US, but for everyone outside the EU.").

[496] Walter Copan, Director, Nat'l Inst. Standards. & Tech, Dep't of Commerce, Developing the NIST Privacy Framework: How Can a Collaborate Process Help Manage Privacy Risks (Sept. 24, 2018), https://www.nist.gov/speech-testimony/developing-nist-privacy-framework-how-can-collaborative-process-help-manage-privacy [hereinafter Copan Keynote] ("It is too soon to tell how large an impact these regulations will ultimately have on products and services that rely on access to users' data, and whether there will be a substantial measurable improvement in desired privacy outcomes.").

[497] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

[498] *Id*.

[499] *See id.* at 48600 ("[NTIA] is requesting comments on ways to advance consumer privacy while protecting prosperity and innovation.").

[500] *See id*.

[501] *See id.* ("NTIA is seeking . . . to . . . lay[] out a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections.").

[502] *Id.* at 48601.

3. **Reasonable minimization**

   Organizations should minimize data collection, storage length, use, and sharing in a manner that is reasonable and appropriate to the context and risk.

4. **Security**

   Organizations should employ security safeguards to protect personal information that are appropriate to the level of risk, and should "meet or ideally exceed" best practices.

5. **Access and correction**

   Users should have reasonable and appropriate access to their personal data and should be able to rectify, complete, amend, or delete that data, but users' access should not interfere with legal obligations or rights.

6. **Risk management**

   Users should expect organizations to manage and mitigate the risk of harmful use or exposure of personal data.

7. **Accountability**

   Organizations should be externally and internally accountable for the use of personal information and should ensure that their third-party servers are accountable.[503]

In addition to identifying desired outcomes, NTIA's request for public comments states that the Trump Administration is in the process of developing "high-level goals for Federal action" related to data privacy.[504] NTIA's proposed privacy framework shares certain elements of prescriptive legal regimes like the GDPR and CCPA. Common features include a right to withdraw consent to certain uses of personal data;[505] accountability for third-party vendors and servicers;[506] and a right to access, amend, complete, correct, or delete personal data.[507] But NTIA's request for public comments does not specifically describe how the Trump Administration intends to accomplish its outcomes and goals. Instead, it states that NTIA "understand[s] that there is considerable work to

[503] *Id.* at 48601–02.

[504] *Id.* at 48602. The notice provides a list of eight "non-exhaustive and non-prioritized" goals: (1) harmonize the "patchwork" regulatory landscape; (2) provide legal clarity while maintaining enough flexibility to allow for novel business models and technologies; (3) apply any action to all private sector organizations that handle personal data that are not covered by sectoral laws; (4) employ a risk- and outcome-based approach rather than a compliance model; (5) ensure consistency with international frameworks to permit data flow across national boundaries; (6) incentive research and development that improve privacy protections; (7) give the FTC enforcement authority; and (8) ensure that data privacy requirements are proportionate to the scale and scope of the information and organization is handling. *Id.* at 48602–03.

[505] *Compare id*. at 48601 ("[C]ontrols used to withdraw the consent of . . . a consumer should be as readily accessible and usable as the controls used to permit the activity."), *with* GDPR, art. 7(3) ("The data subject shall have the right to withdraw his or her consent at any time."); *and* CAL CIV. CODE § 1798.120 (defining the right to opt out of the sale of personal data).

[506] *Compare* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. at 48602 ("Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data."), *with* GDPR, art. 28(1) ("[T]he controller shall use only processors providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."); *and* CAL. CIVIL CODE § 1798.140(c) (defining "Business" as any entity that "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information . . . .").

[507] *Compare* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. at 48602 ("Users should have qualified access [to] personal data that they provided, and to rectify, complete, amend, or delete this data.") *with* §§ Individual Rights and Corresponding Obligations (discussing the rights to access, rectification, and erasure under the GDPR); *and* § The CCPA's Provisions and Requirements (discussing the rights to know, opt out, and delete in the CCPA).

be done to achieve" the identified objectives.[508] The comment period closed on November 9, 2018,[509] and NTIA received input from more than 200 individuals and entities.[510]

Considerations for Congress

The debate over whether Congress should consider federal legislation regulating data protection implicates numerous legal variables and options. "Data protection" itself is an expansive concept that melds the fields of *data privacy* (i.e., how to control the collection, use, and dissemination of personal information) and *data security* (i.e., how to protect personal information from unauthorized access or use and respond to such unauthorized access or use).[511] There is no single model for data protection legislation in existing federal, state, or foreign law. For example, some state laws focus solely on data security or address a particular security concern,[512] such as data breach notifications.[513] Other state laws isolate a single privacy-related issue, such as the transparency of data brokers—companies that aggregate and sell consumers' information, but that often do not have a direct commercial relationship with consumers.[514]

Recent data protection laws such as the CCPA and GDPR appear to indicate a trend toward combining data privacy and security into unified legislative initiatives.[515] These unified data protection paradigms typically are structured on two related features: (1) an enumeration of statutory rights given to individuals related to their personal information and (2) the creation of legal duties imposed on the private entities that possess personal information. The specific list and nature of rights and duties differ depending on the legislation,[516] and some have proposed to define new rights in federal legislation that do not have a clear analog in existing state or foreign law.[517] Consequently, at present, there is no agreed-upon menu of data protection rights and obligations that could be included in federal legislation.

Although data protection laws and proposals are constantly evolving, some frequently discussed legal rights include:

[508] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. at 48602.

[509] *See* Notice and Extension of Comment Period; Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 51449 (2018).

[510] *Comments on Developing the Administration's Approach to Consumer Privacy*, NTIA.GOV (Nov. 13, 2018), https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy.

[511] *See supra* note 2e.

[512] According to the National Conference of State Legislatures, at least 24 states have laws that address data security practices of private sector entities. *See Data Security Laws | Private Sector: Overview*, NCSL.ORG (Jan. 4, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[513] All 50 states have laws defining data breach notification requirements, according to the National Conference of State Legislatures. *See Security Breach Notification Laws*, NCSL.ORG (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[514] *See* VT. STAT. ANN. tit. 9, § 2446 (requiring annual registration of data brokers).

[515] *See supra* §§ The California Consumer Privacy Act (CCPA); The EU's General Data Protection Regulation (GDPR). *See also* Burt & Greer, *supra* note 2 ("New laws focused on data now blend privacy protections with mandates, like the [GDPR] or China's Cybersecurity Law.").

[516] For example, whereas the CCPA defines three primary consumer rights, the GDPR identifies eight rights related to personal data. *Compare* § The CCPA's Provisions and Requirements, *with* § Individual Rights and Corresponding Obligations.

[517] *See*, *e.g.*, S. 3744, 115th Cong. § 3(b)(2) (2018) (proposing to require online service providers to fulfill a "duty of loyalty").

- the right to know what personal data is being collected, used, and disseminated, and how those activities are occurring;
- the right to control the use and dissemination of personal data, which may include the right to opt out or withhold consent to the collection or sharing of such data;
- the right to review personal data that has been collected and to delete or correct inaccurate information;
- the right to obtain a portable copy of personal data;
- the right to object to improper activities related to personal data; and
- the right to learn when a data breach occurs;

Commonly discussed obligations for companies that collect, use, and disseminate personal data include rules defining:

- how data is collected from individuals;
- how companies use data internally;
- how data is disseminated or disclosed to third parties;
- what information companies must give individuals related to their data;
- how data is kept secure;
- when breaches of security must be reported;
- the accuracy of data; and
- reporting requirements to ensure accountability and compliance.

Whether to enact federal data protection legislation that includes one or more of these rights and obligations has been the subject of a complex policy debate and multiple hearings in recent Congresses.[518] Part of the legislative debate concerns how to enforce such rights and obligation and raises questions over the role of federal agencies, state attorneys general, and private citizen suits.[519] In addition, some elements of the data protection proposals and models could implicate legal concerns and constitutional limitations. While the policy debate is outside the scope of this report, the following sections discuss legal considerations relevant to federal data protection proposals that the 116th Congress may choose to consider. These sections begin by analyzing legal issues related to the internal structure and definition of data protection-related rights and obligations and then move outward toward an examination of external legal constraints.

Prescriptive Versus Outcome-Based Approach

A primary conceptual point of debate concerning data protection legislation is whether to utilize the so-called "prescriptive" method or an "outcome-based" approach to achieve a particular law's objectives. Under the prescriptive approach, the government defines data protection rules and requires regulated individuals and entities to comply with those rules.[520] Both the GDPR and CCPA use a prescriptive approach, and some legislation proposed in the 116th Congress would

[518] *See supra* note 10.

[519] *See infra* § Agency Enforcement.

[520] *See* Alan Rual and Christopher Fonzone, *The Trump Admin. Approach to Data Privacy, and Next Steps*, LAW360 (Sept. 27, 2018), https://www.law360.com/articles/1086945/the-trump-admin-approach-to-data-privacy-and-next-steps (contrasting the NTIA's privacy framework with the GDPR and CCPA).

use this method by delineating certain data protection requirements.[521] The Trump Administration, however, has argued that a prescriptive approach can stymie innovation and result in compliance checklists without providing measurable privacy benefits.[522] As an alternative methodology, the Administration advocated for what it described as an outcome-based approach whereby the government focuses on the outcomes of organizational practices, rather than defining the practices themselves.[523] Some federal information technology laws, such as the Federal Information Security Management Act (FISMA),[524] use an outcome-oriented approach to achieve federal objectives, although agency implementation of such laws may become prescriptive in nature.[525] The Administration has not specified how it intends to achieve its desired data protection goals without prescribing data protection rules, but additional direction appears to be forthcoming, according to the NTIA's request for public comment.[526]

Defining Protected Information and Addressing Statutory Overlap

Another issue that may be considered in crafting federal data protection policy is how to define the contours of the data that the federal government proposes to protect or the specific entities or industries that it proposes to regulate.[527] The patchwork of existing data protection statutes define protected information in a variety of ways, many of which depend on the context of the law. For example, HIPAA is limited to "protected health information"[528] and GLBA governs "financial information" that is personally identifiable but not publicly available.[529] By contrast, GDPR and CCPA regulate all "personal" information—a term defined in both laws as information that is associated with a particular individual or is capable of being associated with an individual.[530] Some federal data proposals would apply a similar scope to those of the GDPR and CCPA.[531] If

[521] *See*, *e.g.*, S. 189, 116th Cong. (2019) (requiring, among other things, covered entities to provide certain mandatory disclosures, defining the requirements of the disclosure, and providing individuals with a right to access their personal data in an electronic and easily accessible format).

[522] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. at 48601.

[523] *See id.*

[524] *See* Pub. L. 107-347, 116 Stat. 2899 (codified as amended 44 U.S.C. ch. 35).

[525] For example, implementation of FISMA has become prescriptive in nature, resulting in compliance checklists. *See*, *e.g.*, NAT'L INST. OF SEC. STANDARDS AND TECH., DEP'T OF COMMERCE, NIST SPECIAL PUBLICATION 800-70, REVISION 3, NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS – GUIDELINES FOR CHECKLIST USERS AND DEVELOPERS 6–7 (2015) (discussing the benefits of using "checklists that adhere to the FISMA associated security control requirements").

[526] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. at 48602 (stating the Administration is seeking feedback on how to achieve its data privacy objectives and expressing the view "there is considerable to work to be done" to achieve the Administration's aims).

[527] *See*, *e.g.*, Allison Grande, *What to Watch as Congress Mulls Federal Privacy Legislation*, LAW360 (Feb. 25, 2019), https://www.law360.com/cybersecurity-privacy/articles/1132337/what-to-watch-as-congress-mulls-federal-privacy-legislation ("Much of the debate is likely to be focused on any proposal's definition of personal information, which will play a major role in determining how broadly the regulation will sweep."); *GDPR and CCPA Hearing*, *supra* note 10 (statement of Senator Cortez Masto) ("The tough question for Congress right now as we draft this privacy law is how we define sensitive information versus non-sensitive information.").

[528] *See supra* note 87.

[529] 15 U.S.C. § 6809(4).

[530] *See* GDPR, art. 4(1) ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier . . . ."); CAL. CIV. CODE § 1798.140(o)(1) ("'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.'").

[531] *See*, *e.g.*, H.R. 6864, 115th Cong. § 4(5) (2018) ("The term 'sensitive personal information' means information relating to an identified or identifiable individual . . ."); S. 2728, 115th Cong. § 2(6) (2018) ("[T]the term "personal

enacted, such broad data protection laws have the potential to create multiple layers of federal data protection requirements: (1) general data protection requirements for "personal" information and (2) sector-specific requirements for data regulated by the existing "patchwork" of data protection laws. Other legislative proposals have sought to avoid dual layers of regulations by stating that the proposed data protection requirements would not apply to individuals or entities covered by certain existing federal privacy laws.[532]

Agency Enforcement

Agency enforcement is another key issue to consider when crafting any future federal data protection legislation. As discussed, under the current patchwork of federal data protection laws, there are multiple federal agencies responsible for enforcing the myriad federal statutory protections, such as the FTC, CFPB, FCC, and HHS.[533] Of these agencies, the FTC is often viewed—by industry representatives,[534] privacy advocates,[535] and FTC commissioners themselves[536]—as the appropriate primary enforcer of any future national data protection legislation, given its significant privacy experience.[537]

There are, however, several relevant legal constraints on the FTC's enforcement authority. First, the FTC generally lacks the ability to issue fines for first-time offenses. In UDAP enforcement actions, the FTC may issue civil penalties only in certain limited circumstances, such as when a person violates a consent decree or a cease and desist order.[538] Consequently, the FTC often enters into consent decrees addressing a broad range of conduct, such as a company's data security practices, seeking penalties for violations of those decrees. However, as the *LabMD* case

data" means individually identifiable information about an individual collected online . . . .").

[532] *See, e.g.*, S. 142, 116th Cong. §4(c) (2019).

[533] *See supra* § Federal Data Protection Law.

[534] *See, e.g.*, *Examining Safeguards Hearing*, *supra* note 10 (written statement of Leonard Cali, AT&T Senior Vice President Global Public Policy) ("[T]he federal privacy law can be overseen exclusively by the FTC, an agency with decades of experience regulating privacy practices."); *id.* (responses to written questions, Andrew DeVore, Vice President and Associate General Counsel, Amazon.com, Inc.) ("A national privacy framework should primarily be enforced by the [FTC]. The FTC is the U.S. regulator with core competency and subject matter expertise on consumer privacy, and should continue to serve that role in future frameworks."); *id* (responses to written questions, Bud Tipple, Vice President for Software Technology, Apple Inc.) ("As the current leading federal privacy enforcement agency is the Federal Trade Commission, we believe the FTC should play an important role in interpreting and enforcing comprehensive privacy legislation.").

[535] *See, e.g.*, *id.* (written statement of Nuala O'Connor, President and CEO of Center for Democracy and Technology) ("legislation should . . . give meaningful authority to the FTC and state attorneys general to enforce the law.").

[536] *Oversight of the Federal Trade Commission: Hearing before the Subcomm. On Consumer Protection, Product Safety, Insurance, and Data Security* (Nov. 27, 2018) (statements of commissioners Joseph J. Simons, Rohit Chopra, Noah Joshua Philips, Rebecca Kelly Slaughter, and Christine S. Wilson) (all affirming the view that the FTC is the appropriate enforcement agency for comprehensive privacy legislation).

[537] Some consumer advocacy groups, however, have maintained that instead of FTC enforcement Congress should establish a new data protection agency. *See* Berkley Media Studies Group et al., The Time is Now: *A Framework for Comprehensive Privacy Protection and Digital Rights in the United States*, Citizen.org, https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf (last visited Jan. 18, 2019) ("While the Federal Trade Commission (FTC) helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority. The agency has failed to enforce the orders it has established. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges . . . . Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.").

[538] 15 U.S.C. § 45(l)–(m).

discussed earlier in this report suggests,[539] if the FTC imposes penalties based on imprecise legal standards provided in a rule or order, the Due Process Clause of the Fifth Amendment may constrain the agency's authority.[540] Second, the plain text of the FTC Act deprives the FTC of jurisdiction over several categories of entities, including banks, common carriers, and nonprofits.[541] Third, the FTC generally lacks authority to issue rules under the APA's notice-and-comment process that is typically used by agencies to issue regulations.[542] Rather, the FTC must use a more burdensome—and, consequently, rarely used—process under the Magnuson-Moss Warranty Act.[543]

As some FTC Commissioners and commentators have noted, these legal limitations may be significant in determining the appropriate federal enforcement provisions in any national data security legislation.[544] While Congress may not be able to legislate around constitutional constraints, future legislation could address some of these limitations—for instance, by allowing the FTC to seek penalties for first-time violations of rules, expanding its jurisdictions to include currently excluded entities, or providing the FTC notice-and-comment rulemaking authority under the APA. These current legal constraints on FTC authority may also be relevant in determining whether national legislation should allow private causes of action or enforcement authority for state attorneys general, as some commentators have suggested that private causes of action and enforcement by state attorneys general are essential supplements to FTC enforcement.[545]

---

[539] For further discussion of *LabMD*, see *supra* § Federal Trade Commission Act (FTC Act).

[540] *LabMD*, 894 F.3d at 1235 ("The imposition of penalties upon a party for violating an imprecise cease and desist order—up to $41,484 per violation or day in violation—may constitute a denial of due process.").

[541] *Id.* §§ 44 (defining a "corporation" as "any company . . . which is organized to carry on business for its own profit or that of its members), 45(a)(2) (giving the FTC jurisdiction over "persons, partnerships, or corporations," except banks, savings and loan institutions, federal credit unions, air carriers, common carriers, and entities subject to the Packers and Stockyards Act of 1921).

[542] AUCHTERLONIE & SICKLER, *supra* note 68, at 1-28 (noting that the FTC only has "APA rulemaking authority for specific matters under a variety of other federal laws" and that its primary "Magnuson-Moss rulemaking procedures exceed the notice-and-comment procedures mandated in Section 553 of the APA which otherwise typically apply to agency rulemakings.")

[543] *See infra* § Federal Trade Commission Act (FTC Act). In addition to these legal constraints, the Third Circuit recently held that FTC may not bring civil litigation based on past UDAP violations that are not ongoing or about to occur. *Shire ViroPharma*, 2019 WL 908577, at *9 ("In short, we reject the FTC's contention that Section 13(b)'s 'is violating' or 'is about to violate' language can be satisfied by showing a violation in the distant past and a vague and generalized likelihood of recurrent conduct. Instead, 'is' or 'is about to violate' means what it says—the FTC must make a showing that a defendant is violating or is about to violate the law."). This holding may limit the FTC's ability to bring actions in federal court based on past UDAP violations. For further discussion of this case, see *supra* note 327.

[544] *Oversight of the Federal Trade Commission: Hearing before the Subcomm. On Consumer Protection, Product Safety, Insurance, and Data Security* (Nov. 27, 2018) (statement of Joseph J. Simons, Chairman) (stating that additional penalty authority would be "very important" in any data privacy legislation); *GDPR and CCPA Hearing*, *supra* note 10 (written statement of Amy Moy, Executive Director, Center on Privacy & Technology at Georgetown Law) ("At present . . . the [FTC] does not have the ability levy fines for privacy and data security. This is widely viewed as a challenge by agency officials . . . . To improve privacy and data security for consumers, the FTC—or another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority. . . . As an additional measure of to support regulatory agility, any agency or agencies that are to be tasked with protecting the privacy and security of consumers' information should be given rulemaking authority. Indeed, FTC commissioners have directly asked Congress for rulemaking authority.").

[545] *GDPR and CCPA Hearing*, *supra* note 10 (written statement of Nuala O'Connor, President and CEO of Center for Democracy and Technology) ("[S]tate attorneys general must be granted the authority to enforce the federal law on behalf of their citizens. . . . There will simply be no way for a single agency like the FTC to absorb this magnitude of new responsibilities."); *id* (written statement by Amy Moy, Executive Director, Center on Privacy & Technology at

Private Rights of Action and Standing

Legislation involving privacy may propose to allow individuals to seek private remedy for violations in the courts. Congress may seek to establish a private right of action allowing a private plaintiff to bring an action against a third party based directly on that party's violation of a public statute.[546] As it has done with many sector-specific privacy laws,[547] Congress, in a data protection statute, could provide not only for this right, but also for specific remedies beyond compensatory damages, such as statutory damages[548] or even treble damages[549] for injured individuals. However, it may be very difficult to prove that someone has been harmed in a clear way by many of the violations that might occur under a hypothetical data protection and privacy regime.[550] Victims of data breaches and other privacy violations, generally speaking, do not experience clear and immediate pecuniary or reputational harm.[551] This obstacle might threaten not only a consumer's ability to obtain monetary relief, but also could run up against the limits of the federal courts' "judicial power" under Article III of the U.S. Constitution.

Article III extends the judicial power of the federal courts to only "cases" and "controversies."[552] As part of that limitation, the Supreme Court has stated that courts may adjudicate a case only where a litigant possesses Article III standing.[553] A party seeking relief from a federal court must

---

Georgetown Law) ("Federal agencies cannot possibly hope to police the entire digital ecosystem. State attorneys general are already doing extensive and excellent work on privacy and data security, and they must be empowered to continue to do that good work under any new legislation. . . . Congress should also consider granting individual consumers themselves the right to bring civil actions against companies for violating privacy regulations."); American Civil Liberty Union, Comment Letter on Request for Comments on Developing the Administration's Approach to Consumer Privacy 5–6 (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/aclu_comments_on_developing_the_administrations_approach_to_consumer_privacy.pdf ("It is also necessary for states to maintain a role in enforcing consumer privacy laws. Even a doubling of federal enforcement resourcing is likely to be inadequate to police the growing number of companies that handle consumer data. . . . Consumers should have the right to take companies who violate privacy standards to court. Such a private right of action is necessary to make consumers whole when their privacy is violated, and it also serves as a vital enforcement mechanism in addition to actions brought by regulators.").

[546] *See* Caroline Bermeo Newcombe, *Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute*, 49 LOYOLA UNIV. CHI. L.J. 117, 120 (2017) (defining "private right of action"). *See, e.g.,* 15 U.S.C. § 1681n(a) (imposing liability for actual damages and statutory damages of $1,000 per violation on "[a]ny person who willfully fails to comply" with the Fair Credit Reporting Act).

[547] *See e.g.*, *supra* § Federal Data Protection Law.

[548] *See Statutory Damages,* BLACK'S LAW DICTIONARY 397 (7th ed. 1999) ("Damages provided by statute . . . as distinguished from damages provided under the common law.").

[549] *See Treble Damages*, BLACK'S LAW DICTIONARY 397 (7th ed. 1999) ("Damages that, by statute, are three times the amount that the fact-finder determines is owed.").

[550] *Cf.* Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 281-82 (2009) ("When an individual's personal information is stolen, there is no guarantee that it will be used fraudulently. In fact, only 2% of stolen credit card information from data breaches is subject to misuse. Of all identity theft reports, only 1.5 to 4% are the result of stolen credit card information. This probability goes down even further when the volume of personal information is large—since identity thieves can only make use of a small number of accounts.").

[551] *See, e.g.*, Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) ("The concept of harm stemming from a data breach has confounded the lower courts. There has been no consistent or coherent judicial approach to data-breach harms. More often than not, a plaintiff's increased risk of financial injury and anxiety is deemed insufficient to warrant recognition of harm . . . .").

[552] U.S. CONST. Art. III.

[553] *See, e.g.*, Warth v. Seldin, 422 U.S. 490, 498–99 (1975) ("In its constitutional dimension, standing imports justiciability: whether the plaintiff has made out a 'case or controversy' between himself and the defendant within the meaning of Art. III. This is the threshold question in every federal case, determining the power of the court to entertain

establish standing. Specifically, the party must show that he has a genuine stake in the relief sought because he has personally suffered (or will suffer): (1) a concrete, particularized and actual or imminent injury;[554] (2) that is traceable to the allegedly unlawful actions of the opposing party; and (3) that is redressable by a favorable judicial decision.[555] These requirements, particularly the requirement of "imminence," form significant barriers for lawsuits based on data protection.[556] Imminence, according to the Supreme Court in *Clapper v. Amnesty International*, requires that alleged injury be "*certainly impending*" to constitute injury-in-fact.[557] Speculation and assumptions cannot be the basis of standing.[558] This reasoning has caused courts to dismiss data breach claims where plaintiffs cannot show actual misuse of data, but can only speculate that future thieves may someday cause them direct harm.[559]

These requirements are constitutional in nature and apply regardless of whether a statute purports to give a party a right to sue.[560] This constitutional requirement limits Congress' ability to use private rights of action as an enforcement mechanism for federal rights, as the recent Supreme Court case *Spokeo, Inc. v. Robins* illustrates.[561] *Spokeo* involved a Federal Credit Reporting Act (FCRA) lawsuit brought by Thomas Robins against a website operator that allowed users to search for particular individuals and obtain personal information harvested from a variety of databases.[562] Robins alleged that Spokeo's information about him was incorrect, in violation of the FCRA requirement that consumer reporting agencies "follow reasonable procedures to assure maximum possible accuracy" of consumer reports.[563] As discussed earlier in this report, FCRA provides for a private right of action making any person who willfully fails to comply with its requirements liable to individuals for, among other remedies, statutory damages.[564] The lower court understood that Robins did not specifically allege any actual damages he had suffered, such

---

the suit.").

[554] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

[555] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–62 (1992) (listing the elements of standing).

[556] *See* Solove & Citron, *supra* note 551 at 741 ("In decision after decision, courts have relied on *Clapper* to dismiss databreach cases.") (citing cases).

[557] *Clapper*, 568 U.S. at 410.

[558] *Id.*

[559] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 272-76 (4th Cir. 2017) (rejecting standing in lawsuit arising out of two data breaches, relying on *Clapper* in concluding that plaintiffs' claims were too speculative); In re OPM Data Security Breach Litig., 266 F. Supp. 3d 1, 35 (D.D.C. 2017) (despite acknowledging that data breach exposed sensitive information which could form the "building blocks" of identity theft, where there was no evidence that purpose of breach was to facilitate fraud or theft, threat of identity theft remained too speculative to support standing); Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1284 (M.D. Fla. 2016) ("The Class Action Complaint indicates that, to date, only Plaintiff was affected by the Data Breach, and he has not asserted any out-of-pocket losses that current case law is willing to recognize. Moreover, Plaintiff has only experienced two fraudulent charges on his card in January 2016 and has not reported any fraudulent charges since that time."); *But see* In re Zappos.com, Inc., 888 F.3d 1020, 1025 (9th Cir. 2018) (holding that "increased risk of future identity theft" could give rise to standing in data breach case following *Clapper*); Attias v. Carefirst, Inc., 865 F.3d 620, 628-29 (D.C. Cir. 2017) (holding that plaintiffs plausibly alleged "substantial risk" of identity theft in data breach case where "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm").

[560] Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997) ("It is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.").

[561] 136 S.Ct. 1540 (2016).

[562] *Id.* at 1545.

[563] *Id.*

[564] *Id.* (citing 15 U.S.C. § 1681n(a)).

as the loss of money resulting from Spokeo's actions.[565] Nonetheless, the court concluded that the plaintiff had standing to seek statutory damages because his injury was sufficiently particular to him—FCRA had created a statutory right for Robins and his personal interest was sufficient for standing.[566]

The Supreme Court disagreed with the lower court, however, explaining that the lower court had erred by eliding the difference between Article III's "concreteness" and "particularization" requirements.[567] Specifically, the Court concluded that a plaintiff must demonstrate a concrete injury separate from a particularized injury, meaning that plaintiffs must show that their injury "actually exist[s]."[568] While tangible injuries, like monetary loss, are typically concrete, a plaintiff with an "intangible injury" must show that it is "real" and not "abstract" in order to demonstrate concreteness.[569] For example, the *Spokeo* Court suggested that the mere publication of an incorrect zip code, although it could violate FCRA, would not be a sufficiently concrete injury for standing purposes.[570] As a result, the Court remanded the case to the lower court to determine if the injury alleged in the case was both particularized *and* concrete.[571]

Spokeo does not eliminate Congress' role in creating standing where it might not otherwise exist. The Supreme Court explained that the concreteness requirement is "grounded in historical practice" and, as a result, Congress' judgment on whether an intangible harm is sufficiently concrete can be "instructive."[572] However, as *Spokeo* explained, Congress cannot elevate every privacy violation to the status of a concrete injury. Both before and after *Spokeo*, the lower courts have resolved standing disputes in lawsuits involving privacy and data protection, where parties argue about whether particular injuries are sufficiently concrete for purpose of Article III.[573]

---

[565] *Id.* at 1544-45.

[566] *Id*. at 1546.

[567] *Id.* at 1548.

[568] *Id.* at 1549.

[569] *Id.* at 1548–49.

[570] *Id.* at 1550.

[571] *Id.* at 1550. On remand, the lower court determined that Robins's alleged injury was both concrete and particularized, and thus, Robins had standing. *See* Robins v. Spokeo, 867 F.3d 1108, 1118 (9th Cir. 2017), *cert denied* Spokeo v. Robins, 138 S. Ct. 931 (2018).

[572] *Spokeo*, 136 S. Ct. at 1549.

[573] *See, e.g.*, Eichenberger v. ESPN, 876 F.3d 979, 983–84 (9th Cir. 2017) (holding that standing exists for violations of the right to privacy under the Video Privacy Protection Act); Dreher v. Experian Information Solutions, 856 F.3d 337, 345–46 (4th Cir. 2017) (holding that customer failed to demonstrate concrete injury in complaint over listing of credit card company, rather than servicer, on credit report); Susinno v. Work Out World, Inc., 862 F.3d 346, 352 (3d Cir. 2017) (holding that customer's receipt of unsolicited calls on her cell phone in violation of Telephone Consumer Protection Act was sufficiently concrete to give rise to standing); *In re* Horizon Healthcare Services Inc. Data Breach Litig., 846 F.3d 625, 640–41 (3d Cir. 2017) ("So the Plaintiffs here do not allege a mere technical or procedural violation of FCRA. They allege instead the unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent. There is thus a de facto injury that satisfies the concreteness requirement for Article III standing."); Santana v. Take-Two Interactive Software, 717 Fed. App'x. 12, 15–16 (2d Cir. 2017) (holding that software company's alleged violations of the notice provisions of the Illinois Biometric Information Privacy Act did not raise a material risk of harm because plaintiffs did not allege any risk that the data would be misused or disclosed harming the plaintiffs); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930–31 (8th Cir. 2016) (holding that plaintiff failed to allege sufficiently concrete injury where cable company allegedly kept personally identifiable information too long in violation of Cable Communications Policy Act); *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) (concluding that plaintiff's allegation that Google combined their personal information from various services without authorization was in sufficient to establish injury-in-fact, as "an allegation that Google profited is not enough equivalent to an allegation that such profiteering deprived Plaintiffs of economic value").

Congress can possibly resolve some of these disputes by elevating some otherwise intangible injuries to concrete status. But *Spokeo* illustrates that there may be a residuum of harmless privacy violations for which Congress cannot provide a judicial remedy.

Preemption

Another legal issue Congress may need to consider with respect to any federal program involving data protection and privacy is how to structure the federal-state regime—that is, how to balance whatever federal program is enacted with the programs and policies in the states. Federal law, under the Supremacy Clause,[574] has the power to preempt or displace state law. As discussed above, there are a host of different state privacy laws, and some states have begun to legislate aggressively in this area.[575] The CCPA in particular represents a state law that is likely to have a national effect.[576] Ultimately, unless Congress chooses to occupy the entire field of data protection law, it is likely that the state laws will end up continuing to have a role in this area. Further, given that the states are likely to continue to experiment with legislation, the CCPA being a prime example, it is likely that preemption will be a highly significant issue in the debate over future federal privacy legislation.[577]

As the Supreme Court has recently explained, preemption can take three forms: "conflict," "express," and "field."[578] Conflict preemption requires any state laws that conflict with a valid federal law to be without effect.[579] Conflict preemption can occur when it is impossible for a private party to simultaneously comply with both federal and state requirements, or when state law amounts to an obstacle to the accomplishment of the full purposes of Congress.[580] Express preemption occurs when Congress expresses its intent in the text of the statute as to which state laws are displaced under the federal scheme.[581] Finally, field preemption occurs when federal law occupies a 'field' of regulation "so comprehensively that it has left no room for supplementary state legislation."[582] Ultimately, the preemptive scope of any federal data protection legislation will turn on the "purpose" of Congress and the specific language used to effectuate that purpose.[583]

---

[574] U.S. CONST. Art. VI, cl. 2.

[575] *See supra* § The California Consumer Privacy Act (CCPA).

[576] *Id.*

[577] *See, e.g.*, Jessica Guynn, *Amazon, AT&T, Google Push Congress to Pass Online Privacy Bill to Preempt Stronger California Law*, USA TODAY (Sept. 26, 2018), https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/; Harper Neidig, *Chamber of Commerce calls for Congress to Block State Privacy Laws*, THE HILL (Sept. 9, 2018), https://thehill.com/policy/technology/405433-chamber-of-commerce-calls-for-congress-to-block-state-privacy-laws.

[578] Murphy v. NCAA, 138 S. Ct. 1461, 1480 (2018).

[579] Mutual Pharmaceutical Co., Inc. v. Bartlett, 133 S. Ct. 2466, 2473 (2013).

[580] *Id. See also* Arizona v. United States, 567 U.S. 387, 399–400 (2012) (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

[581] *Murphy*, 138 S. Ct. at 1480.

[582] *Id.* (quoting R.J. Reynolds Tobacco Co. v. Durham County, 479 U.S. 130, 140 (1986)).

[583] *See* Wyeth v. Levine, 555 U.S. 555, 565 (2009) ("The purpose of Congress is the ultimate touchstone in every pre-emption case . . . [but] in all pre-emption cases, and particularly in those in which Congress has legislated in a field which the States have traditionally occupied we start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless it was the clear and manifest purpose of Congress.") (internal quotations and citations omitted).

If Congress seeks to adopt a relatively comprehensive system for data protection, perhaps the most obvious means to preempt a broad swath of state regulation would be to do so "expressly" within the text of the statute by including a specific preemption provision in the law. For example, several existing federal statutes expressly preempt all state law that "relate to" a particular subject matter.[584] The Supreme Court has held that this "related to" language encompasses any state law with a "connection with, or reference to" the subject matter referenced.[585] Similar language can be used to displace all state laws in the digital data privacy sphere to promote a more uniform scheme.[586]

Congress could alternatively take a more modest approach to state law. For example, Congress could enact a data protection framework that expressly preserves state laws in some ways and preempts them in others. A number of federal statutes preempt state laws that impose standards "different from" or "in addition to" federal standards, or allow the regulator in charge of the federal scheme some authority to approve certain state regulations.[587] These approaches would generally leave intact state schemes parallel to or narrower than the federal scheme.[588] For example, a statute could permit a state to provide for additional liability or different remedies for violation of a federal standard.[589] Congress could do the same with federal data protection legislation, using statutory language to try to ensure the protection of the provisions of state law that it sought to preserve.[590]

[584] *See, e.g.*, 29 U.S.C. § 1144(a) ("[T]he provisions of this subchapter and subchapter III shall supersede any and all State laws insofar as they may now or hereafter relate to any employee benefit plan…"); 49 U.S.C. § 14501(a)(1) ("No State or political subdivision thereof and no interstate agency or other political agency of 2 or more States shall enact or enforce any law, rule, regulation, standard, or other provision having the force and effect of law relating to. . . scheduling of interstate or intrastate transportation . . . ."); 49 U.S.C. § 41713(b)(1) ("Except as provided in this subsection, a State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier . . . .").

[585] Morales v. Trans World Airlines, 504 U.S. 374, 383–84 (1992).

[586] *See, e.g.*, S. 142, 116th Cong. § 6 (2019) ("This Act, including any regulations promulgated under section 4(a), shall supersede any provision of the law of a State relating to a covered provider that is subject to such a regulation, to the extent that the provision relates to the maintenance of—(1) records covered by this Act; or (2) any other personally identifiable information or personal identification information.").

[587] *See, e.g.*, 7 U.S.C. § 136v(b) ("Such State shall not impose or continue in effect any requirements for labeling or packaging in addition to or different from those required under this subchapter."); 21 U.S.C. § 360k(a) (providing that "no State . . . may establish or continue in effect with respect to a device . . . any requirement" that is "different from, or in addition to" the requirements of federal law, however, allowing the Secretary of HHS to exempt state laws which are more stringent than federal law).

[588] *See* Medtronic, Inc. v. Lohr, 518 U.S. 470, 495 (1996) ("While such a narrower requirement might be 'different from' the federal rules in a literal sense, such a difference would surely provide a strange reason for finding pre-emption of a state rule insofar as it duplicates the federal rule. The presence of a damages remedy does not amount to the additional or different 'requirement' that is necessary under the statute; rather, it merely provides another reason for manufacturers to comply with identical existing 'requirements' under federal law.").

[589] *See, e.g.*, Bates v. Dow Agrosciences LLC 544 U.S. 431, 448–50 (2005) (holding that Congress did not intend to deprive injured parties of state law remedies by language prohibiting requirements "in addition to or different from" the federal requirements).

[590] *See, e.g.*, H.R. 6547, 115th Cong. § 6 (2018) ("This Act and the regulations promulgated under this Act supercede a provision of law of a State or a political subdivision of a State only to the extent that such provision—(1) conflicts with this Act or such regulations, as determined without regard to section 2(d)(2);(2) specifically relates to the treatment of personal data or de-identified data; and (3) provides a level of transparency, user control, or security in the treatment of personal data or de-identified data that is less than the level provided by this Act and such regulations.").

First Amendment

Although legislation on data protection could take many forms, several approaches that would seek to regulate the collection, use, and dissemination of personal information online may have to confront possible limitations imposed by the First Amendment of the U.S. Constitution. The First Amendment guarantees, among other rights, "freedom of speech."[591] Scholars have split on how the First Amendment should be applied to proposed regulation in the data protection sphere. In one line of thinking, data constitutes speech, and regulation of this speech, even in the commercial context, should be viewed skeptically.[592] Other scholars have argued that an expansive approach would limit the government's ability to regulate ordinary commercial activity, expanding the First Amendment beyond its proper role.[593] This scholarly debate informs the discussion, but does not provide clear guidance on how to consider any particular proposed regulation.

The Supreme Court has never interpreted the First Amendment as prohibiting all regulation of communication. Instead, when confronting a First Amendment challenge to a regulation, a court asks a series of questions in order to determine whether a particular law or rule runs afoul of the complicated thicket of case law that has developed in this area. The first question courts face when considering a First Amendment challenge is whether the challenged regulation involves speech or mere non-expressive conduct. As the Supreme Court has explained, simply because regulated activity involves "communication" does not mean that it comes within the ambit of the First Amendment.[594] Where speech is merely a "component" of regulated activity, the government generally can regulate that activity without inviting First Amendment scrutiny.[595] For example, "a

[591] U.S. CONST. amend. I.

[592] *See, e.g.*, Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CAL. L. REV. 335, 356–65 (2017) (arguing for an expansive free speech doctrine, and acknowledging that this view would "threaten[] privacy regimes"); Jane R. Bambauer, *Is Data Speech?* 66 STAN. L. REV. 57, 112–13 (2014) (arguing that First Amendment protects right to create knowledge, acknowledging that this right would undermine hypothetical privacy regulations, such as the "Consumer Privacy Bill of Rights"); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000) (arguing that any First Amendment doctrine that protected a right to control others' communication of personally identifiable information would be contrary to the First Amendment).

[593] *See, e.g.*, Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1159–60 (2018) ("Behind these technologies are people and organizations who want to use the First Amendment as a deregulatory tool to protect business practices that affect the lives of many other people. In the United States, at last, the constitutional question is whether companies in the Second Gilded Age will be able to use the First Amendment guarantees of speech and press in the same way that industrial organizations used the constitutional idea of freedom of contract in the First Gilded Age."); Neil M. Richards, *Why Data Privacy Law is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1508 (2015) ("In a democratic society, the basic contours of information policy must ultimately be up to the people and their policy making representatives, and not to unelected judges. We should decide policy on that basis, rather than on odd readings of the First Amendment.").

[594] *See* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) ("Numerous examples could be cited of communications that are regulated without offending the First Amendment . . . . Each of these examples illustrates that the State does not lose its power to regulate commercial activity deemed harmful to the public whenever speech is a component of that activity.") (citing cases).

[595] *Id. See also* Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1766–67 (2004) (arguing that areas of regulation in which the First Amendment has not been applied, including "copyright, securities regulation, panhandling, telemarketing, antitrust, and hostile-environment sexual harassment," demonstrate the importance of the question of whether the First Amendment applies).

law against treason…is violated by telling the enemy the Nation's defense secrets," but that does not bring the law within the ambit of First Amendment scrutiny.[596]

Assuming the regulation implicates speech rather than conduct, it typically must pass First Amendment scrutiny.[597] However, not all regulations are subject to the same level of scrutiny. Rather, the Court has applied different tiers of scrutiny to different types of regulations. For example, the Court has long considered political and ideological speech at the "core" of the First Amendment—as a result, laws which implicate such speech generally are subject to strict scrutiny.[598] Pursuant to this standard, the government must show that such laws are narrowly tailored to serve a compelling state interest.[599] By contrast, the Court has historically applied less rigorous scrutiny to laws regulating "commercial speech."[600] Commercial speech is subject to a lower level of scrutiny known as the *Central Hudson* test, which generally requires the government to show only that its interest is "substantial" and that the regulation "directly advances the governmental interest asserted" without being "more extensive than necessary to serve that interest."[601]

These principles have provided general guidance to lower courts in deciding cases that intersect with data protection, but implicit disagreements between these courts have repeatedly demonstrated the difficulty in striking the balance between First Amendment interests and data-

[596] R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 389 (1992). *See also* Rumsfeld v. Forum for Academic and Institutional Rights, Inc., 547 U.S. 47, 62 (2006) ("The compelled speech to which the law schools point is plainly incidental to the Solomon Amendment's regulation of conduct, and 'it has never been deemed an abridgment of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed.'") (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949)).

[597] A possible exception involves a regulation of unprotected speech. In general, speech is protected under the First Amendment unless it falls within one of the narrow categories of unprotected speech recognized by the Supreme Court. *See* United States v. Stevens, 559 U.S. 460, 468–69 (2010) ("[T]he First Amendment has 'permitted restrictions upon the content of speech in a few limited areas,' and has never 'include[d] a freedom to disregard these traditional limitations.' These 'historic and traditional categories long familiar to the bar'—including obscenity, defamation, fraud, incitement, and speech integral to criminal conduct—are 'well-defined and narrowly limited classes of speech . . . .'" (internal citations omitted)). Even regulations aimed at unprotected speech are subject to some First Amendment limitations; for example, "a law may be invalidated as overbroad if 'a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep.'" *See* Washington State Grange v. Washington State Republican Party, 552 U.S. 442, 449 n.6 (2008)). *See also* CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion (2019).

[598] *See e.g.*, Citizens United v. FEC, 558 U.S. 310, 340 (2010) ("Laws that burden political speech are 'subject to strict scrutiny,' which requires the Government to prove that the restriction 'furthers a compelling interest and is narrowly tailored to achieve that interest.'" (citation omitted)); McIntyre v. Ohio Elections Com'n, 514 U.S. 334, 346 (1995) ("When a law burdens core political speech, we apply 'exacting scrutiny,' and we uphold the restriction only if it is narrowly tailored to serve an overriding state interest."); Buckley v. Valeo, 424 U.S. 1, 14–15 (1976) (per curiam) ("Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression."); West Virginia State Board of Educ. v. Barnette, 319 U.S. 624, 642 (1943) ("If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.").

[599] *See Citizens United*, 558 U.S. at 340.

[600] Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980). *Central Hudson* defines "commercial speech" as "expression related solely to the economic interest of the speaker and its audience." *Id.* at 561. The Court has also defined "commercial speech" as "speech which does 'no more than propose a commercial transaction.'" Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 762 (1976) (quoting Pittsburgh Press Co. v. Human Relations Comm'n, 413 U.S. 376, 385 (1973)).

[601] *Central Hudson*, 447 U.S. at 566. In addition, commercial speech must "concern lawful activity and not be misleading" to come within the protection of the First Amendment. *Id.*

protection regulation. For example, in 2001 in *Trans Union Corp. v. FTC*,[602] the D.C. Circuit upheld an FTC order that prohibited Trans Union from selling marketing lists containing the names and addresses of individuals. [603] The court assumed that disclosing or using the marketing lists was speech, not conduct, but concluded that the FTC's restrictions on the sale of the marketing lists generally concerned "no public issue," and, as such, was subject to "reduced constitutional protection."[604] The court derived its "no public issue" rule from the Supreme Court's case law on defamation, which generally views speech that is solely in the private interest of the speaker as being subject to lower First Amendment protection from defamation suits than speech regarding matters of a public concern.[605] Applying this "reduced constitutional protection" to the context of Trans Union's marketing lists, the court determined that the regulations were appropriately tailored.[606] While the *Trans Union* court did not cite to *Central Hudson*, other courts have gone on to apply similar reasoning to uphold data protection laws from constitutional challenge under the ambit of *Central Hudson*'s commercial speech test.[607]

In contrast with the relatively lenient approach applied to a privacy regulation in *Trans Union*, in *U.S. West v. FCC*,[608] the Tenth Circuit struck down FCC regulations on the use and disclosure of Consumer Proprietary Network Information (CPNI).[609] The regulations stated that telecommunications carriers could use or disclose CPNI only for the purpose of marketing products to customers if the customer opted in to this use.[610] The court determined that these provisions regulated commercial speech because they limited the ability of carriers to engage in consumer marketing.[611] Applying *Central Hudson*, the court held that although the government alleged a general interest in protecting consumer privacy, this interest was insufficient to justify the regulations. The panel ruled that the regulations did not materially advance a substantial state interest because the government failed to tie the regulations to specific and real harm, supported by evidence.[612] The court also concluded that a narrower regulation, such as a consumer opt-out, could have served the same general purpose.[613]

After the Tenth Circuit's decision in *U.S. West*, the FCC responded by making minor changes to its regulations, maintaining some elements of the opt-in procedure for the use of CPNI and reissuing them with a new record.[614] After this reissuance, the D.C. Circuit considered these modified-but-similar regulations in a 2009 case.[615] In that case, the D.C. Circuit upheld the

[602] 245 F.3d 809 (D.C. Cir. 2001), *cert denied*, 536 U.S. 915 (2002).

[603] *Id.* at 812.

[604] *Id.*

[605] *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 761-63 (1985).

[606] *Trans Union*, 245 F.3d at 812.

[607] *See e.g.*, Boelter v. Hearst Commc'ns, 192 F. Supp. 3d 427, 444 (S.D.N.Y. 2016) (concluding that sale of demographic information about consumers to "data miners and other third parties" was speech within the meaning of the First Amendment, but holding that it was nonetheless subject to regulation as commercial speech and subject to reduced protection as speech on a matter of "purely private concern").

[608] 182 F.3d 1224 (10th Cir. 1999)

[609] *Id.* at 1239-40. *See* § Common Carriers, *supra*, for a discussion of the current CPNI requirements.

[610] *U.S. West*, 182 F.3d at 1230.

[611] *Id.* at 1232.

[612] *Id.* at 1235–39. The government also asserted an interest in promoting competition, but the court held that this interest, standing alone would not be sufficient to overcome First Amendment concerns. *Id.* at 1237.

[613] *Id.* at 1239.

[614] Fed. Commc'ns Comm'n, Report and Order and Further Notice of Proposed Rulemaking, 07–22 (April 2, 2007).

[615] Nat'l Cable and Telecomms. Ass'n v. Fed Commc'ns Comm'n, 555 F.3d 996, 1000–02 (D.C. Cir. 2009).

regulations without attaching much significance to the FCC's changes, and apparently implicitly disagreeing with the Tenth Circuit about both the importance of the privacy interest at stake and whether the opt-in procedure was proportional to that interest.[616]

The Supreme Court's first major examination of the First Amendment in this context came in 2011. That year, the Court decided *Sorrell v. IMS Health, Inc.*,[617] a case that is likely to be critical to understanding the limits of any future data protection legislation. In *Sorrell*, the Court considered the constitutionality of a Vermont law that restricted certain sales, disclosures, and uses of pharmacy records.[618] Pharmaceutical manufacturers and data miners challenged this statute on the grounds that it prohibited them from using these records in marketing, thereby imposing what they viewed to be an unconstitutional restriction on their protected expression.[619]

Vermont first argued that its law should be upheld because the "sales, transfer, and use of prescriber-identifying information" was mere conduct and not speech.[620] The Court explained that, as a general matter, "the creation and dissemination of information are speech within the meaning of the First Amendment," and thus there was "a strong argument that prescriber identifying information is speech for First Amendment purposes."[621] Ultimately, however, the Court stopped short of fully embracing this conclusion, merely explaining that it did not matter whether the actual transfer of prescriber-identifying information was speech because the law nonetheless impermissibly sought to regulate the content of speech—the marketing that used that data, as well as the identities of speakers—by regulating an input to that speech.[622] As the Court explained, the Vermont law was like "a law prohibiting trade magazines from purchasing or using ink."[623]

Second, Vermont argued that, even if it was regulating speech, its regulations passed the lower level of scrutiny applicable to commercial speech.[624] The Court disagreed. The Court explained that the Vermont law enacted "content- and speaker-based restrictions on the sale, disclosure and use of prescriber identifying information" because it specifically targeted pharmaceutical manufacturers and prohibited certain types of pharmaceutical marketing.[625] As the Court stated in a previous case, "[c]ontent-based regulations are presumptively invalid" because they "raise[] the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace."[626] Further, the *Sorrell* Court observed that the legislature's stated purpose was to diminish the effectiveness of marketing by certain drug manufacturers, in particular those that

[616] *Id.* at 1001-02.

[617] 564 U.S. 552 (2011).

[618] *Id.* at 557.

[619] *Id.* at 565.

[620] *Id.* at 570 (noting the argument that "prescriber-identifying information" was a commodity with "no greater entitlement to First Amendment protection than 'beef jerky'").

[621] *Id.* at 570 (citing Bartnicki v. Vopper, 532 U.S. 514, 526–27 (2001)) ("On the other hand, the naked prohibition against disclosures is fairly characterized as a regulation of pure speech. . . . It is true that the delivery of a tape recording might be regarded as conduct, but given that the purpose of such a delivery is to provide the recipient with the text of recorded statements, it is like the delivery of a handbill or a pamphlet, and as such, it is the kind of 'speech' that the First Amendment protects.").

[622] *Sorrell*, 564 U.S. at 571.

[623] *Id.* (citing Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue, 460 U.S. 575, 591-93 (1983) (striking down ink and paper tax that targeted a small group of newspapers)).

[624] *Id.* at 571.

[625] *Id.* at 563–64.

[626] R.A.V. v. City of St. Paul, 505 U.S. 377 382-88 (1992).

promoted brand-name drugs, suggesting to the Court that the Vermont law went "beyond mere content discrimination, to actual viewpoint discrimination."[627] As a result, the Court concluded that some form of "heightened scrutiny" applied.[628] Nevertheless, the Court reasoned that, even if *Central Hudson*'s less rigorous standard of scrutiny applied,[629] the law failed to meet that standard because its justification in protecting physician privacy was not supported by the law's reach in allowing prescriber-identifying information's use "for any reason save" marketing purposes.[630]

Most of the lower courts outside the data protection and privacy context that have considered *Sorrell* have held that *Sorrell*'s reference to "heightened scrutiny" did not override the *Central Hudson* test in commercial speech cases, even where those cases include content- or speaker-based restrictions.[631] Others, however, have held that content- and speaker-based restrictions must comport with something more rigorous than the traditional *Central Hudson* test, but it is not clear what this new standard requires or where it leads to a different outcome than *Central Hudson*.[632] As a result, while *Sorrell*'s impact on privacy and data protection regulation has been considered by a few courts, no consensus exists on the impact it will have. [633] However, a few commentators have observed that the case will likely have an important effect on the future of privacy regulation, if nothing else, by having all but concluded that First Amendment principles apply to the regulation of the collection, disclosure, and use of personally identifiable information as speech, not conduct.[634]

With respect to such future regulation, policymakers will likely want, at the minimum, to meet the *Central Hudson* requirement of ensuring that any restrictions on the creation, disclosure or

[627] *Sorrell*, 564 U.S. at 565.

[628] *Id.*

[629] *Id.* at 572.

[630] *Id.* at 572–73.

[631] *See, e.g.*, Retail Digital Network, LLC v. Prieto, 861 F.3d 839, 849–50 (9th Cir. 2017) (en banc) ("[B]ecause *Sorrell* applied *Central Hudson*, there is no need for us to craft an exception to the *Central Hudson* standard."); 1-800-411-Pain Referral Serv., LLC v. Otto, 744 F.3d 1045, 1055 (8th Cir. 2014) ("The upshot is that when a court determines commercial speech restrictions are content- or speaker-based, it should then assess their constitutionality under *Central Hudson*."); Discount Tobacco City & Lottery, Inc. v. United States, 674 F.3d 509, 533 (6th Cir. 2012) (applying *Central Hudson*); Vugo, Inc. v. City of Chicago, 273 F. Supp. 3d 910, 916 n.4 (N.D. Ill. 2017) ("[T]he Seventh Circuit does not appear to view *Sorrell* as requiring a higher standard than *Central Hudson*.").

[632] *See* Wollschlaeger v. Governor of Fla., 848 F.3d 1293, 1308 (11th Cir. 2017) (concluding that record-keeping, inquiry, and anti-harassment provisions of state Firearm Owners Privacy Act failed to meet "heightened scrutiny"); Educ. Media Co. at Va. Tech, Inc. v. Insley, 731 F.3d 291, 298 (4th Cir. 2013) ("However, like the Court in *Sorrell*, we need not determine whether strict scrutiny is applicable here, given that, as detailed below, we too hold that the challenged regulation fails under intermediate scrutiny set forth in *Central Hudson*."); United States v. Caronia, 703 F.3d 149, 164–167 (2d Cir. 2012) (concluding that content- and speaker-based restrictions in drug misbranding case under the FDCA are subject to "heightened scrutiny" but concluding that they failed even the *Central Hudson* test).

[633] *See, e.g.*, Chamber of Commerce for Greater Philadelphia v. City of Philadelphia, 319 F. Supp. 3d 778, 784-85 (E.D. Pa. 2018) (after discussing how *Sorrell* has created a "lack of clarity around the commercial speech doctrine," concluding that intermediate scrutiny applied to government prohibition on asking prospective employees about wage history) (citing cases); Boelter v. Hearst Commc'ns, 192 F. Supp. 3d 427, 447 (S.D.N.Y. 2016) (evaluating the constitutionality of the Video Rental Privacy Act); King v. Gen. Info. Servs., 903 F. Supp. 2d 303, 311–13 (E.D. Pa. 2012) (holding that information disseminated in consumer report was speech, but law restricting disclosure of certain information was commercial speech analyzed under *Central Hudson*).

[634] *See, e.g.*, Richards, *supra* note 593 at 1506 ("Before *Sorrell*, there was a settled understanding that general commercial regulation of the huge data trade was not censorship"); Ronald J. Krotoszynski, Jr., *The Polysemy of Privacy*, 88 IND. L. J. 881, 883 n.6 (2013) (noting that, post *Sorrell*, "the First Amendment, and more specifically the commercial speech doctrine, make the validity of such privacy protection open to serious constitutional doubts").

use of information are justified by a substantial interest and that the regulations are no more extensive than necessary to further that interest.[635] To illustrate, the Court in *Sorrell* identified HIPAA[636] as a permissible "privacy" regulation because it allowed "the information's sale or disclosure in only a few narrow and well-justified circumstances."[637] This dictum suggests that Congress is able to regulate in the data protection sphere as long as it avoids the pitfalls of the law in *Sorrell*. However, it may not always be easy to determine whether any given law involves speaker or content discrimination. In *Sorrell* itself, for instance, three dissenting Justices argued that the content and speaker discrimination that took place under the Vermont law was inevitable in any economic regulation.[638] As a result, resolving these issues as data privacy legislation becomes more complex is likely to create new challenges for legislators.

Conclusion

The current legal landscape governing data protection in the United States is complex and highly technical, but so too are the legal issues implicated by proposals to create unified federal data protection policy. Except in extreme incidents and cases of government access to personal data, the "right to privacy" that developed in the common law and constitutional doctrine provide few safeguards for the average internet user.[639] Although Congress has enacted a number of laws designed to augment individual's data protection rights, the current patchwork of federal law generally is limited to specific industry participants, specific types of data, or data practices that are unfair or deceptive.[640] This patchwork approach also extends to certain state laws.[641] Seeking a more comprehensive data protection system, some governments—such as California and the EU—have enacted wide-ranging laws regulating many forms of personal data.[642] Some argue that Congress should consider creating similar protections in federal law,[643] but others have criticized the EU's and California's approach to data protection.[644]

Should the 116th Congress consider a comprehensive federal data protection program, its legislative proposals may involve numerous decision points and legal considerations. An initial decision point is the scope and nature of any legislative proposal. There are numerous data protection issues that could be addressed in any future legislation,[645] and different possible approaches for addressing those issues (such as using a "prescriptive" or "outcome-based"

[635] *See Boelter*, 192 F. Supp. 3d at 447.

[636] *See supra* at § Health Insurance Portability and Accountability Act (HIPAA).

[637] *Sorrell*, 564 U.S. at 573.

[638] *Id.* at 590 ("If the Court means to create constitutional barriers to regulatory rules that might affect the content of a commercial message, it has embarked upon an unprecedented task—a task that threatens significant judicial interference with widely accepted regulatory activity. . . . Nor would it ease the task to limit its 'heightened' scrutiny to regulations that only affect certain speakers. As the examples that I have set forth illustrate, many regulations affect only messages sent by a small class of regulated speakers, for example, electricity generators or natural gas pipelines.") (Breyer, J., dissenting).

[639] *See supra* § Origins of American Privacy Protection.

[640] *See supra* § Federal Data Protection Law.

[641] *See supra* § State Data Protection Law

[642] *See supra* §§ *id.*; GDPR Provisions and Requirements.

[643] *See supra* note 491.

[644] *See supra* note 522.

[645] *See supra* § Considerations for Congress.

approach).[646] Other decision points may include defining the scope of any protected information[647] and determining the extent to which any future legislation should be enforced by a federal agency.[648] Further, to the extent Congress wants to allow individuals to enforce data protection laws and seek remedies for the violations of such laws in court, it must account for Article III's standing requirements. Under the Supreme Court's 2016 *Spokeo Inc. v. Robins* decision, plaintiffs must experience more than a "bare procedural violation" of a federal privacy law to satisfy Article III and to sue to rectify a violation of that law.[649] Federal preemption also raises complex legal questions—not only of *whether* to preempt state law, but what form of preemption Congress should employ.[650] Finally, from a First Amendment perspective, Supreme Court jurisprudence suggests that while some "privacy" regulations are permissible, any federal law that restricts protected speech, particularly if it targets specific speakers or content, may be subject to more stringent review by a reviewing court.[651]

[646] *See supra* § Prescriptive Versus Outcome-Based Approach.

[647] *See supra* § Defining Protected Information and Addressing Statutory Overlap.

[648] *See supra* § Agency Enforcement.

[649] *See supra* § Private Rights of Action and Standing.

[650] *See supra* § Preemption.

[651] *See supra* § First Amendment.

Appendix. Summary of Federal Data Protection Laws

Federal Law	Information Federal Law protects	Covered Persons Under Federal Law	Nature of the Regulations	Agencies with Civil Enforcement Role	Criminal Penalties	Private Right of Action
Gramm-Leach-Bliley Act (GLBA)	Nonpublic personal information (NPI)	Financial institutions	Consumer opt-out requirement for data sharing Consumer disclosure requirements Data security requirements	Consumer Financial Protection Bureau (CFPB), Federal Trade Commission (FTC), federal banking agencies	Yes	No
Health Insurance Portability and Accountability Act (HIPAA)	Protected health information (PHI)	Healthcare providers, health plans, and health care clearinghouses	Consumer consent requirement for data sharing Consumer disclosure requirements Data security and data breach disclosure requirements	Department of Health and Human Services (HHS)	Yes	No
Fair Credit Reporting Act (FCRA)	Consumer reports	Credit Reporting Agencies (CRAs), furnishers of information to CRAs, and users of consumer reports issued by CRAs	Accuracy and use requirements for consumer reports Consumer disclosure requirements	CFPB, FTC	Yes	Yes
The Communications Act	Customer proprietary network information (CPNI) Personally identifiable information (PII)	Common carriers Cable operators and satellite carriers	Consumer consent requirement for data sharing Consumer disclosure requirements Data security requirements	Federal Communications Commission (FCC)	Yes	Yes

Federal Law	Information Federal Law protects	Covered Persons Under Federal Law	Nature of the Regulations	Agencies with Civil Enforcement Role	Criminal Penalties	Private Right of Action
Video Privacy Protection Act (VPPA)	Personally identifiable information (PII)	Video tape service providers	Consumer consent requirement for data sharing	None	No	Yes
Family Educational Rights and Privacy Act (FERPA)	Education records	Educational agencies or institutions receiving federal funds	Consumer consent requirement for data sharing Consumer disclosure requirements	Department of Education (DOE)	No	No
Federal Securities Laws	N/A	Publicly traded companies and any other companies required to file regular reports with the SEC	Possible data security and data breach disclosure requirements	Securities and Exchange Commission (SEC)	Yes	Yes
Children's Online Privacy Protection Act (COPPA)	Individually identifiable information collected online from a child under the age of thirteen	Operators of websites or online services that (1) direct their website or service to children, or (2) have actual knowledge they are collecting personal information from a child	Consumer consent requirement for data collection and sharing Consumer disclosure requirements Data security requirements	FTC	No	No

Federal Law	Information Federal Law protects	Covered Persons Under Federal Law	Nature of the Regulations	Agencies with Civil Enforcement Role	Criminal Penalties	Private Right of Action
Electronic Communications Privacy Act (ECPA)	Wiretap Act: Wire, oral, or electronic communications in transit Stored Communications Act (SCA): Electronic communications in storage Pen Register Act: Non-content information related to a communication	All persons or entities	Authorization requirement for intercepting communications in transit or accessing stored communications	None	Yes	Yes (except Pen Register Act)
Computer Fraud and Abuse Act (CFAA)	Information contained on a "protected computer"	All persons or entities	Authorization requirement for accessing information on a protected computer	None	Yes	Yes
Federal Trade Commission Act (FTC Act)	n/a	All persons or commercial entities other than common carriers, certain financial institutions, and nonprofits	Data privacy and security policies and practices must not be "unfair or deceptive"	FTC	No	No

Federal Law	Information Federal Law protects	Covered Persons Under Federal Law	Nature of the Regulations	Agencies with Civil Enforcement Role	Criminal Penalties	Private Right of Action
Consumer Financial Protection Act (CFPA)	n/a	All persons who (1) offer or provide a consumer financial product or service ("covered persons") or (2) provide a "material service" to a covered person in connection with providing the consumer financial product or service ("service providers")	Data privacy and security policies and practices must not be "unfair, deceptive, or abusive"	CFPB	No	No

Source: Congressional Research Service, based on the sources cited in this report.

Author Information

Stephen P. Mulligan
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Wilson C. Freeman
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.