Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated October 12, 2022

Data Protection and Privacy Law: An Introduction

Recent controversy surrounding how third parties protect the privacy of individuals in the digital age has raised national concerns over legal protections of Americans' electronic data. The current legislative paradigms governing cybersecurity and data privacy are complex and technical and lack uniformity at the federal level. This In Focus provides an introduction to data protection laws and an overview of considerations for Congress. (For a more detailed analysis, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.)

Defining *Data Protection*

As a legislative concept, data protection 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). Historically, many laws addressed these issues separately, but more recent data protection initiatives indicate a trend toward combining data privacy and security into unified legislative schemes.

Federal Data Protection Laws

While the Supreme Court has interpreted the Constitution to provide individuals with a right to privacy, this right generally guards only against government intrusions. Given the limitations in constitutional law, Congress has enacted a number of federal laws designed to provide statutory protections of individuals' personal information. However, these statutory protections are not comprehensive in nature and primarily regulate certain industries and subcategories of data. These laws—which differ based on their scope, who enforces them, and their associated penalties—include:

- **Children's Online Privacy Protection Act:** provides data protection requirements for children's information collected by online operators.
- **Communications Act of 1934:** includes data protection provisions for common carriers, cable operators, and satellite carriers.
- **Computer Fraud and Abuse Act:** prohibits the unauthorized access of protected computers.
- **Consumer Financial Protection Act:** regulates unfair, deceptive, or abusive acts in connection with consumer financial products or services.
- **Electronic Communications Privacy Act:** prohibits the unauthorized access or interception of electronic communications in storage or transit.
- **Fair Credit Reporting Act:** covers the collection and use of data contained in consumer reports.
- **Federal Securities Laws:** may require data security controls and data breach reporting responsibilities.
- **Federal Trade Commission (FTC) Act:** prohibits unfair or deceptive acts or practices.
- **Gramm-Leach-Bliley Act:** regulates financial institutions' use of nonpublic personal information.
- **Health Insurance Portability and Accountability Act:** regulates health care providers' collection and disclosure of protected health information.
- **Video Privacy Protection Act:** provides privacy protections related to video rental and streaming.

Of these laws, the FTC Act's prohibition of "unfair or deceptive acts or practices" (UDAPs) is especially important in the context of data protection. The FTC has brought hundreds of enforcement actions based on the allegation that companies' data protection practices violated this prohibition. One of the well-settled principles in FTC practice is that companies are bound by their data privacy and data security promises. The FTC has taken the position that companies act *deceptively* when they handle personal information in a way that contradicts their posted privacy policies or other statements or when they fail to adequately protect personal information from unauthorized access despite promises that they would do so. In addition to broken promises, the FTC has maintained that certain data protection practices are *unfair*, such as when companies have default privacy settings that are difficult to change or when companies retroactively apply revised privacy policies. However, while the FTC's enforcement of the UDAP prohibition fills in some statutory gaps in federal data protection law, its authority has limits. In contrast to many of the sector-specific data protection laws, the FTC Act does not require companies to abide by specific data protection policies or practices and has historically been interpreted not to reach entities that have not made explicit promises concerning data protection. In August 2022, the FTC issued an advance notice of proposed rulemaking and request for public comment (87 FR 51273) on whether it should implement more comprehensive data protection regulations.

State Data Protection Laws

Adding to the complex patchwork of federal laws, some states have developed their own statutory frameworks for data protection. Every state has passed some form of data breach response legislation, and many states have consumer protection laws of various types. In addition, California created one of the first state-level comprehensive data protection regimes through the California Consumer Privacy Act (CCPA).

The CCPA governs any company doing business in California that meets certain minimum thresholds, including companies with websites accessible there. The law provides consumers with three main "rights." First, consumers have a *right to know* information that businesses have collected or sold about them, requiring businesses to inform consumers about the personal data being collected. Second, the CCPA provides consumers with a *right to opt out* of the sale of their personal information. Third, the CCPA gives consumers the right, in certain cases, to request that a business delete any information collected about the consumer (i.e., *right to delete*). The CCPA is enforced via civil penalties in enforcement actions brought by the California attorney general.

Foreign Data Protection Law

In addition to U.S. states such as California, some foreign nations have enacted comprehensive data protection legislation. The EU, in particular, has long applied a more wide-ranging data protection regulatory scheme, and its data protection law, the General Data Protection Regulation (GDPR), has served as a model for other jurisdictions developing data protection policy. The GDPR requires any entity that processes personal data to identify a legal basis for its action (such as consent or "legitimate interests"), and it enumerates eight data privacy rights afforded to individuals. The regulation also includes data breach notification requirements, data security standards, and conditions for cross-border data flows outside the EU.

Issues for Congress

Data protection policy proposals are constantly evolving, and there is no agreed-upon menu of data protection options. Depending on the contours of a particular proposal, federal-level data protection legislation could implicate various legal concerns, including constitutional limitations.

Conceptual Issues. A primary conceptual point of debate in data protection policy is whether to use a "prescriptive" approach in which the law defines data protection rules and obligations or an "outcome-based" model where legislation focuses on the outcomes of organizational practices rather than dictating what those practices should be. Both the GDPR and the CCPA use a prescriptive approach, but some observers advocate for an outcome-based paradigm. Another overarching issue 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. Whereas some federal proposals would cover all "personal" information, others have sought to avoid dual layers of regulation by stating that the proposed requirements would not apply if regulated by existing federal privacy law.

Enforcement. Agency enforcement is another key issue. There are multiple federal agencies responsible for enforcing the myriad federal data protection laws, such as the FTC, Consumer Financial Protection Bureau, Federal Communications Commission, and Department of Health and Human Services. Of these agencies, the FTC is often viewed as the leading data protection enforcement agency given its significant experience. However, there are several legal constraints on its enforcement ability. In particular, the FTC cannot seek monetary penalties for first-time UDAP violations but may seek only cease-and-desist orders or injunctions. It may generally seek only civil penalties after a company has violated a cease-and-desist order or settlement agreement. The FTC also lacks jurisdiction over certain entities including banks, nonprofits, and common carriers.

Federalism and Preemption. Another legal issue Congress may need to consider with respect to any federal data protection program 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. If Congress seeks to adopt a relatively comprehensive system for data protection, Congress could expressly preempt many state laws related to a particular subject matter. Congress could alternatively take a more modest approach to state law by expressly preserving state laws in some ways and preempting them in others. Congress has the option to generally leave intact state schemes parallel to or narrower than the federal scheme or to render such parallel regulation invalid.

First Amendment. Although legislation on data protection could take many forms, several approaches that would 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. While the Supreme Court has recognized that data protection regulation can implicate the First Amendment, this does not mean such laws would be invalid. Instead, the validity of a given information privacy law may depend upon the nature of the law it regulates (e.g., commercial matters can be subject to less scrutiny from a court) and whether the law singles out particular viewpoints or speakers for regulation.

Private Rights of Action. Finally, Congress may seek to establish a private right of action allowing a private plaintiff to bring a lawsuit based on a violation of the new data protection law. However, it may be difficult to prove that someone has been harmed by many of the violations that might occur under a hypothetical data protection regime. Victims of data breaches and other privacy violations, generally speaking, are not always clearly harmed. This obstacle could run up against the limits of the federal courts' "judicial power" under Article III of the U.S. Constitution. Any federal private right of action, therefore, would be limited in its application to cases in which individuals can show a concrete and particularized harm from a statutory violation.

Stephen P. Mulligan, Legislative Attorney
Chris D. Linebaugh, Legislative Attorney

IF11207

Disclaimer