Reforming the U.S. Approach to Data Protection and Privacy

Rather than a comprehensive legal protection for personal data, the United States has only a patchwork of sector-specific laws that fail to adequately protect data. Congress should create a single legislative data-protection mandate to protect individuals' privacy.

Report *by* Nuala O'Connor

January 30, 2018

Trading information about Equifax and the company logo are displayed on a screen where the stock is traded on the floor of the New York Stock Exchange in New York on September 8, 2017. Brendan McDermid/Reuters

Introduction

Half of all Americans believe their personal information is less secure now than it was five years ago, and a sobering study from the Pew Research Center reveals how little faith the public has in organizations, whether governmental or private-sector, to protect their data—and with good reason. In 2017, there was a disastrous breach at Equifax, Yahoo's admission that billions of its email accounts were compromised, Deep Root Analytics' accidental leak of

personal details of nearly two hundred million U.S. voters, and Uber's attempt to conceal a breach that affected fifty-seven million accounts. Individuals are left stymied about what action they can take, if any, to protect their digital assets and identity.

Yet record-shattering data breaches and inadequate data-protection practices have produced only piecemeal legislative responses at the federal level, competing state laws, and a myriad of enforcement regimes. Most Western countries have already adopted comprehensive legal protections for personal data, but the United States—home to some of the most advanced, and largest, technology and data companies in the world—continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data. U.S. citizens and companies suffer from this uneven approach—citizens because their data is not adequately protected, and companies because they are saddled with contradictory and sometimes competing requirements. It is past time for Congress to create a single legislative data-protection mandate to protect individuals' privacy and reconcile the differences between state and federal requirements.

A Patchwork of Existing Protections

The United States lacks a single, comprehensive federal law that regulates the collection and use of personal information. Instead, the government has approached privacy and security by regulating only certain sectors and types of sensitive information (e.g., health and financial), creating overlapping and contradictory protections.

The rules that govern health information illustrate this problem. The Health Insurance Portability and Accountability Act (HIPAA), the United States' primary health privacy and security law, only applies to "covered entities" holding "protected health information." Federal regulators acknowledge [PDF] that most Americans have no grasp of when their health information is protected by the law and when it is not—or what security standards apply in either case. Separate privacy laws govern specific areas of the U.S. health-care system [PDF]: student immunizations and other school health records are generally covered by the Family

Educational Rights and Privacy Act (FERPA), which was enacted in 1974, when student records existed in physical file cabinets and not digital clouds. FERPA, in turn, intersects with and sometimes conflicts with the Children's Online Privacy Protection Act (COPPA), which does protect data, but only of children under the age of thirteen.

> "Widespread collection of personal information puts [people's] privacy and security at risk."

State laws add to this patchwork, particularly with respect to data breaches. Many states recognize that widespread collection of personal information [PDF] puts their residents' privacy and security at risk. Starting with California, which enacted the first data-breach notification law in 2003, forty-eight states have passed laws that require individuals to be notified if their information is compromised. These laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and even what constitutes a breach. Notification requirements also vary: New Jersey requires that the state police cybercrime unit be notified, while Maryland requires that the state attorney general be notified before any affected individual is.

Enforcement of these laws is also complicated. While state attorneys general have an important role to play, the Federal Trade Commission (FTC) considers itself the "top cop on the privacy beat." The FTC has the general power to prohibit "unfair and deceptive trade practices" under Section 5 of the FTC Act, and has attempted to establish a data-security baseline through over sixty different enforcement actions. However, companies have begun to aggressively push back

against the FTC's legal authority to police data-security practices, and the FTC has limited jurisdiction over banks, insurance companies, nonprofit entities, and even some internet service providers.

The Challenge of Preventing and Responding to Data Breaches

Experienced security professionals advise even the most sophisticated organizations that they will eventually experience a breach. Even organizations with multiple layers of digital and physical security are vulnerable to the persistent threats of commercial and governmental intrusion, as well as inept or intentionally malicious insiders. Perfect security is impossible, and the informational injuries that can result from the collection and (mis)use of data are constantly evolving.

As a result, many lawmakers sought to respond to the Equifax breach and similar breaches by reassessing data-breach notification rules. Members of Congress are reintroducing data-breach protection proposals, and industry voices have suggested that the United States could have finally reached the "tipping point" that will lead to the creation of a single national data-breach notification standard.

> "Breach-notification laws . . . place the burden on the individuals whose information has been compromised."

cfr

This is a common refrain after every headline-making breach, but enacting data-breach legislation, while well-intentioned, will likely result in little meaningful improvement for data-security practices. While breach-notification laws shame companies that do not disclose breaches, they ultimately place the burden on the individuals whose information has been compromised: they need to maintain ongoing vigilance about identity theft and other fraud, some of which could occur years after the initial incident. Eliminating conflicting state notice provisions at the federal level, while simplifying the experience for both consumer and institution, does nothing to address this problem.

Companies need clearer rules, and individuals need to be able to incentivize companies to secure data. Most data breaches, even with the costs of disclosure and response and the attendant reputational harm, do not result in significant financial harm to companies. Even when regulators such as the FTC get involved, the likelihood of any monetary fine is small. A more comprehensive legal framework is needed: one that offers a mix of incentives for better security practices, disclosures, and individual protections.

Toward a Baseline Privacy and Security Proposal

The twenty-first-century economy will be fueled by personal data. But it is not yet clear what rules will govern this information, with whom information will be shared, and what protections will be put in place. A baseline data-protection law would provide a legal framework for answering these questions.

Such a proposal is not new. The FTC has continually called on [PDF] Congress to enact flexible and technologically neutral privacy and security laws, and nearly six years ago the Barack Obama administration put forward a blueprint for its Consumer Privacy Bill of Rights, based on Fair Information Practice Principles (FIPPs). The FIPPs are generally thought of as processes and procedures that organizations should implement; the Privacy Bill of Rights recognized that individual Americans have an ongoing interest in how information about them is collected, used, and shared by companies and government entities alike.

The rights proposed by the Obama administration were widely embraced by the advocacy community and civil society. However, the Obama administration's proposal was a victim of bad timing and lost momentum. Enamored with Silicon Valley, the administration largely let the industry craft its own rules, and a draft legislative bill was quietly put forward only three years after the initial proposal. Since then, data practices across all industry sectors have continued to fall short of individual privacy and security expectations.

> "Lawmakers' failure to provide users with a set of privacy rights has made the United States a global outlier."

The Donald J. Trump administration appears to have little appetite for technology policy or legal regulation in general, and lawmakers' continuing failure to provide users with a set of privacy rights has also made the United States a global outlier. While the U.S. legal framework on personal data has not meaningfully changed in several decades, the European Union has enacted multiple data-protection directives. With the revised General Data Protection Regulation (GDPR), the European Union has become the focal point of the global dialogue on individual data privacy. In contrast to U.S. law, EU law protects all personal data, regardless of who collects it or how it is processed. Other advanced economies, such as Canada, Israel, and Japan, have pivoted toward creating privacy regimes that are compatible with the EU's GDPR rather than with the patchwork approach of the United States. This puts U.S. companies at a disadvantage globally as emerging economies adopt simpler, and often more EU-style, comprehensive approaches.

cfr Recommendations

The U.S. Congress should join other advanced economies in their approach to data protection by creating a single comprehensive data-protection framework. Meaningful federal laws and regulations should seek to resolve the differences among the existing federal and state legal rights and responsibilities. This would not only simplify compliance for U.S. companies, but would also strengthen and bring the United States in line with emerging data-protection norms. Congress could implement an effective baseline privacy regime with at least the following four qualities.

First, the law should cover all institutions, not just tech companies, credit-rating agencies, and other narrow sectors of the economy. Data protection is not only part of corporate social responsibility in a digital age, it is also both an institutional risk and an essential compliance function for any organization that collects, uses, or shares personal information or other potentially sensitive consumer data.

Second, the law should harmonize the inconsistencies and fill the gaps created by the existing sectoral approach. Health information is sensitive regardless of whether it is input into a consumer application, generated by a wearable device, or conveyed to a medical professional. A baseline privacy law could polish away the inconsistent consent requirements, access rights, and security protections around health information that exist in between and outside of HIPAA, FERPA, and COPPA, for example.

> “Incentives for companies to protect data should skew toward prevention, rather than self-flagellating disclosures.”

cfr

Third, incentives for companies to protect data should skew toward prevention, rather than self-flagellating disclosures. Disclosure after the fact only helps the legal and compliance industries that have cropped up in the wake of recent breaches. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals. Companies should offer easy-to-use individual access, correction, and deletion mechanisms for users' data, and documented risk assessments and other compliance requirements, which leave a paper trail. When these mechanisms are backed by the force of law, companies are put on notice that they need to prioritize data security, which in turn gives privacy and security professionals and consumer advocates more leverage to push for better industry practice. If the United States adopted the significant fines for noncompliance seen in the European Union's GDPR, corporate practice could be reshaped—for not just major technology firms but also small and medium-sized enterprises and nonprofit entities.

Fourth, the U.S. legal framework should recognize and provide mechanisms to address the harms that result from privacy violations. Lawmakers and courts recognize the harm of breaches, but the definition of a "privacy harm" should be expanded. Identity theft is one such harm, but so too are the inconveniences suffered by affected individuals and their gnawing sense that they lack control over their "digital selves." These less quantifiable harms that result from the exposure of bits and bytes of individuals' personal lives should be recognized by law: as the depths of these harms are plumbed and addressed over time, individuals should be afforded a private right of action to hold companies accountable, and regulators should have the ability to penalize entities that flout their duty to be responsible stewards of personal information. Jack Balkin, the director of Yale Law School's Information Society Project, has suggested that companies be thought of as "information fiduciaries" and proposed a grand bargain that would extend a duty of care for personal information in exchange for legal certainty and safe harbors for industry.

cfr

A simpler and more comprehensive approach to individual digital dignity is warranted, especially after this past year of increasing magnitude of breaches and digital stewardship failures. A baseline privacy framework could ensure that all companies become responsible and ethical stewards of data, bring the United States in line with global standards, and better protect the data of U.S. citizens.

This Cyber Brief is part of the Digital and Cyberspace Policy program. ***The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.***