Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

What Legal Obligations do Internet Companies Have to Prevent and Respond to a Data Breach?

Chris D. Linebaugh
Legislative Attorney

October 25, 2018

Recently, large Internet companies—i.e., companies that do most of their business on the Internet, such as social media platforms or search engines—have made headlines after failing to secure their users' personal information. For example, on September 28, 2018, Facebook announced a security breach affecting tens of millions of user accounts. According to Facebook, hackers exploited a vulnerability in its code that allowed them to steal "access tokens," which are the "equivalent of digital keys" that "keep people logged in to Facebook." Facebook later disclosed that, of the affected accounts, hackers accessed the names and contact details of 15 million users and the biographical information of another 14 million users. Just over a week after Facebook's breach, on October 8, 2018, Google, in announcing the end of its social network Google+, disclosed that a software glitch exposed the personal data associated with up to 500,000 Google+ accounts. Google explained that it discovered and resolved the glitch in March 2018 and that there was no evidence anyone misused the exposed data. The Internet search giant reportedly made an initial decision not to disclose the incident, before reversing course and shutting down the Google+ platform following a Wall Street Journal investigation.

These incidents raise the question: what legal obligations do Internet companies have to prevent and respond to data breaches? This Sidebar considers the answer to this question under federal and state law. The Sidebar then discusses several factors Congress might consider when weighing future legislation.

Federal and State Law on Preventing Data Breaches

In contrast to the European Union, which recently adopted a wide-reaching data privacy law called the General Data Protection Regulation (GDPR), there is no comprehensive federal law requiring all entities or individuals who collect personal information electronically to maintain the security of such data. Rather, the few federal data security laws that do exist are primarily directed at specific industries. For

Congressional Research Service
7-5700
www.crs.gov
LSB10210

instance, the Gramm-Leach Bliley Act (GLBA) and its implementing regulations require financial institutions to maintain comprehensive information security programs to safeguard customers' nonpublic personal information. Similarly, the regulations implementing the Health Insurance Portability and Accountability Act (HIPAA) require covered healthcare companies to maintain safeguards to prevent data security threats to electronic "protected health information." Other sector-specific federal laws that require certain entities to adopt data security measures or limit the circumstances under which those entities may disclose personal information include the Driver's Privacy Protection Act (governing state departments of motor vehicles), the Privacy Act of 1974 (governing federal agencies), the Fair Credit Reporting Act (governing credit reporting agencies), and the Children's Online Privacy Protection Act (COPPA) (governing online operators that direct their services at children or knowingly collect children's data).

Notably, no federal data security law specifically directs Internet companies falling outside the reach of these sector-specific statutes to adopt security measures designed to protect personal data from unauthorized hacks or unintentional exposure. Such companies may nonetheless have obligations under federal consumer protection laws. In particular, the Federal Trade Commission (FTC) Act empowers the FTC to prevent companies from engaging in "unfair or deceptive acts or practices" (commonly referred to as "UDAPs") "in or affecting commerce." The FTC Act allows the FTC to seek equitable relief, including preliminary or permanent injunctions, in UDAP enforcement actions. The Commission may, however, only seek civil monetary penalties if the party has violated a consent decree or a regulation defining a specific type of conduct as a UDAP.

The FTC has used its UDAP authority to bring a number of enforcement actions against companies that fail to invest adequately in data security. Often, the FTC maintains that such failures are "deceptive" because they contradict companies' past security promises. For instance, in 2014 the social media company Snapchat settled FTC charges alleging that its failure to secure its "Find Friends" feature allowed hackers to compile 4.6 million user names and phone numbers. The FTC alleged that Snapchat acted deceptively because the company's privacy policy said that it had taken reasonable data security measures. Along with "deceptive" claims, the FTC has also recognized that failing to safeguard user data adequately may be "unfair." The FTC Act provides that an act or practice is only "unfair" if it "causes or is likely to cause substantial injury to consumers," is not "reasonably avoidable by consumers," and is "not outweighed by countervailing benefits." At least one court has agreed that a company's failure to safeguard user data may, in some circumstances, meet this standard. However, the extent to which the FTC may rely on its "unfairness" authority is unclear. A recent Eleventh Circuit decision suggests that the FTC needs to allege specific failures and remedies in order to successfully issue a cease and desist order based on a company's "unfair" data security measures. In that case, *LabMD v. FTC*, the court noted that the FTC's order "contains no prohibitions" but "commands [the company] to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness." The court concluded that such an order is unenforceable, reasoning that penalizing a company for failing to comply with an imprecise standard "may constitute a denial of due process" and that the order "effectually charges the district court [enforcing the order] with managing the overhaul."

In addition to the FTC Act's UDAP provision, Internet companies must comply with a number of state laws regulating data security. Thus far, at least 22 states have enacted laws of general applicability governing data security. These statutes generally require companies to maintain "reasonable" security procedures to protect personal information. While many state laws do not specify what constitutes a "reasonable" procedure, some states, like Massachusetts, specify in detailed regulations the types of measures required. State consumer protection laws and common law causes of action—such as negligence, negligence per se (often based on federal statutes, like FCRA or GLBA), negligent misrepresentation, fraud, or breach of contract—may also apply. For instance, following Home Depot's data breach affecting more than 50 million cardholders, consumers sued the company alleging negligence, negligence per se, and violations of multiple state consumer protection laws.

Federal and State Law on Responding to Data Breaches

Federal laws and regulations impose relatively few obligations on companies that suffer data breaches and are generally directed at specific sectors, such as the banking (under GLBA interagency guidance) or healthcare industries (under HIPAA regulations). However, as the Security and Exchange Commission (SEC) indicated in February 2018 guidance, publicly traded companies may be required to report breaches in their public filings with the SEC because federal securities laws and regulations prohibit companies from omitting material facts necessary to make statements made in connection with the purchase or sale of any security "not misleading." The SEC guidance does not articulate a bright-line approach for determining when companies must report a data breach and does not include any categorical exemptions, such as exemptions for *de minimis* breaches. Rather, the guidance directs companies to consider whether a breach is material to investors in light of factors such as the nature of the compromised information, potential magnitude of the breach, and range of harm caused by the breach. Since issuing the guidance, the SEC has brought at least one enforcement action against a company for failure to report a data breach. In April 2018, Yahoo! Inc.'s successor company agreed to pay a $35 million penalty to settle SEC charges that the company mislead investors by failing to report a major 2014 data breach in which hackers acquired personal data associated with hundreds of millions of user accounts.

Although there are few federal laws regulating responses to data breaches, the states have addressed the issue. As of March 2018, all 50 states have enacted data breach response laws. The laws' specifics vary significantly, however, creating, in the view of some commentators, uncertainty for companies responding to data breaches. For instance, some states require notification after any breach of non-encrypted personal information (e.g., New York), while others require notification only if the breach is likely to cause "substantial harm" to individuals (e.g., Alabama). Furthermore, some states require companies to notify affected individuals within a certain time frame, such as 30 days (e.g., Florida), 45 days (e.g., Washington), or 60 days (e.g., Delaware), while others simply require companies to provide notice "without unreasonable delay" (e.g., California). State laws also differ in how they define personal information, whether and when companies must notify any state agencies, the required contents of the notice, the required method of notice (e.g., some states allow for substitute notice, while others do not), and who can bring actions for violations (while most states only empower the attorney general to enforce violations, some states allow private causes of actions in addition to attorney general enforcement).

Despite their differences, state laws generally require companies to notify affected individuals regardless of whether the breach resulted from an inadequate data security program. State laws typically define a triggering breach as involving the "unauthorized acquisition" of personal information. These definitions generally do not require that the "unauthorized acquisition" be caused by companies' security failures, nor do they necessarily contain carve-outs for companies with adequate data security programs in place (e.g., California, Texas, New York). Because breaches are typically defined as the "unauthorized acquisition" of personal data, companies generally are not required to notify individuals when there is a lack of evidence that the company's failure resulted in a third party possessing personal data without authorization. Nonetheless, a handful of states (Puerto Rico, New Jersey, Florida, and Connecticut) depart from this general rule by defining data breaches to include the "unauthorized access" to personal information. As some commentators have noted, "unauthorized access" may be a lower standard that covers situations where personal data is merely exposed to unauthorized individuals, even if those individuals did not actually gain possession of the data.

Considerations for Congress

While there is a relative absence of federal law on how Internet companies should prevent and respond to data breaches, a number of bills have been introduced on this issue. Any data security legislation raises several legal considerations for Congress. First, Congress might evaluate the scope of the covered subject matter and entities. In terms of subject matter, legislation could impose preventative data breach measures

(e.g., H.R. 6864), responsive data breach measures (e.g., H.R. 3816), or both (e.g., H.R. 4081). In terms of entities, legislation could cover all companies subject to the FTC or another agency's jurisdiction (e.g., H.R. 5388), or it could take a sector-specific approach and only cover Internet companies (e.g., S. 2728). Second, Congress might consider the appropriate enforcement agency and the nature of its authority. While many proposed bills would designate the FTC as the primary enforcer, legislation has differed on the way in which the FTC would enforce violations. For instance, some bills would rely on the existing framework under the FTC Act by directing the FTC to treat violations of the bill as violations of a UDAP regulation. Other bills would give the FTC and Department of Justice shared enforcement authority or would create an entirely new "Office of Cybersecurity" to enforce violations. Third, to address concerns about the lack of uniformity among state data breach legislation, Congress might consider the extent to which any new federal legislation would preempt state laws. For example, some legislation would expressly preempt any similar state laws, while others are silent on the issue or would only preempt "less stringent" state laws. These and other legal issues could be of importance as Congress considers legislation in light of recent concerns over how Internet companies are protecting and responding to threats to cybersecurity.