Changing Views on Privacy

By Samantha Green

In the digital age, sharing personal information online is a way of life. It's how we connect with others, gain access to valuable services and information, pay bills, book trips, support causes, buy clothes, view health records and schedule appointments. Practically anything we need to do can be done in a few clicks, or simply by asking Alexa. And throughout each of these common exchanges, companies collect our personal and financial information.

Although these practices have been in place for years, there is a widespread shift underway in how United States citizens view the protection of their personal data. A boilerplate consent form isn't enough anymore. People want to understand the full scope of how sensitive information is accessed, shared with third parties, used for targeted advertising, and what is being done to safeguard their privacy in the process.

BREACH IN TRUST

Massive data breach scandals are a key cause behind this rising concern around privacy. The events that transpired between Facebook and Cambridge Analytica — in which the political analytics firm harvested personal information of up to 87 million users without their consent — exposed just how much we don't know about how our personal information is used and exploited. This went far beyond a data breach. It was a breach in trust, one that was detrimental to how our global democracy works.

Another recent breach making headlines involved the brand Under Armour. This spring, it admitted that close to 150 million MyFitnessPal accounts were hacked when an unauthorized party acquired data from the app that included usernames, passwords and email addresses.

These breaches, among many others, are creating a growing sense of angst among Americans who use social media. Pew Research Center studies have shown that people are anxious about the security of their personal information. A 2014 survey found that 91 percent of Americans "agree" or "strongly agree" that people have lost control over how their personal information is collected and used by various entities. A 2017 survey found that just 9 percent of social media users were "very confident" that social media companies would protect their data. About half of users were "not at all" or "not too" confident that their data were in safe hands. Six in 10 Americans have said they would like to do more to protect their privacy. Additionally, two thirds have said current laws are not good enough in protecting people's privacy, and 64 percent support more regulation of advertisers.

As companies remain under intense scrutiny and user trust wanes, the shift in public opinion is putting pressure on organizations — especially tech giants — to be much more transparent about their privacy policies, and for the government to create new privacy protections. In the United States, there is no single, overarching federal law regulating the collection and use of personal data. There are broad consumer protection laws that prohibit unfair or deceptive practices involving the disclosure of — and security procedures for protecting — personal information, including the Health Insurance Portability and Accountability Act

(HIPAA), and The Federal Trade Commission (FTC) Act. But we don't have sweeping legislation like the EU's General Data Protection Regulation (GDPR).

LEGISLATION INTRODUCED

In April, Senators Amy Klobuchar and John Kennedy released the Social Media Privacy Protection and Consumer Rights Act of 2018, a comprehensive bill that would impose strong regulations on companies that collect data on users. Among the provisions, it would require websites to provide their users with a free copy of the data that is being collected on them, as well as information on other parties who have gained access to it. It is unclear where the Act will go from here, or when or even whether it will get a vote, but it's important to note that there is bi-partisan support for legislation that mirrors the GDPR.

The GDPR went into effect across the EU in May. It restricts how companies collect, store and use personal data. The laws require companies to clearly explain how they plan to use and secure people's personal information, as well as how other entities will access that data. If they don't comply, they face severe penalties, ranging from up to 10 million, or 2 percent of the worldwide annual revenue of the prior financial year (whichever is higher), or for the most significant violations up to 20 million, or 4 percent of the worldwide annual revenue of the prior financial year (whichever is higher).

Supervisory authorities also have more power to monitor and enforce the new law, conduct investigations on compliance, order companies to provide information, and obtain access from companies to all personal data and information that the authorities think they need to perform their tasks. Individuals also have enhanced rights under the law. The political slogan for the GDPR is the "Right to be Forgotten" — a right for individuals to have personal data erased.

As United States consumers demand more rights over their personal data and stricter oversight of tech companies, states and localities are taking matters into their own hands and drafting tougher data protection laws. All 50 United States, as well as the District of Columbia, Guam, Puerto Rico and the United States Virgin Islands, have created breach notification laws that require businesses to notify consumers if their personal information is compromised. Several states take it a step further by requiring companies to be more transparent in how they process consumer data.

California recently passed what is arguably the country's strongest digital privacy law, and many states could be following suit. Echoing key elements of the GDPR, it grants consumers the right to know what information companies are collecting, why it's being collected and how it's being shared online. The legislation, which goes into effect in 2020, gives people the right to tell companies to delete their data, as well as not to share or sell their personal information. It includes a provision that children under 16 must opt in to allow companies to collect their data. Additionally, the law also makes it easier for consumers to sue companies following a data breach.

> MASSIVE DATA BREACH SCANDALS ARE A KEY CAUSE BEHIND THIS RISING CONCERN AROUND PRIVACY.

Colorado just passed the Protections for Consumer Data Privacy Act into law, which significantly tightens reporting requirements for organizations hit by a data breach and requires much firmer measures be taken to protect consumers' personal information. Organizations must maintain policies for disposing of documents containing consumer data and must notify Colorado residents of any potential personal information exposure no later than 30 days after discovering a data breach — the shortest of any state.

In May, Vermont passed the country's first law regulating data brokers — organizations that buy and sell personal information. It requires them to register with the state government, better inform consumers on the data that's being collected, provide instructions for opting out of such collection, ensure that their security practices are current and notify authorities when a breach occurs. The GDPR has also inspired recent data protection ordinances in Chicago, where the Personal Data Collection and Protection Ordinance was introduced in June.

Amidst countless data breaches and identity thefts, it is clear that the American public demands more from both tech companies and lawmakers to protect their personal information and invaluable right to privacy. With states taking the lead, this cultural shift in how we feel about privacy could spur big changes across the country, and even lead to comprehensive privacy legislation. The bottom line: People want more control, more accountability from companies, more oversight and more understanding of how their personal information is being used.

SAMANTHA GREEN is the Manager of Thought Leadership for Epiq. She serves as a subject matter expert on all aspects of electronic discovery, data privacy and cybersecurity, drawing on her more than 15 years of litigation and consulting experience. As a litigator, she has taken a number of cases from pre-discovery through trial and has handled a broad spectrum of cases, from government investigations (including FCPA and antitrust matters) to HSR second requests and commercial litigation matters.
sagreen@epiqglobal.com