ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Is US Privacy Law Standing Still?

Technology, Privacy, and eCommerce

Cheat Sheet

Snowden. The Snowden revelations highlighted fundamental problems with US data protection that still need to be addressed.

On hold. The evolution of US rights-based privacy laws has halted and is unlikely to move forward absent a 9/11-level catastrophe.

Troubled road. Progress in US data privacy law would require overcoming business resistance, establishing consensus around privacy, educating consumers on rights, and addressing the challenges of federalism.

Privacy-forward framework. Build a privacy framework in line with highest compliance requirements, regardless of your jurisdiction.

When the European Union's General Data Protection Regulation (GDPR) came into force in May 2018, followed only two months later by the surprising passage of the California Consumer Privacy

Act (CCPA) into law, the prospect for consumer privacy rights in the United States looked bright.

One can be forgiven, at the time, for making comparisons to the fall of the Berlin wall and the subsequent collapse of Eastern-bloc governments and the Soviet Union – it seemed that the dominos of weak privacy protections for individuals would shortly fall in the same fashion.

However, it was not to be. One recent post-mortem on privacy law at the US state level opined that the potential for meaningful – and meaningfully enforced – privacy legislation emerging out of the states is limited. Another (and perhaps more cynical) assessment is that the advancement of GDPR-style, "rights-based" privacy laws at the US state and federal levels has largely halted, and that absent some 9/11-style catastrophe, US consumers have seen the last of such laws for the near term. The reasons for this are varied and require a look back into (relatively) recent privacy law history.

The two eras of privacy law

Perhaps the most succinct way of looking at the evolution of privacy rights is to divide privacy history into two eras – Before Edward Snowden (BES) and After Edward Snowden (AES). BES can be characterized by the passage into law of a landmark privacy law at the US federal level, the Privacy Act of 1974, and the slow but steady evolution of federal privacy law thereafter.

Examples include The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm–Leach–Bliley Act (GLBA) (1999). The publication of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980 significantly impacted the drafting and enactment of Directive 95/46/EC (Data Protection Directive), the first EU-wide data protection law.

After dramatic growth of the public internet in 1995, the need for additional protection of personal data in electronic form became especially acute. It precipitated the passage into EU law Directive 2002/58/EC (ePrivacy Directive), followed by an update in 2009, Directive 2009/136/EC. Further development of data protection laws around the world during this period was fairly slow. However, this would soon change.

The Snowden revelations

In June of 2013, National Security Agency (NSA) contractor Edward Snowden disclosed surveillance operations conducted by the agency, now his former employer. The scope of the surveillance was extensive. Among the revelations was a program called PRISM, which involved the NSA's tapping into the communications of internet service providers such as Microsoft, Google, Yahoo, and Facebook, and harvesting personal data. Facebook was forwarding data about its users to the NSA "for reasons of espionage, national security, and other matters."

The controversy surrounding the revelations was fierce and widespread. Multinational companies with operations in the United States but headquartered elsewhere threatened to cut off business with US-based internet and technology companies. The publication of PowerPoint slides depicting how the NSA intercepted data en route to companies such as Google only served to visualize and underscore the contempt for privacy the agency seemed to have. However, this "upstream" interception and collection of electronic communications from undersea "trunk" lines coming into the United States appeared to be legal. Two legal mechanisms, Executive Order (EO) 12333 and the Foreign Intelligence Surveillance Act (FISA) § 702, were cited as the authority for such operations.

During this period, the European Union's replacement for the Data Protection Directive was being drafted. The Snowden revelations undoubtedly influenced the direction of that replacement, the General Data Protection Regulation (EU) 2016/679 (GDPR) — perhaps substantially. What is indisputable is that the revelations directly lead to two significant (if not landmark) legal decisions, those addressing privacy complaints by Maximilian Schrems.

The Schrems decisions

Shortly after the Snowden revelations, Maximilian Schrems, an Austrian attorney and privacy advocate, filed a complaint against Facebook Ireland with Ireland's data protection authority, the Data Protection Commissioner (Facebook's EU headquarters is in Ireland). The kernel of Schrems' complaint was that the NSA's electronic surveillance programs defeated any promises to provide "adequate" protection to EU personal data under the US-EU Safe Harbor data transfer program. This was because the NSA had generalized access to electronic communications from the European Union and did not offer any legal tribunal for EU data subjects to challenge such interceptions. Facebook's transfer of EU personal data from its operations in Ireland to its operations in the United States therefore did not offer protection that was essentially equivalent to that of EU law and should be stopped. The matter worked its way up to the Court of Justice of the European Union (CJEU), which ruled on Oct. 6, 2015, that the program was invalid.

That decision, now known as Schrems I, should have ended the matter. However, the Commissioner informed Schrems that Facebook relied on another data transfer mechanism, Standard Contract Clauses (SCCs), not Safe Harbor, to transfer the data. Schrems then started the entire process over with an amended complaint.

Surprises with Schrems II

Soon after the invalidation of the Safe Harbor program, negotiators at the US Department of Commerce and the EC accelerated discussions of a replacement for Safe Harbor. Within 10 months the EC deemed the EU-US Privacy Shield Framework adequate, and US-based enterprises began self-certifying under the new program's mandates.

Meanwhile, Schrems' amended complaint wound its way through Ireland's court system, and the matter wound up back at the CJEU. On July 16, 2020, the CJEU handed down what would become known as Schrems II. The decision both invalidated Privacy Shield and called into question data transfers using SCCs. It was surprising that Schrems' focus was on SCCs, not Privacy Shield, which had yet to be implemented at the time of his amended complaint, but the Court chose to address it anyway. The Court used the same reasoning as before: US authorities' unfettered interception of incoming electronic communications was both permissible under US law and did not offer legal recourse to EU data subjects.

Adding to the problem for exporters was the fact that the Court issued a new mandate for transfers of personal data using SCCs to any country not deemed "adequate." Transferers (called "exporters") now had to conduct a *de novo* review of their cross-border data protection program and determine whether existing controls were sufficient. If not, the exporter would have to implement "additional safeguards" or "supplementary measures" to make the export legitimate. Worse yet, there was no grace period to make changes — exporters would have to resolve any legitimacy questions about data transfers immediately.

The Court did not offer any examples of what controls would satisfy this new mandate, which only exacerbated the problem for US-based data importers. On Nov.10, 2020, the European Data Protection Board (EDPB), an EU-based data protection authority and privacy think tank, published a “recommendations” document that cited some scenarios that might meet the new standard. However, the scenarios were not particularly helpful; in some instances, they bordered on the absurd.

On May 14, 2021, the Irish High Court denied Facebook’s challenge to a September 2020 order by the Irish Data Protection Commissioner to suspend data transfers from the European Union to the United States, effectively ending such transfers. The Snowden revelations highlighted fundamental problems with data protection in the United States; problems that have not been addressed at the federal level, and imperfectly at the state level.

Data protection laws stalling at the US state level

Starting with the 2016 legislative sessions, US state legislatures have been relatively active in introducing and advancing data protection legislation. However, the vast majority of the bills making their way into law were (and are) not particularly ambitious in their scope. Nearly all are centered around updating existing breach notification statutes, mandating the employment of “reasonable” security controls, or expanding the definition of personal data.

New York Department of Financial Services’ cybersecurity regulations, 23 NYCRR Part 500, which became enforceable on March 1, 2017, set a relatively high bar in mandating controls, but was limited to banks and similar institutions. Since enforcement of GDPR began in May 2018, a total of three rights-based, GDPR-like consumer data protection laws have been passed into law: the California Consumer Privacy Act of 2018 (CCPA), the Virginia Consumer Data Protection Act (VCDPA), and the Colorado Privacy Act (CPA). In addition, a substantial amendment to the CCPA, the California Privacy Rights Act of 2020 (CPRA), was approved by California voters in November of 2020.

These statutes share a core set of consumer rights vis-à-vis businesses that possess consumer personal data:

- Access to consumer personal data, and to amend or delete it, and
- Data “portability,” i.e., to receive data in a reasonably usable form that potentially could be re-used with other online service providers.

They also share a core set of business mandates:

- Implement reasonable security controls based on the risk to the data;
- Obtain consumer permission for sale or transfer of personal data to third parties; and
- Demonstrate transparency of privacy practices, typically with a web-based privacy statement.

There is more to these laws than just the foregoing, but these core rights and mandates represent what has come to be expected as “table stakes” in the privacy profession. In light of the many state legislatures that have introduced rights-based privacy legislation since 2018 (some multiple times), it is remarkable that so few have made their way into law. It raises an important question: Why? The answer reflects the federal nature of the US legal system, the political power of corporations (especially technology corporations), and cultural issues.

A troubled road to the GDPR standard in the United States

Why has the prospect for GDPR-like data protection laws in the United States, at both the federal and state levels, dimmed over the past few years? Four reasons represent the majority of the answer:

1. Resistance from businesses

Businesses have consistently and forcefully fought the passage of rights-based data protection laws, owing to the perceived regulatory burden they face. While a private right of action for aggrieved consumers is often cited as a sticking point (the proposed Washington Privacy Act being a recurring example), **any** additional regulatory burden seems to be a non-starter. Noteworthy here is that state government agencies and nonprofit organizations are not subject to laws like the CCPA, in stark contrast to the GDPR.

2. Privacy form over substance

Even when data protection laws are followed by businesses (witness the many Do Not Sell My Personal Information links on websites), the problem remains: How do consumers truly understand what they are consenting to when they give their consent for sale or sharing of their personal data? Something as innocuous as geolocation data, for example, can, when aggregated, reveal intimate details about someone's life. Understanding the downstream effect of the sharing and use of personal data is difficult for professionals; it is all but impossible for consumers.

3. Consensus about the nature of privacy

The concept of privacy and application of data protection law is deeply cultural. Even within a culture, obtaining consensus about what is considered "personal" data can be difficult. For example, under the GDPR, personal data includes business email addresses as well as IP and MAC addresses. Prior to the GDPR's implementation, IT professionals in the United States would have looked at this notion with incredulity, yet it was now a reality. Conversely, uses of personal data considered acceptable in the United States may draw responses of "How is this legal?" when applied in Europe.

4. Federalism and federal law

Federalism becomes a challenge when members of Congress introduce legislation that preempts state law. While the idea of one national data protection law that offers a single standard is appealing (and likely necessary for an "adequacy" status to be granted by the European Commission), the risk of a standard that provides a relatively low "ceiling" is anathema to privacy advocates. Given the prospect that preemption would vitiate or even nullify the CCPA and CPRA, getting the California Congressional delegation on board for such a law is unlikely.

Yet another challenge is federal law itself. As discussed earlier, the Snowden revelations highlighted two legal mechanisms, E.O. 12333 and FISA § 702, as particularly troublesome. With respect to the former, not even American citizens have the opportunity for redress in court; with the latter, abuses of § 702 have both been well documented and litigated.

What can change the course of data protection law in the United States?

The prospects for further development of laws protecting personal data are unencouraging at the state level and bleak at the federal level. This is owing to a lack of a sense of urgency among legislators for such laws and the inability of privacy professionals and advocates to obtain consensus about precisely what data protection standards are a “must have” versus a “nice to have.”

The intrusion into the US Office of Personnel Management and the theft of some 22 million records of government employees from 2014 to 2015 should have been a catalyst for promulgating robust data protection at the federal level. So should the 2017 intrusion into Equifax’s databases and theft of highly personal data of nearly 150 million Americans. So should reports of abuse of the personal data of some 87 million Facebook users by the data analytics company Cambridge Analytica from 2015-2018.

However, such laws never appeared. At this point, the only prospect for significant advancement of data protection at the federal level is as the result of some 9/11-style privacy catastrophe. What that catastrophe may look like is unclear.

The May 2021 ransomware attack on energy company Columbia Pipeline that caused gasoline shortages for several days accelerated the publication of a presidential executive order addressing improvements in cybersecurity. Perhaps the most likely scenario, then, is a catastrophic attack on America’s energy, healthcare, or financial sectors -- an attack that results in the promulgation of significant new cybersecurity laws. Such laws would enable privacy considerations to be “tacked on” during the period of legislative debate. While the thought of depending on some national misfortune to advance privacy could be considered depressing, at this point, it represents perhaps the best chance US persons have.

Key Data Privacy and Compliance Trends for 2022

This is one of the most fascinating and interesting areas of the law, and it touches each of us personally and professionally. The authors identify five trends to know about for next year.

How to build a privacy forward data protection practice

Where do we go from here? It is time to prepare for potential federal regulation at best or a patchwork of state data protection laws at worst. In the past 12 months, we’ve seen the introduction of more than 30 comprehensive state privacy laws. While only California, Colorado, and Virginia successfully passed comprehensive privacy legislation, there is a clear message that businesses need to take a privacy-forward approach to data protection in the United States

A privacy-forward data protection practice is about embracing the privacy law requirements that already exist, whether you are covered by the GDPR or CCPA. It’s about building a privacy framework with the highest standards supporting compliance regardless of the jurisdiction. It begins with knowing how and what data a company collects from its consumers, how it uses, stores, and ultimately disposes of those data when the purpose for using those data has been met. It’s also about transparency and the security of the data.

From our perspective, one of the biggest challenges that companies face is knowing what data they possess, where it’s located, and understanding and controlling who has access to it. This can be

especially challenging when you consider the sizable amount of unstructured data that most companies have.

We describe unstructured data as datasets that are not stored in a structured database format. This includes texts, MS Word documents, photos, audio files, MS PowerPoints, social media, etc. Knowing the location of your data is a critical component of a privacy-forward strategy, especially with GDPR and CCPA where individuals or consumers have the right to ask what information the company possesses about them. These data subject or personal information requests allow an individual to ask for access, a copy of the data, deletion, and in some cases, correction of the data. They also allow an individual to stop a company from selling their information.

With the implementation of the CPRA (CPRA amends the CCPA and becomes operational in January 2023, with a one-year lookback period), consumers can also stop a company from sharing their data. Part of any comprehensive privacy-forward data protection practice needs to include a data mapping exercise so that you can answer the questions about what data you have about a consumer. This mapping exercise also needs to include downstream data uses.

Finally, the importance of security and privacy comes from the top down, so your management team needs to discuss security and privacy as a part of every company strategy conversation.

Prepare now

The growing volume of cyberattacks that have breached governments, corporations, and citizens, along with big tech controversies, has led to the eroding state of data privacy. Naturally, we see the emergence of new legislation that regulates how organizations treat consumer data.

The state of US data protection laws is uncertain and undoubtedly complex, but by adopting a privacy-forward mindset, you will be better prepared to ensure regulatory compliance, preventing costly data breaches from happening, and adapting to new laws and regulations on the horizon.

Scott Giordano

VP, Corporate Privacy & General Counsel

Spirion

Scott Giordano is vice president, corporate privacy and general counsel at Spirion.

Jennifer K. Mailander

Senior Director & Deputy General Counsel

Fannie Mae

Jennifer K. Mailander is senior director and deputy general counsel for Fannie Mae. She is on Spirion's board of directors and is also a founding member and former chair of ACC's Women in the House Network.