On July 16, 2020, the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield and ruled that U.S. data protection laws do not provide EU data subjects adequate protection. In regard to the General Data Protection Regulation (GDPR) and European Union’s Charter of Fundamental Rights, the Court took a far-reaching decision, also known as Schrems II (Data Protection Commissioner v. Facebook Ireland Ltd.)[1]. This decision symbolizes the extensive reach of the GDPR, and the standards set by this European legislation for the world of data privacy and more specifically for the United States. With a new administration in charge, is it time for a U.S. Federal data protection regulation to be voted into law?

When the GDPR became enforceable on May 25, 2018, lawmakers aimed at protecting personal data considering data privacy as a fundamental right[2]. Facing an ever-increasing number of data breaches[3] and a lack of enforcement from member states[4], the EU was in need of a uniformization of its data protection laws in order to protect its citizens. The GDPR updated regulations previously unfit for the evolution of the global digital economy and its reliance on data collection. Among many other provisions, the GDPR extended the definition of personal data and created a framework for citizens to exercise their rights to access and delete data. This innovative regulation also granted data subjects a right to correct incorrect data and created a requirement for explicit consent when consumers give their data. It is worth noticing that the GDPR also created a uniform system of data breach notification requiring organizations to adopt faster turnarounds and stricter risk assessment measures under the threat of heftier penalties.
In parallel, the U.S. has followed a very different path in regard to data protection. If one wants to understand the reasons why a federal data protection regulation has become necessary in the U.S., it is essential to identify the two major trends followed by lawmakers in this field. On the one hand, the U.S. lacks a comprehensive digital privacy law that would cover more than just certain specific industries. On the other hand, a federal data protection regulation would require a uniformization of the heterogeneous legislations already existing among the 50 States, for example, data breach notification.

When it comes to data privacy law, it would be exaggerated to assert that the U.S. does not have a legal framework to protect its citizens. Nevertheless, this framework is based on a vertical architecture with industry-specific regulations that do not entirely protect the digital activities of data subjects. For example, the U.S. Privacy Act of 1974 implemented restrictions on personal data held by U.S. government agencies. This piece of legislation played a pioneering role for it contained provisions regarding the right of U.S. citizens to access any data held by government agencies, the right to correct this data when incorrect, and the obligation for U.S. government agencies to respect data minimization principles when collecting data[5].

Another example of the sectoral approach[6] adopted in the U.S. concerning data privacy laws is the Health Insurance Portability and Accountability Act of 1996[7]. Among other health insurance provisions, the legislation included data privacy sections which aimed at protecting healthcare data and protected health information (PHI). In particular, HIPAA's minimum necessary standard[8] gave a good example of the privacy by design principle which is now a standard provision in data privacy laws. Through a complex set of rules, HIPAA also created a system limiting the use of PHI for marketing or commercial purposes by requiring explicit authorization of the patient.

Aside from these industry-focused legislations, the U.S. has been missing a single and comprehensive legal tool to regulate data privacy, especially in regard to the activities of technology and social media companies. In the recent years, the U.S. government has used the Federal Trade Commission (FTC) as an alternative to protect consumer privacy. Under the FTC Act of 1914, the U.S. government has issued huge
fines to companies like Facebook[9] or Uber[10] which engaged in prohibited “unfair or deceptive acts or practices”[11]. More precisely, the FTC has held Facebook accountable for misleading representations of its ability to control the privacy of users’ personal information. In fact, the FTC tools of regulation are indirect and imperfect privacy enforcement mechanisms. Instead, the U.S. would largely benefit from a federal data privacy law forcing companies to have privacy policies.

At the State level, the fragmented data privacy laws have been undermining legal certainty and creating inconsistencies in the ever-growing digital industry. Having to comply with dozens of regulations, companies are facing higher costs in order to abide by the rules. As a result, different rights are guaranteed by different legislations in various States. While the Californian Consumer Privacy Act (CCPA) provides a right to access[12] and a right to delete personal data[13], it does not offer the possibility to correct incorrect data. On the contrary, if the New York Privacy Act (NYPA)[14] was to be voted into law in the next few months, it would grant the right to correct data to data subjects, granting similar rights to the EU GDPR. The NYPA would apply to any company without a revenue threshold, in opposition with the CCPA that applies only to for-profit businesses with annual gross revenues of $25+ million.

A similar diversity of data breach notification regulations among States is causing difficulties for companies to make sense of the mechanisms of how, when, and who to report a breach to. To illustrate this patchwork of regulations, it is worth focusing on the required notification that must follow a security breach without unreasonable delay: “18 states include a specific deadline for notifying affected individuals; 2 require a 30-day notice, 2 states require a 60-day notice, 1 has a 90-day limit; 1 has a 15-day notice for medical information; 1 requires notice 7 business days after law enforcement review; and the remaining 11 states require a 45-day notice.”[15] Adding to the diversity of notification deadlines, some States have no guidelines regarding the content of data breach notifications. Companies are also facing various types of penalties depending on the States’ regulation they violate, including civil or criminal penalties, or both. Therefore, it seems clear that the diversity of privacy laws at the State level has created a complex set of rules that could benefit from a federal regulation.
In light of the current challenges in the U.S., a growing bipartisan trend has been pushing for a federal data protection regulation. The Application Privacy, Protection and Security Act of 2020 (APPS Act) was among the few bipartisan comprehensive privacy laws presented to the last Congress. However, bills kept coming from both sides of the aisle with unequal levels of consumer protection[16]. Under the new Biden administration, Republicans and Democrats are likely to be opposed on how strictly the federal law should preempt on States rights to pass their own privacy laws. But both parties will be influenced by the international momentum data privacy has accumulated in the recent years. It has become a more pressing issue to end the sectoral approach to privacy in order to safeguard the rights of Americans in light of the Internet of things and the boom of data collection. The need for a comprehensive federal statute addressing innovative business models has never been greater.


Privacy Act, 5 U.S.C. § 552a (1974): “(e) Agency requirements. Each agency that maintains a system of records shall—(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency [...]”


Health Insurance Portability and Accountability Act of 1996 (HIPAA).


California Consumer Privacy Act of 2018 (CCPA) § 1798.100(d).

California Consumer Privacy Act of 2018 (CCPA) § 1798.105(a).

