Building a better working world

Public policy spotlight: the evolving consumer privacy landscape

Considerations for businesses and other stakeholders managing through the uncertainty

May 2019

Introduction

The amount and types of data held, shared and used by businesses and organizations have exploded in recent years, spurring policy debates and yielding new and often overlapping regulations aimed at protecting consumer data and privacy. The European Union (EU) General Data Protection Regulation (GDPR), in force since May 2018, and the forthcoming January 2020 implementation of the California Consumer Privacy Act (CCPA) are creating uncertainty and challenges for companies as they navigate the growing jurisdictional fragmentation.

Complicating matters further, several other US states are considering legislation to establish their own consumer privacy regimes. The potential for a growing patchwork of laws within the US and around the world warrants consideration of how such developments impact business models and practices. It also raises questions of how innovation will be impacted as data continues to increase in importance and value to businesses.

In light of these concerns, pressure is building for Congress to establish a national standard that would preempt state laws. The path for federal legislation, however, is fraught with potential roadblocks amplified by Washington's increasingly partisan environment.

This publication examines the evolving consumer privacy landscape in the United States; highlights major international developments, especially with respect to the GDPR; and outlines key business considerations to help companies navigate the uncertainty, plan for changes in the regulatory environment and manage new rules and policies.

Executive highlights

- The US Congress is considering issues that are likely to inform a federal consumer privacy standard. The Senate is working to draft bipartisan legislation, but timing is unclear. On the House side, the path forward is less certain, complicated by Speaker Nancy Pelosi's (D-CA) recent statements that she would not support a bill that preempts the new California data privacy law.[1]
- About 30 states are in the process of considering consumer data privacy legislation, biometric data rules or updates to data breach statutes. Many of the state legislative proposals are less comprehensive than the CCPA and focus on one specific area or industry, such as data brokers. However, comprehensive privacy reforms are still pending in nine states.
- The California legislature is also considering amendments to the CCPA, but final details are not expected until later this year. Under existing law, the CCPA becomes effective 1 January 2020, but the deadline for the California State Attorney General to commence enforcement was extended to 1 July 2020, or six months after the final regulations are published, whichever comes first.[2]
- More than three dozen countries or jurisdictions have recently adopted policies and rules aimed at protecting consumer data privacy, but the EU's GDPR is most impactful because of the extent of changes required for most companies and its potential for significant fines.
- Enforcement of the GDPR has begun in earnest and can provide insights into which obligations European data protection authorities are most focused, as well as how they respond to violations (e.g., with fines, instructive guidance or requests to cease certain practices).

1. Rep. Nancy Pelosi (D-CA), Speaker of the US House of Representatives, interviewed by Kara Swisher, Recode Decode, 12 April 2019, https://www.vox.com/2019/4/12/18307957/nancy-pelosi-donald-trump-twitter-tweet-cheap-freak-presidency-kara-swisher-decode-podcast-interview, accessed May 2019.
2. CCPA § 13(c).

In-depth

This publication explores recent consumer privacy developments at various level of government:

1. **Outlook on federal efforts**
   - Congressional efforts
   - Trump administration efforts
2. **US state activities**
3. **International developments: the GDPR remains most impactful**

1. Outlook on federal efforts

Congressional efforts

Congress is taking up the challenge of trying to establish a single national standard for consumer privacy. As part of the process, some members are reviewing the GDPR and CCPA for potential leading practices and lessons learned. While there is a chance that a comprehensive privacy bill could move forward and be signed into law this year, legislating will be difficult because:

- Multiple congressional committees have legislative jurisdiction over privacy.
- States with stricter rules (e.g., California) often resist federal preemption of their rules.
- Policymakers in Washington have limited expertise and understanding about the operational and technical implications of related policy decisions.
- The long-standing populist nature of the issue has divided the Republican and Democratic caucuses.
- The increasingly partisan environment also creates additional hurdles in the lead-up to an election year.

Several members of Congress have introduced data privacy bills, but so far these have been viewed as "messaging" positions and are not expected to advance. Some concepts embodied in these bills could be included in a final agreement as details are negotiated; however, it is the chairmen of the committees with primary jurisdiction over consumer privacy — i.e., the Senate Commerce and House Energy and Commerce Committees — who will drive the process. As of this publication's issuance, neither committee has released a bill or framework for reform, but both have begun holding fact-finding hearings to consider issues that would need to be resolved in any potential legislation. Other committees in both the House and Senate are also seeking to engage on the issue and find a role for their committee in the legislative process, further complicating the matter.

Questions for boards and business leaders to consider

The evolving consumer privacy landscape presents new challenges for boards and business leaders. Companies need to consider how they will respond to and manage potentially conflicting directives. Below are some questions companies can consider as they prepare for a range of potential new requirements in this area:

- How do new or pending consumer privacy regulations and frameworks impact the organization? How should policies and practices be modified to foster compliance and interoperability with various regimes?
- How will new or pending privacy regulations and frameworks impact the organization's strategy, competitive position, and business models and practices?
- Does the organization have appropriate resources dedicated to implementing required changes and sustainably managing new business processes?
- How is the organization building workflows and processes that support the intake, management and fulfillment of individual data rights?
- How is the organization using personal data to support innovation, including artificial intelligence, machine learning and automated decision-making? How would these use cases be received by consumers, employees, the media or regulators?
- Is there a clear understanding by senior management of the business purpose for the data collected and retained?
- Are appropriate considerations being given to evolving data remediation requirements? This could include deletion, anonymization and pseudonymization (i.e., the process to de-identify personally identifiable information).
- Has the organization considered how new or pending developments could impact the following areas?
  - Employment, supplier, customer and other third-party contractual provisions
  - IT systems dealing with data storage, transfer and security
  - Compliance programs and procedures, including ongoing monitoring
  - Preparedness plans for a data breach, notification requirements, and related regulatory and reputational issues
- Does the organization have capabilities to identify and respond to the policy developments unfolding at the state and federal levels in the US and around the globe?
- Does the organization understand the need to incorporate and infuse "privacy by design" in the development of new products and processes?

As Congress considers privacy legislation, the following concepts are expected to be a part of the debate:[3]

- **National preemption** – whether a single national standard should override state laws on consumer privacy. The business community has made this a priority, and it has strong support from congressional Republicans and some Democrats. Given the importance of preemption to business stakeholders, certain Democrats may be well-positioned to leverage preemption to seek concessions during the legislative process. Such policy priorities could include more expansive Federal Trade Commission (FTC) rulemaking authority, strong enforcement and liability provisions and perhaps even new private rights of action (see more details in "Private rights of action" below).
- **Application to all industries** – whether all entities, regardless of industry sector, that collect information about consumers should be subject to the same requirements and primary enforcement by a single federal regulator (i.e., the FTC). This is complicated by existing laws governing certain sectors, including financial services and health care. How policymakers will navigate the existing set of complicated laws and regulations in highly regulated sectors is still not clear.
- **Private rights of action** – whether individual Americans should be allowed to sue companies over alleged privacy violations. This could be a critical sticking point in the debate for many Democrats who view the exclusion of such rights as curtailing Americans' access to the courts. The business community is concerned about exposure to frivolous lawsuits.
- **Transparency** – the nature, extent and kinds of information that should be shared with consumers about business practices with respect to the collection, use and sharing of personal information.
- **Consumer rights** – how to operationalize the protection of consumer privacy rights in a complicated ecosystem and within the supply chain. Companies will likely need a mechanism that provides consumers with: (1) the right to reasonably access the information a company has about them, (2) the right to delete data within certain limits of the law (e.g., while still allowing businesses to comply with anti-fraud requirements), (3) the right to correct erroneous information and (4) the right to port their personal information (i.e., take the data from one vendor and provide it to another).
- **Consumer choice or consent** – whether consumers should be able to opt-in or opt-out of the collection, use and sharing of sensitive personal data. Stakeholders are divided. The opt-in requirement places a greater burden on the entity collecting the data to obtain consumer consent, and so the nature of data falling into either category could easily become a matter of contention. Further, this provision could have significantly negative ramifications for the online advertising industry.
- **Enforcement** – what entities should be charged with enforcement of consumer privacy rules. There is consensus among Democrats and Republicans about expanding the role of the FTC, including granting it some rulemaking authority (described in the next point below). Most Democrats, some Republicans and even some leading industry groups support a dual role through which both the FTC and the state attorneys general would enforce the federal law. However, among stakeholders who support dual enforcement, there is disagreement about the details and the extent of the enforcement authority.
- **Rulemaking authority** – historically, the GOP and some in the business community have advocated for rules to be prescribed by Congress, while Democrats pressed for the FTC to have more expansive rulemaking authority so that regulations could be adapted to address changes in technology and industry practices. There are signs that some Republicans and business community stakeholders are reconsidering their position on the issue. A turning point in the debate came last fall when all five FTC commissioners testified before Congress and advocated for the agency to have additional authority. The scope of any proposed FTC rulemaking authority will be the source of contentious debate.
- **Competition** – recent scandals involving social media platforms and large technology companies have led some policymakers in Congress and the Trump administration to raise anticompetitive concerns. Some members of Congress have asserted that privacy legislation should include an element of additional oversight for these companies.

Senate efforts

The Republicans control the Senate but still need to meet the 60-vote requirement to pass legislation. Given the current breakdown, at least eight Senate Democrats would need to support a bill for it to pass and be sent to the House for consideration. The Senate Commerce Committee is undertaking efforts to develop a bipartisan draft bill, but timing and the path forward are not clear. Other committees are also considering their role in consumer privacy reform, e.g., the Senate Banking Committee.

3. This is not an exhaustive list of all the possible issues that could be raised during the legislative process; however, it includes major issues policymakers in Washington are likely to consider in the coming months.

House efforts

Democrats control the House, and many members, including Speaker Pelosi, are likely to have significant concerns about a federal law that would preempt the CCPA or their own state's efforts (see further discussion in the US state activities section). Many moderate Democrats support preemption. As a result, there appears to be a divide within the party on the foundational issue of preemption. Some Democrats support the CCPA or GDPR as the floor for federal legislation, others oppose federal preemption and many members have not had enough time to fully consider the issue. There is also disagreement among Democratic leaders on the Energy and Commerce Committee, which has primary jurisdiction over consumer privacy in the House. This is likely to further slow the process. Some House Democrats have suggested that they may have to wait for a bipartisan bill to come from the Senate before the House is able to act.

Trump administration efforts

Heeding concerns from the business community and various privacy stakeholders, last fall, the Trump administration **announced** its support for a national **unified privacy standard** and called on Congress to establish it after a series of listening sessions driven by the White House's National Economic Council. The administration also announced that the National Institute of Standards and Technology (NIST) would undertake an effort to develop voluntary enterprise-level standards designed to help organizations manage privacy risk. NIST recently released its initial discussion draft of the framework for **feedback**.[4] Comments will not be made public, and the process is meant to inform NIST's ongoing stakeholder engagement efforts.

In a parallel and coordinated effort, the Commerce Department's National Telecommunications and Information Administration (NTIA) released a broad framework outlining the administration's approach to privacy and invited stakeholders to comment (see comments **here**). The NTIA framework was viewed as a signal to the global market about the direction the White House wanted Congress to pursue. Specifically, the NTIA framework states that:[5]

- "Organizations should be transparent about how they collect, use, share and store users' personal information.
- Users should be able to exercise control over the personal information they provide to organizations.
- The collection, use, storage and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks.
- Organizations should employ security safeguards to protect the data that they collect, store, use or share.
- Users should be able to reasonably access and correct personal data they have provided.
- Organizations should take steps to manage the risk of disclosure or harmful uses of personal data.
- Organizations should be accountable for the appropriate use of personal data that has been collected, maintained or used by its systems."

The NIST effort continues to move forward as the White House considers next steps to help push for legislation. Meanwhile, the FTC has been holding a series of **hearings** with technology industry representatives to explore consumer privacy and competition concerns. The FTC is also expected to continue with enforcement actions, having initiated or resolved 29 actions from 2017 through 2018.[6]

2. US state activities

About 30 states are in the process of considering consumer data privacy, biometric data rules or updates to data breach statutes. Most of the proposed legislation is not focused on creating consumer privacy legislation as comprehensive as the CCPA. Instead, many states are considering laws that focus on one specific area or industry, such as data brokers. For example, Vermont became the first state to regulate data brokers that collect and sell personal information about consumers with a law that went into effect 1 January 2019.[7]

There are several states, however, that are following in California's footsteps and considering comprehensive consumer privacy legislation. It is still early, and more details should come into focus later this summer or early in the fall as states move forward with their legislative processes.

4. "Department of Commerce Launches Collaborative Privacy Framework Effort," National Institute of Standards and Technology, 4 September 2018, www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort, accessed May 2019.
5. "NTIA Seeks Comment on New Approach to Consumer Data Privacy," National Telecommunications and Information Administration, 25 September 2018, www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy, accessed May 2019.
6. "FTC Enforcement Trends in Consumer Protection," Skadden, Arps, Slate, Meagher & Flom LLP, 11 February 2019, https://www.skadden.com/insights/publications/2019/02/ftc-enforcement-trends-in-consumer-protection, accessed May 2019.
7. "Vermont First State to Pass Data Broker Law," National Law Review, 4 June 2018, https://www.natlawreview.com/article/vermont-first-state-to-pass-data-broker-law, accessed May 2019.

In addition to efforts underway in California, the following states are still considering a form of comprehensive consumer privacy legislation. The status of each bill and likelihood of adoption are still to be determined.

- **Hawaii**: **SB 418** – modeled after the CCPA. Organizations' data controllers must respond to consumer requests for a copy of their information within 45 days. Penalties are not specified. No new private rights of action in the bill. While the bill will not move in the 2019 session, it could carry over into the 2020 session.
- **Maryland**: **SB 613** – would provide for similar consumer rights as the CCPA. Creates a broad right to delete personal information that an organization holds on the individual, and provides fewer exceptions for internal business use. No new private rights of action. While the bill will not move in the 2019 session, it could carry over into the 2020 session.
- **Massachusetts**: **SD 120** – modeled after the CCPA, with more specific provisions. Creates a new private right of action for consumers against businesses or organizations believed to have violated the Act. This bill could move forward in 2019.
- **Minnesota**: **HF 1030** – would require telecom and internet service providers to obtain advance written consent from consumers before collecting personal information. Prohibits refusal of service if the customer has not consented. Effective upon enactment. This bill could move forward in 2019.
- **New Jersey**: **AB 4640** – would require businesses to notify individuals of collection of personally identifiable information and establishes security standards. This bill could move forward in 2019.
- **New York**: **SB 224** – would give consumers notice if their personal info is shared or sold. Provides a consumer right to demand access to what information is held. This bill could move forward in 2019.
- **Oregon**: **SB 703** – would prohibit the sale of de-identified health information if signed authorization is not obtained first. Gives patients right to be paid for allowing sale and use of data. This bill could move forward in 2019.
- **Rhode Island**: **SB 234** – aligns to the CCPA, but without a state attorney general role in rulemaking or enforcement. Effective upon enactment. No new private right of action. This bill is eligible for consideration but unlikely to move forward before 2020.
- **Washington state**: **SB 5376** – modeled after the GDPR and would provide consumers with rights to request personal data, correct errors, delete data, port data and object to uses of their personal data (not including data already regulated by federal law, such as financial data or information protected by the Health Insurance Portability and Accountability Act). No new private rights of action. While the bill will not move in the 2019 session, it could carry over into the 2020 session.

California developments

The California legislature is considering amendments to the CCPA, a far-reaching consumer privacy law passed in June 2018 that included significant compliance obligations. The changes would clarify various aspects of the legislation, including the role of the California Attorney General in its **enforcement**.

As of May 2019, around 20 bills had been introduced to amend the CCPA.[8] Some bills would bring improvements sought by the business community, but others would move in the opposite direction, creating additional challenges for companies. For example, one proposal would significantly expand the private right of action currently included in the CCPA to cover all aspects of the law instead of just data breaches. Other amendments under consideration include clarifying amendments to assist businesses in compliance, such as the explicit exclusion of employees and contractors from the CCPA's definition of "consumer." Bills aimed at amending the CCPA are not likely to be adopted by the legislature until later this summer or early in the fall.

In addition to the legislative efforts underway, California Attorney General Xavier Becerra recently held a listening tour to better understand the challenges and concerns of businesses regarding implementation. The CCPA is set to go into effect on 1 January 2020, but the enforcement date was extended to 1 July 2020, or six months after the publication of implementing regulations, whichever comes first.

8. "A Deep Dive into Proposed Amendments to the CCPA," JDSUPRA, 1 April 2019, https://www.jdsupra.com/legalnews/a-deep-dive-into-proposed-amendments-to-79691/, accessed May 2019.

3. International developments: GDPR remains most consequential

To date, more than three dozen countries have adopted policies and rules aimed at protecting consumer data privacy, and many more are considering proposals. Of these, the EU's **GDPR** is the most impactful. In effect since May 2018, the GDPR includes requirements related to privacy impact assessments, privacy by design, enhanced consent requirements, new data subject rights, appointment of a data protection officer in certain circumstances, new obligations imposed on data processors, 72-hour breach notifications and new accountability requirements.

The GDPR applies to organizations that are established in the EU, where personal data is processed in the context of its EU establishment's activities. Separately, the GDPR also applies to non-EU established organizations that target or monitor EU data subjects. Most EU Member States have implemented their own privacy and data protection laws that align with the GDPR, with minor and permitted exemptions.

EU Member States' data protection authorities (DPAs) have taken different approaches to enforcement, and there has been little clarity on the methods used when determining fine amounts. Fines for a breach can be substantial under the regulation — up to 4% of total annual worldwide turnover or €20 million. However, only a relatively small number of reported breaches have been investigated and subject to fines. In these cases, there has been a large disparity in **fine amounts**, ranging from less than €5,000 to more than €50 million.

Over **59,000** breaches have been reported since the GDPR went into effect; however, only **91** GDPR-related fines have been issued. German regulators have assessed **64** of the fines.

Source: "**DLA Piper GDPR Data Breach Survey**," DLA Piper LLP (US), February 2019.

Managing GDPR compliance

- Organizations should continue to evaluate opportunities to support GDPR compliance with long-term, technology-enabled solutions that manage for automation and scale where it makes sense to do so.
- Organizations should develop and implement a strategy to periodically review their compliance with the GDPR, accounting for enforcement learnings, DPA guidance and evolving industry-leading practices.
- Businesses should continue to consider developments in overseas jurisdictions and the extent to which they have significant operations in those jurisdictions, and analyze the enforcement schema to inform risk-based decisions. For more information, contact an EY Privacy professional.

Contacts

Public policy

Les Brorsen
EY Americas Vice Chair, Public Policy
Ernst & Young LLP
+1 202 327 5968

Bridget Neill
EY Americas Deputy Vice Chair, Public Policy
Ernst & Young LLP
+1 202 327 6297

Emily Coyle
Director, Public Policy
Ernst & Young LLP
+1 202 327 6367

Data privacy

Scott Margolis
Managing Director,
Ernst & Young LLP
+1 303 885 7728

Phil Nemmers
Partner,
Ernst & Young LLP
+1 515 362 7012

Angela Saverice-Rohan
EY Americas Privacy Leader, Ernst & Young LLP
+1 213 977 3153

Data privacy for financial services

Cindy Doe
Principal, Digital Risk and Integrated Cyber Risk Offerings Leader,
Ernst & Young LLP
+1 617 375 4558

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. 06261-191US

1902-3052012

ED None

ey.com