WILMERHALE

Congress Begins Consideration of Comprehensive Federal Privacy Legislation

February 19, 2019

*T*he enactment in June 2018 of California's sweeping new privacy law, the California Consumer Privacy Act (CCPA), has both increased momentum for enactment of a general federal privacy law and spurred state legislatures to consider privacy bills of their own. A series of widely publicized incidents involving major technology companies' data handling practices and the coming into force of the European Union's General Data Protection Regulation (GDPR) have added urgency to both efforts. This report reviews proposals for federal privacy legislation. A companion report will review proposals at the state level.

Federal lawmakers have put forward at least eight proposals over the past year. Two of the eight have been introduced in the current session of Congress. The rest were unveiled in the prior congressional session, and new versions of many of those will likely appear again in the current Congress. We summarize the current status and key provisions of these bills below.

Congressional debate over these proposals and the principles that may animate additional bills will begin in earnest with hearings by the House Energy and Commerce Committee on February 26 and the Senate Commerce Committee on February 27.

Additional Sources of Proposals: NTIA, FTC, Trade Associations, Advocacy Groups

Congressional consideration of possible federal privacy legislation will likely draw on the results of processes for soliciting public input undertaken by two Executive Branch agencies in 2018.

In September 2018, the Commerce Department's National Telecommunications and Information Administration (NTIA) published a request for comments (RFC) addressing how the federal government could "advance consumer privacy while protecting prosperity and innovation." The NTIA sought input on how seven outcomes in privacy practices could best be achieved: (1) transparency; (2) control; (3) reasonable minimization; (4) security; (5) access and correction; (6) risk management; and (7) accountability. The NTIA also identified eight high-level goals for federal action: (1) harmonize the regulatory landscape; (2) legal clarity while maintaining the flexibility to innovate; (3) comprehensive application; (4) employ a risk- and outcome-based approach; (5) interoperability; (6) incentivize privacy research; (7) FTC enforcement; (8) scalability. The NTIA's request prompted a staggering 204 comments from companies, trade associations, consumer and privacy advocacy organizations, academics, local governments, and interested citizens. Many of these voices are likely to be heard in congressional hearings, and their recommendations are likely to be used by legislators in constructing bills.

In June 2018, the Federal Trade Commission (FTC) announced it would be undertaking a series of public hearings

and requests for public comments over the next 9-12 months addressing "whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy." Included among the 11 topics on which the FTC sought input were privacy, big data, and consumer protection. The FTC's requests drew hundreds of responses.

In addition to submitting responses to the NTIA and FTC, many trade associations and advocacy organizations have issued their own sets of principles for general federal privacy legislation.[1] These too are likely to provide grist for Congress's legislative mill, as may the voluntary privacy framework being developed by the Commerce Department's National Institute of Standards and Technology (NIST) through a process similar to the one used to develop its successful cybersecurity framework.[2] Finally, in response to a request from Rep. Frank Pallone (D-NJ), the chairman of the House Energy and Commerce Committee, the Government Accountability Office (GAO) recently issued a report recommending "that Congress consider developing comprehensive Internet privacy legislation to better protect consumers."

Some Key Issues

Key issues Congress will consider as it crafts privacy legislation include:

- **Covered businesses and other organizations.** Will the organizations subject to the law be limited to those with certain kinds of online presences or activities? Will there be thresholds in terms of economic size or of the number of individuals whose personal information is handled? Will non-commercial organizations be covered? Will there be exemptions for certain kinds of businesses or industries based on their coverage by other regulatory frameworks?
- **Definition of covered personal information.** The trend in amendments to state data breach laws has been to broaden the kinds of personal information triggering obligations concerning collection, sharing, and disclosure. The CCPA builds on that trend with a definition (akin to that used in the GDPR) under which not only specific data fields are covered but also any information that can be linked to particular individuals (or even households) is included. The federal proposals vary both in the kinds of data they enumerate as covered and in the extent to which they contain a catchall provision reaching broader and perhaps less readily identified types of data.
- **Rights of individuals.** The federal bills vary both in the kinds of data handling they would address—collection, storage, use for marketing, disclosing or selling to third parties—and the kinds of control they would give individuals over their personal data, e.g., correction, restrictions on handling, or deletion. They also vary in establishing opt-in or opt-out consent requirements for different uses of personal information.
- **FTC authority.** Most of the federal proposals entrust their enforcement to the FTC, under its mandate to prevent "unfair or deceptive acts or practices." State attorneys general are also generally permitted to sue on behalf of their citizens. But the bills are divided on what authority the FTC should be given to promulgate rules to shape the substance of the governing legal framework and on whether the FTC or state attorneys general should be empowered to seek civil penalties for violations. Currently, the FTC does not have the authority to seek civil penalties for privacy or data security violations under Section 5 of the FTC Act in the first instance.
- **Preemption.** One of the central impetuses for federal privacy legislation is to avoid a patchwork of inconsistent state laws. But the federal bills released so far vary considerably in whether they address preemption directly and, if so, the scope of the preemptive effect provided.
- **Private right of action.** Will affected individuals be permitted to sue over alleged violations and, if so, with what remedies? The CCPA permits private claims over data breaches but not privacy violations, and the federal proposals floated so far have refrained from authorizing private suits.

Proposed Federal Bills

1. American Data Dissemination (ADD) Act (S. 142)

Current status: Introduced by Sen. Rubio (R-FL) in January 2019, the bill has been referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

- Would not impose substantive requirements, but would create a process for establishing requirements for companies that "provide services using the Internet" akin to the requirements that apply to federal agencies under the Privacy Act.
- The FTC would have six months from the ADD Act's enactment to submit recommendations to Congress for privacy legislation that would be "substantially similar, to the extent practicable, to the requirements applicable to agencies under the Privacy Act of 1974."
- If Congress fails to enact a qualifying law within two years of the ADD Act's enactment, the FTC would be required to promulgate final regulations in the following three months based on the ADD Act's specifications.
- Those specifications include:
  - a prohibition on disclosure without prior consent except under specific exemptions, including when the use is compatible with the purpose of collection;
  - an obligation to keep records of disclosures;
  - access and correction rights;
  - an exemption for certain small, newly formed businesses;
  - exemptions for personal information governed by the Health Insurance Portability and Accountability Act (HIPAA) and its regulations or by the Family Educational Rights and Privacy Act of 1974 (FERPA);
  - FTC authority to resolve possible conflicts between the ADD Act, on the one hand, and the Children's Online Privacy Protection Act (COPPA) or Gramm-Leach Bliley Act (GLBA) and their implementing regulations, on the other; and
  - enforcement by the FTC.
- The ADD Act or regulations issued pursuant to it would supersede state law "relating to a covered provider, to the extent that the provision relates to the maintenance of: (1) records covered by [the ADD] Act; or (2) any other personally identifiable information or personal identification information."

2. Social Media Privacy and Consumer Rights Act (S. 189)

Current status: Originally introduced by Sen. Klobuchar (D-MN) and Sen. Kennedy (R-LA) in April 2018 (as S. 2728), the bill was reintroduced in January 2019 and referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

- Operators of "covered online platforms," defined as "any public-facing website, web application, or digital application (including a mobile application)," would be required:
  - to give consumers prior notice and the ability to opt out of collection and use by third parties of "personal data of the user produced during the online behavior of the user, whether on the online platform or otherwise," both when the user first opens an account and whenever a new product results in new forms of data collection or use;

    - to disclose terms of service, including concerning collection and use of personal data, in a form that is "easily accessible," "of reasonable length," "clearly distinguishable from other matters," and stated in "language that is clear, concise, and well organized";
    - to maintain and publish a description of their privacy and data security program, including who would have access to users' personal data and for what purposes and how privacy risks of new products will be addressed;
    - to provide consumers, upon request, with a copy of their personal data and a list of persons who received the data from the operator, free of charge and in an easily accessible form;
    - to notify affected users of transfers of personal data in violation of the operator's privacy or data security policies within 72 hours of the company's becoming aware of the violation and provide options to prevent the company's further collection, use, storage, and/or sharing of the consumer's personal data; and
    - to audit their privacy and data security program every two years.
- Many of the bill's requirements would not apply to the development of "privacy-enhancing technology."
- The FTC, state attorneys general, and other state consumer protection officials could enforce the law; the FTC's authority would extend to nonprofit organizations and common carriers.

3. Data Care Act (S. 3744)

Current status: Introduced by Sen. Schatz (D-HI) and 14 other Democratic Senators in December 2018, the bill has not been re-introduced in the current congressional session.

Key provisions:

- "Online service providers," defined as entities "engaged in interstate commerce over the internet or any other digital network" and that "in the course of business, collect[] individual identifying data about end users," would be required to fulfill fiduciary duties of care, loyalty, and confidentiality.
    - The duty of care would require service providers to "reasonably secure individual identifying data from unauthorized access" and promptly notify affected end users of a breach of that duty.
    - The duty of loyalty would prohibit a service provider from using individual identifying data or data derived from individual identifying data to benefit the service provider to the detriment of an end user and that would result in reasonably foreseeable and material physical or financial harm to an end user or would be unexpected and highly offensive to a reasonable end user.
    - The duty of confidentiality would prohibit service providers from disclosing or sharing individual identifying data except as consistent with the duties of care and loyalty; require the service provider to enter into a contract with the recipient imposing on the recipient the same fiduciary duties; and require the service provider to audit the practices of the recipient to ensure its fulfillment of the duties.
- The FTC would be given rulemaking authority to exempt categories of online service providers from the law—considering the privacy risks based on such factors as size, complexity and nature of offerings, and sensitivity of consumer information handled and the costs and benefits of coverage—and to create more detailed breach notification requirements.
- The FTC, state attorneys general, and state consumer protection officials would have enforcement authority; the FTC's authority would extend to nonprofit organizations and common carriers.
- The bill explicitly states that it would not preempt state laws or regulations (or supersede other federal laws or regulations).

4. Consumer Data Protection Act

Current status: Sen. Wyden (D-Or) released a discussion draft in November 2018. The bill has not yet been introduced.

Key provisions:

- "Covered entities" would be defined as persons, partnerships or corporations over which the FTC has jurisdiction and which (i) had at least $50 million in average annual gross receipts for the three prior years; (ii) had personal information on at least 1 million consumers and 1 million consumer devices; and (iii) was a data broker or other commercial entity that, "as a substantial part of its business, collects, assembles, or maintains personal information personal information concerning an individual who is not a customer or an employee of that entity in order to sell or trade the information or provide third-party access to the information."
- The FTC would be given rulemaking authority to define and enforce:
  - reasonable cybersecurity and privacy practices and procedures,
  - consumer access and correction rights for stored personal information, and
  - disclosure to consumers of third parties with whom data is shared.
- Covered entities that have not less than $1 billion in annual revenue and that collect, store, or use personal information on more than 1 million consumers or consumer devices or ones that collect, use, or store personal information of more than 50 million consumers or consumer devices would be required to submit to the FTC annual data protection reports—certified to by their CEO and Chief Information Security Officer (CISO)—describing in detail how they were in compliance with regulations issued by FTC.
- The FTC would be required within two years of enactment to create a "Do Not Track" website that would allow consumers to opt out of the sharing, storage, and use of their personal information.
- Covered entities would be able to offer free services in exchange for being allowed to share consumers' information, but they would be required to provide a paid option and clear and conspicuous notice of the terms; the price of the paid option could not be greater than the value to the company of the consumer's data.
- The FTC would be given civil penalty authority, up to $50,000 per violation or 4% of annual gross revenue, whichever is greater.

5. Consumer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act (S. 2639/H.R. 5815)

Current status: Introduced by Sen. Markey (D-MA) and Sen. Blumenthal (D-CT) in April 2018, the bill was referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

- "Edge providers" would be defined as providers of a service over the Internet, or using a software program, mobile application or connected device, that requires subscribers to share various kinds of personal information, requires users to sign up for an account, requires users to purchase the service without an account, or provides a search function
- The FTC would be required to promulgate regulations within one year of enactment that would require edge providers:
  - to notify consumers about the types of sensitive personal information they collect, use, and share, and for what purposes;

- to provide opt-in consent for the use, sharing, or sale of sensitive personal information;
- to ensure that deidentified sensitive personal information cannot be re-identified;
- to assess the reasonableness of any discounts or incentives they offer consumers in exchange for consent to use or share their sensitive personal information;
- to serve consumers regardless of whether they consent to the use and sharing of their data;
- to maintain reasonable data security practices; and
- to notify customers of a breach of sensitive personal information when harm is reasonably likely.

- Various federal agencies would have enforcement authority over companies within their jurisdiction; the FTC would have jurisdiction outside those jurisdictions, including over telecommunications companies; state attorneys general would also have enforcement authority.

6. Information Transparency & Personal Data Control Act (H.R. 6864)

Current status: Introduced by Rep. DelBene (D-WA-1) and Rep. Jeffries (D-NY-8) in September 2018, the bill was referred to the Committee on Energy and Commerce.

Key provisions:

- The FTC would be required to promulgate regulations within one year of enactment requiring operators of websites or online services that are within the FTC's jurisdiction or that are common carriers within the jurisdiction of the Federal Communications Commission (FCC) and that collect, buy, or use sensitive personal information:
  - to provide users with notice of a privacy and data use policy in clear, concise, intelligible form and in clear and plain language, which must identify the types of information collected, used, and shared, with which third parties, and for what uses;
  - to provide users with express opt-in consent to any functionality involving the collection, storage, use, or sharing of sensitive personal information (except where consistent with the company's relationship with the user);
  - to provide users with opt-out consent for the collection, storage, use, or sharing of other personal information; and
  - to undertake annual privacy audits by outside evaluators.
- Several kinds of operations would be exempted: those necessary for preventing and detecting fraud; protecting the security of people or systems; protecting the health, safety, rights or property; providing information in response to valid legal process; and monitoring and enforcing agreements between a covered operator and another party.
- The FTC, state attorneys general, and other authorized state officers would have enforcement authority.

7. Application Privacy, Protection, and Security (APPS) Act (H.R. 6547)

Current status: Introduced by Rep. Johnson (D-GA-4) and four other Representatives from both parties in July 2018, the bill was referred to the Subcommittee on Digital Commerce and Consumer Protection of the House Energy and Commerce Committee.

Key provisions:

- Developers of mobile apps subject to the jurisdiction of the FTC would be required:
  - to provide notice to users of their personal data collection, use, storage, and sharing practices before collecting personal data about the user, including identifying the types of personal data

collected, the parties with which personal data is shared, and the uses for which the data is used and shared;
    - to get users' consent before collecting personal data about them;
    - to provide users with a method to withdraw consent; and
    - to take reasonable and appropriate steps to prevent unauthorized access to personal data and de-identified data collected by the app.
- The FTC would be required to issue implementing regulations within one year of enactment, including with respect to the form of the required notice.
- Both the FTC and state attorneys general would have enforcement authority.
- The bill contains a safe harbor for companies that comply with a code of conduct developed through the NTIA's multi-stakeholder process and approved by the FTC.
- The bill states that it and its implementing regulations would preempt only state laws that conflict with them, specifically relate to the treatment of personal data or de-identified data, and provide a level of transparency, user control, or security in the treatment of personal data or de-identified data lower than that provided by the bill.

8. Data Broker Accountability and Transparency Act (H.R. 6548/S. 1815)

Current status: The House version was introduced by Rep. Johnson (D-GA-4) and three other Democratic Representatives in July 2018. It was referred to the Subcommittee on Digital Commerce and Consumer Protection. The Senate version was introduced by Sen. Markey (D-MA), Sen. Sanders (I-VT), and three other Democratic Senators in September 2017. It was referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

- Covered data brokers, defined as commercial entities that collect, assemble, or maintain personal information about individuals who are not customers or employees in order to sell or provide third parties access to that information, would be:
    - prohibited from obtaining or disclosing or attempting to obtain or disclose personal information or any other information relating to a person by making a false, fictitious, or fraudulent representation;
    - prohibited from soliciting any other person to obtain or disclose such information in such fraudulent ways;
    - required to provide individuals with a means to review at the individual's request at least once per year information that specifically identifies the individual and to dispute the accuracy of such information;
    - required to correct inaccurate information within a period specified by the FTC by regulation;
    - required to give individuals a reasonable opportunity to express their preference that their information not be used or shared for marketing purposes;
    - required to maintain a website providing individuals with clear notice about the access, dispute, and correction process in a form specified by the FTC by regulation; and
    - required to establish measures that facilitate auditing its compliance.
- The FTC would have rulemaking authority to flesh out the law's requirements, including modifying the definition of "personal information," and to create exceptions.
- Both the FTC and state attorneys general would have enforcement authority.
- Companies subject to the Fair Credit Reporting Act (FCRA) would remain subject to FCRA rather than this law.

Conclusion

WilmerHale's Cybersecurity and Privacy Practice will continue to track and provide periodic reports on the development of federal privacy legislation over the course of 2019.

---

1. *See, e.g.*, US Chamber of Commerce; Internet Association; Business Software Alliance; National Retail Federation; American Bar Association; American Bankers Association; Center for Democracy & Technology; Center for Democracy & Technology; Electronic Frontier Foundation; Information Technology & Innovation Foundation. The US Chamber of Commerce has also recently issued a draft model federal privacy bill.

2. Our alert on the NIST privacy framework process is here.

Contributors

Jonathan G. Cedarbaum

PARTNER

D. Reed Freeman, Jr.

PARTNER

Lydia Lichlyter

ASSOCIATE