
Congressional Committees Hold Hearings on Federal Privacy Legislation

March 1, 2019

This week both the House and Senate held hearings kicking off the legislative process for federal privacy legislation. Legislators from both parties voiced support for comprehensive and bipartisan legislation. Most of the witnesses were representatives of industry associations, joined by privacy advocates and one professor.

As suggested in our recent preview [report](#), the central points of discussion included: (i) the extent to which the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) should serve as models or cautionary tales; (ii) the appropriate scope of federal preemption of state privacy requirements; (iii) possible limits on the collection, use and sharing of certain kinds of highly sensitive information; (iv) rights that consumers and other individuals whose personal information is handled should have to control those activities; (v) whether smaller companies and startups should receive special treatment; and (vi) expanded enforcement powers for the Federal Trade Commission (FTC).

Summaries of each of the hearings can be found below, along with links to witness statements, transcripts, and model bills that were considered.

House Energy and Commerce Hearing

On February 26, the House Energy and Commerce Committee's Subcommittee on Consumer Protection and Commerce held a hearing titled "[Protecting Consumer Privacy in the Era of Big Data](#)." A full transcript of the hearing is available [here](#). The witnesses, a mix of industry representatives and privacy advocates, were:

- [Brandi Collins-Dexter](#) from Color of Change, an online civil rights organization;
- [Dave Grimaldi](#) from the Interactive Advertising Bureau (IAB), a trade group for online advertisers;
- [Roslyn Layton](#) from the American Enterprise Institute (AEI), a public policy think tank;
- [Nuala O'Connor](#) from the Center for Democracy & Technology (CDT), a nonprofit focused on online privacy, who also spoke at the Senate Commerce Committee's [hearing](#) last October; and

- [Denise Zheng](#) from Business Roundtable, a group of CEOs of major US corporations.

Witnesses and subcommittee members expressed support for some form of federal privacy legislation, both in order to strengthen protections for consumers and in order to provide uniform national standards. There was also substantial consensus that while the CCPA and the GDPR provide important points of reference for federal privacy standards, those models also reflect in certain respects overly prescriptive approaches that may harm innovation and competition.

In her opening statement, Rep. Jan Schakowsky (D-IL), chair of the subcommittee, suggested that the current notice-and-choice system of privacy protection places significant burdens on consumers and called for expanded FTC enforcement powers. She highlighted the difficulty for consumers of reading and understanding the many privacy policies they encounter, saying that “[a] person should not need to have an advanced law degree to avoid being taken advantage of.” Several other Representatives, including Rep. Frank Pallone (D-NJ), chair of the full committee, echoed Schakowsky’s theme of reducing burdens on consumers.

Other issues that provoked significant discussion included:

Federal Preemption

Many Representatives, particularly Republicans, highlighted the compliance problems caused when companies have to operate under a patchwork of state laws, thus emphasizing the importance of establishing national standards that would trump state requirements. Rep. McMorris Rodgers (R-WA), the subcommittee’s ranking member, for example, stated that the internet “knows no borders” and that putting in place uniform federal standards “makes common sense.” A number of other members of the subcommittee echoed this theme, some even suggesting that state privacy laws could run afoul of the Dormant Commerce Clause.

Use Limitations and Individual Rights

Witnesses across the panel expressed support for establishment of clear use limitations—setting out specific things that may not be done with data—and recognition of data subject rights such as rights to access, correct and delete their personal information.

The CDT’s [model bill](#) includes both types of protections, and Ms. O’Connor specifically referred in her testimony to concerns about secondary uses of sensitive data; that is, uses beyond the scope of the original transaction. For certain kinds of sensitive data, such as biometric information and Social Security numbers, she argued that no secondary uses should be permitted, even with consent; a separate transaction would be required instead.

The IAB did not go that far, but Mr. Grimaldi spoke in favor of “clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law.” Ms. Zheng focused instead on the framework of data subject rights, voicing the Business Roundtable’s support for consumer rights to transparency, control, access, correction and deletion.

Small Businesses

Representatives from both parties raised concerns about new requirements imposing compliance costs that could be borne only by large companies, thus disadvantaging smaller firms and startups and entrenching incumbent companies' advantages in some markets.

Definition of Personal Information

While the general definition of "personal information" did not draw significant attention, several Representatives raised concerns about the collection, use and sharing of particular kinds of information such as health, geolocation and audio data. Rep. Blunt Rochester (D-DE) suggested that, as under the CCPA, inferences drawn from data and used to create profiles of individuals should be included in the definition of information triggering data subjects' rights.

FTC Authority

Many Representatives appeared to take it as a given that the FTC would be charged with the enforcement of any law that is passed. Rep. Schakowsky stated that "it is important to equip regulators and enforcers with the tools and funding necessary to protect privacy," but she also described a need to understand why the FTC has not used its existing tools and authority more forcefully. Ms. Collins-Dexter argued in her remarks for the establishment of a new federal agency focused on privacy.

Senate Committee on Commerce, Science, and Transportation Hearing

On February 27, the Senate Committee on Commerce, Science, and Transportation held a hearing on [Policy Principles for a Federal Data Privacy Framework in the United States](#). A full transcript of the hearing is available [here](#). The witnesses, drawn from industry associations and academia, were:

- [Jon Leibowitz](#), former FTC chairman, co-chair of the 21st Century Privacy Coalition, a coalition of major communications companies;
- [Randall Rothenberg](#), CEO of the Interactive Advertising Bureau, a trade group representing 650 media and technology companies;
- [Michael Beckerman](#), president and chief executive officer of the Internet Association; an internet company trade group;
- [Woodrow Hartzog](#), professor of law and computer science at Northeastern University School of Law and Khoury College of Computer Sciences;
- [Brian Dodge](#), chief operating officer of the Retail Industry Leaders Association; and
- [Victoria Espinel](#), president and CEO, BSA | The Software Alliance, a software industry advocacy organization.

Chairman Roger Wicker (R-MS) began the hearing by emphasizing the benefits of innovation, technology and connectivity and the risks associated with collecting consumer data. He suggested that a "uniquely American" federal data privacy framework could preserve the benefits of the internet economy while protecting Americans.

By contrast, Ranking Member Maria Cantwell (D-WA) followed Sen. Wicker's opening by describing a number of major data breaches and incidents involving the use or sale of personal information for

purposes unauthorized by the affected individuals. She praised the GDPR as an important model for congressional efforts.

The witnesses diverged in their views on the appropriate approach to privacy regulation. A number of the witnesses from industry groups emphasized user choice, control and transparency. Dr. Hartzog and Ms. Espinel suggested that these principles did not go far enough; they advocated express prohibitions on collection and use of some types of data.

Federal Preemption

Chairman Wicker began the question-and-answer portion of the hearing with this topic. With the exception of Dr. Hartzog, the panelists favored federal preemption of state privacy standards. They raised the same specter of a confusing and expensive patchwork of state laws that had concerned a number of House panelists.

Use Limitations and Data Subject Rights

Witnesses and lawmakers proposed several models and guiding principles to inform substantive protections and limitations. Mr. Beckerman argued that federal privacy legislation should focus on individual rights and give users the ability to access, delete, correct and move their personal information. Mr. Dodge echoed these elements.

Dr. Hartzog, in contrast, asserted that the notice-and-choice framework is broken. He suggested a new model of “trust rules,” asking that data collectors be honest, discreet, protective and loyal. In addition, he recommended establishing several “data boundaries,” including (i) prohibiting the collection and aggregation of certain kinds of data (biometric and genomic data, for example) and (ii) requiring companies to have a “legitimate interest” in collecting data.

A key theme throughout Ms. Espinel’s testimony was the importance of distinguishing between data controllers (those who determine the means and purposes of processing data) and data processors (those who store, process and perform other operations on data on behalf of controllers). She said that data protection responsibility should differ across the categories and data controllers should have heightened responsibilities. She also suggested that uses of consumer data that violate a user’s reasonable expectations should be prohibited.

Mr. Leibowitz cautioned that privacy should not be about who collects an individual’s personal information, but about what information is collected, and how it is protected and used. It should therefore be industry- and technology-neutral.

Definition of Personal Information

The witnesses agreed that different types of data warrant different protections, but they disagreed on the details. Mr. Leibowitz, for example, named health and financial information, precise location information, Social Security numbers and children’s information as categories that deserve special protections. Mr. Dodge suggested that data that was aggregated, publicly available, pseudonymous, de-identified, related to a household instead of an individual, harmless or collected from an employee should be excluded from the definition of sensitive personal information.

Small Businesses

In contrast with the House hearing, the Senate hearing saw little discussion of the potentially harsher impact of new requirements on smaller businesses. Sen. Young (R-IN) raised the issue briefly, suggesting that adoption of the GDPR had discouraged investment in startups and had helped larger incumbent companies gain increased market share. A number of the witnesses agreed that creating a small business carve-out for certain requirements may be appropriate.

FTC Authority

Witnesses and lawmakers agreed that the FTC should have primary enforcement authority for any new data privacy legislation. The witnesses also expressed support for the FTC's being given civil penalty authority, rulemaking authority and additional resources for enforcement. Several witnesses also suggested that state attorneys general should have concurrent enforcement authority with the FTC.

Mr. Leibowitz contended that federal legislation should not include criminal penalties or a private right of action. Dr. Hartzog argued that a private right of action is necessary for robust enforcement.

Conclusion

WilmerHale's [Cybersecurity and Privacy Practice](#) will continue to monitor and provide periodic updates on the development of comprehensive federal privacy legislation over the course of 2019.

Contributors



Jonathan G. Cedarbaum

PARTNER



D. Reed Freeman, Jr.

PARTNER



Lydia Lichlyter

ASSOCIATE
