Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What Businesses Want: A National Consumer Privacy Law

By **David Saunders** (September 30, 2019, 4:14 PM EDT)

David Saunders

In 2001, Hollywood gave us the rom-com, "What Women Want," and 2019 saw the release of "What Men Want." If Hollywood is any indicator, we are constantly in search of an understanding of what others around us want. Certainly as a lawyer working with clients, at the end of the day, what we really want to understand what our clients want.

Well, at least with respect to 51 of the CEOs of some of the largest companies in the United States — from AT&T to Zebra Technologies Corporation — we know at least part of the answer: They want "a comprehensive consumer data privacy law." We know that because on Sept. 10, 51 CEOs signed a letter from the Business Roundtable that was sent to every member of the U.S. Congress, requesting just that.

The letter itself is a balancing act, attempting to find the middle ground between "enable[ing] continued innovation and growth in the digital economy," i.e., not stifling corporate growth and profits while also giving consumers "meaningful rights over their personal information." Those two goals are often in tension, and that tension is currently on display as California considers amendments to its hastily drafted California Consumer Privacy Act of 2018.

As to why these business leaders want a "comprehensive" "consumer privacy framework" at the national level, the letter explains:

> Consumers should not and cannot be expected to understand rules that may change depending upon the state in which they reside, the state in which they are accessing the internet, and the state in which the company's operation is providing those resources and services.

While framed as an issue of consumer understanding — undoubtedly an issue — the "increasingly fragmented and more complex" laws that are developing on a state-by-state basis also "threaten[]" "innovation and global competitiveness" of U.S. companies. Put differently, if companies have to invest millions of dollars every year updating privacy and data security practices to catch up to the newest CCPA copy-cat bill, that could distract from the business objectives of a company. Both explanations as to why a national privacy bill is desirable are not only spot on, but are completely understandable.

On its face, the request to Congress is simple: develop a single, unified law that creates a single privacy and data security rubric for companies to follow. As is often the case, however, the devil lies in the details.

The Business Roundtable's letter attaches a "Framework for Consumer Privacy Legislation,"[1] which the Business Roundtable released in December 2018. That document reflects a thoughtful mix of current policy and data security concepts in an attempt to unify what has become a vast and disparate array of privacy laws, regulations and rules at the state and federal level. The keys to the framework are that "a national consumer privacy law should preempt any provision of a statute, regulation, rule or agreement or equivalent of a state or local government" and should apply "across industry sectors." To keep with our Hollywood theme and invoke "The Lord of the Rings," there would be one law to rule them all.

Digging in a little more, we see that the proposed framework draws from the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the EU's General Data Protection Regulation and other federal and state laws. The principles set forth at the beginning of the framework are foundational privacy objectives: (1) robust protections for consumers and enforced accountability; (2) endorsing a principles-based approach and not proscribing specific technologies or protections for companies to employ; (3) eliminating the disparate regulations that exist presently and (4) "facilitat[ing] international transfers."

We see each of these goals play out through the rest of the framework, starting with the Business Roundtable's views as to which entities should be covered by a national consumer privacy law. On this score, the Business Roundtable suggests that the law apply across all industries. Gone would be the day where there are different laws for medical information and financial information; they would all be treated the same. Interestingly, while not committing to the concept, the framework looks out for the startups of the world and suggests that "[c]are should be given to how or if small companies that do not process much personal data or engage in low risk processing of data should be covered."

This concept may be a dead issue to consumer rights advocates who likely would take the view that if a company is handling even one personal record, the law should apply. However, the concept of a sliding-scale approach to privacy is well ingrained and rooted in existing privacy laws. As many lawyers and even those who have tried to start their own business know, sometimes the cost of privacy compliance is prohibitive in the early stages of a business. The last aspects of applicability for the framework should be familiar: preemption over all state and local laws as well as a commonplace exception that permits sharing of information for government or law enforcement activities.

The framework next addresses one of the hotter battlegrounds in privacy today: what counts as personal data. Almost every state data breach law includes a different definition of personal information, and the GDPR definition is different than that of CCPA, which is different from HIPAA's and so on. In short, practically every privacy law that is enacted has its own definition of what is protected. The proposed framework would do away with all of these competing definitions and develop a single rubric: "data that is held by the organization and identifies, or is identifiable to a natural, individual person."

Included in this framework would be "information derived from a specific device that reasonably could be used to identify a specific individual." Excluded, however, would be de-identified data and certain data in the public domain; common exceptions to most current privacy laws. This framework would offer a narrower protection than what the CCPA proposes (which applies to households and not just individuals), but would be broader in many ways that the sector-specific laws and data breach laws that exist. The framework also proposes a GDPR-like categorization of personal information so that certain information that "may present increased risk" is handled or treated with additional care. Though the framework suggests this division of data types, it leaves silent what the impact of this data categorization would or should be.

With respect to the implementation and corporate governance surrounding privacy policies and practices, the framework suggests a "risk-based" approach; one that "assess[es] and balance[es] the interests in and benefits of the processing to organizations, individuals and society against the potential risks and applying appropriate mitigations." Put more succinctly, a sliding-scale privacy model that would be built off regular "privacy impact assessments" and "policies and procedures that reflect" privacy principles appropriately. This approach to implementation is akin to the current HIPAA framework, which requires covered entities to adopt appropriate administrative, technical and physical safeguards based on the company's risk assessment of the information they possess versus how it is handled and the threats to that information.

This type of privacy implementation is undoubtedly business-friendly and would likely be the subject of much negotiation with consumer advocates who likely would seek certain minimum protections. Again, however, the difficulty with requiring any one method of compliance is stifling smaller companies or developing a law where enforcement authorities look the other way because it is practically impossible for smaller companies without massive assets or good legal counsel to comply.

Perhaps the most interesting part of the framework for consumer rights advocates is how the framework addresses what individual rights consumers should have with respect to their data. On this score, the framework models the CCPA and to some degree, the GDPR. The framework proposes rights around transparency, consumer control of their data, access and correction and deletion.

Put differently, a person would have a right to know what is collected about them, to control (under certain circumstances) how or if that information was shared with a third party, to correct or amend the information and to request deletion of the information within reason. And once again there is the rub. While on its face, the framework outlines broad rights for consumers, the details of the framework contain exceptions that range from business necessity to creating incentives for individuals to allow the sharing of their data or lose free content from the business. These types of exceptions would undoubtedly be the subject of much negotiation if a national consumer privacy bill were to move through Congress.

The framework also contemplates a uniform data breach notification standard — doing away with the competing laws of the 50 states plus the territories. This would undoubtedly be a relief not only to businesses, who currently have to send different notices with different content to different people and places for any widespread incident as well as to consumers, who have become barraged in the recent past with notices of data incidents.

And finally, the enforcement mechanism for this theoretical law would lie with both the Federal Trade Commission and state attorneys general. The right of state attorneys general to pursue claims under any federal data protection law is perceived by many in the industry to be a key factor in gaining state support for any effort to create a national law and preventing states from trying to challenge or legislate around the law. As a result, it is not a surprise that the framework contemplates the ability of states to enforce what would be a federal law.

While enforcement would lie with the FTC and the state attorneys general, the framework precludes a private right of action. This issue of whether an individual can pursue claims against a company related to privacy and data security issues is a hotly contested one. The litigation space is rapidly filling with more aggressive plaintiffs attorneys who are finding new and creative ways to bring individual — and more often — class action litigations against companies for violations of a variety of state and federal privacy laws. Whether these class actions have a demonstrable benefit to the individual class members beyond what could be accomplished through a federal or state attorney general regulatory proceeding is hard to

discern. Regardless, the lack of a private right of action – one of the CCPA hallmarks that some, including the California attorney general have sought to expand – would likely be a point of much discussion during the drafting of any legislation.

And so here we are, at the end of our tour through the Business Roundtable's letter and framework, and the inevitable question is whether anything will come of this letter and framework. Unfortunately, dear reader, this ending is a bit like the end of "The Sopranos"; a fade to black without truly being sure of what happens next. The only thing we know is that this letter will land in the Russell, Dirksen, Hart, Cannon, Longworth, Rayburn and Capitol offices and what happens after that we shall have to wait and see. In this author's view, it is more likely that we will have more, and perhaps many more, CCPA copycat laws at the state level before we get anything resembling the one law to rule them all, a "comprehensive consumer data privacy law." The one thing we can say, however, is that it seems to be the things that businesses want.

David Saunders is a partner at Jenner & Block LLP.

[1] Available at https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf.