DORSEY
DORSEY+WHITNEY LLP

Will California's New Privacy Law be Preempted? Federal Hearings and Public Comments Begin

October 4, 2018 – The TMCA
by Jamie Nafziger and Cody Wamsley

Although numerous attempts have been made to pass a comprehensive U.S. privacy law over the years, this one might actually succeed. Efforts have begun on multiple fronts. From Senate Commerce Committee hearings to several federal agencies vying for which will lead a federal regulatory effort, privacy is a hot topic in Washington, DC. Businesses should take immediate action to enter the discussions if they have not already done so. Comments on a proposed federal framework are due **October 26, 2018**. The Commerce Committee will hold additional hearings in October. Industry is coming to the table in an attempt to avoid facing a jumble of inconsistent state privacy laws.

Fresh off their European privacy compliance efforts, U.S. businesses have begun facing another significant compliance hurdle: the monumental California Consumer Privacy Act of 2018 (CCPA), which takes effect in 2020. Amendments have already been passed to the CCPA and more are in the works for 2019. Other states have begun considering enacting their own comprehensive privacy statutes. Facing an increasingly complex and inconsistent patchwork of privacy laws both in states and internationally, U.S. businesses have begun lobbying for a federal standard to preempt the state efforts.

On September 26, the United States Department of Commerce National Telecommunications and Information Administration (NTIA) published a Request for Comment (RFC) seeking input from industry participants in developing a "user-centric"

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

set of privacy outcomes and associated goals for federal action to achieve such outcomes. This RFC was issued into an environment where, simultaneously, the National Institute of Standards and Technology (NIST) is beginning work on a voluntary Privacy Framework. In addition, the United States Senate Committee on Commerce, Science, and Transportation held a hearing on "Examining Safeguards for Consumer Data Privacy" on the same day. Given these three concurrent efforts by entities within the federal government, it is apparent that industry pressure on the government to relieve companies of the increasing burden of complying with a growing patchwork of privacy laws has reached a point where federal action is inevitable.

The RFC provides industry participants with an immediate opportunity to provide input on such actions through the Executive Branch. The RFC seeks input on seven user-centric privacy outcomes:

1. Transparency – the ability for users to understand what organizations are doing with their data
2. Control – the ability for users to have a say in what organizations do with their data
3. Reasonable Minimization – preventing organizations from collecting or using data for more than reasonable purposes
4. Security – ensuring that organizations protect user data
5. Access and Correction – the ability for users to see and rectify personal data that organizations have collected about them
6. Risk Management – ensuring that organizations take steps to prevent harmful uses of data
7. Accountability – holding organizations responsible for their use of data

The RFC also seeks input on eight goals for federal action:

1. Harmonize the regulatory landscape – eliminate or align the patchwork of privacy regulations, at least within the United States
2. Provide legal clarity while maintaining the flexibility to innovate – provide clear rules with which organizations can know they are in compliance
3. Apply comprehensively – apply privacy rules to all organizations to the extent they are not governed by existing sectoral privacy laws such as COPPA, GLBA, HIPAA, and FCRA
4. Employ a risk and outcome-based approach – allow organizations flexibility in compliance with laws (eliminate checkbox compliance)
5. Increase Interoperability – align U.S. privacy laws with international privacy laws to decrease friction for international commerce
6. Incentivize privacy research – encourage development of privacy protections
7. Support FTC enforcement – provide the FTC with clear authority to enforce privacy regulations
8. Provide Scalability – allow for scaled penalties based on reasonable factors

In addition, the RFC seeks input on what next steps the Trump Administration should take, which key definitions should be included in any privacy efforts, what resource changes would be needed for the FTC to enforce privacy regulations, the impact of privacy regulation on international commerce, and other ideas commenters have to improve privacy regulations in the U.S., not mentioned in the RFC.

Several organizations have already released public comment on proposed frameworks, see Electronic Frontier Foundation, Google, Interactive Advertising Bureau, Internet Association, Microsoft, and U.S. Chamber of Commerce.

The RFC was released on the same day the Senate Commerce Committee held a hearing on the same topic, but under a different framework. Unlike the RFC, the Senate is seeking to draft federal legislation to govern privacy in the U.S. At yesterday's hearing, representatives from AT&T, Amazon, Google, Twitter, Apple, and Charter Communications gave testimony to help the Committee formulate an approach to developing broad federal privacy laws. In the hearing, it was clear that all industry representatives were looking to limit the growing patchwork of privacy regimes that have become a burden for organizational compliance. Industry participants focused on federal preemption throughout their testimony. Indeed, Senator Schutz stated that "the holy grail is preemption" from the standpoint of companies while he noted that from his perspective, such an effort is not likely to succeed if it does not go as far as California's recent CCPA in terms of consumer rights and protections.

Some of the additional takeaways from the hearing, which may be useful for companies thinking about responding to the RFC or increasing their advocacy efforts, are:

- All companies present recognized the importance of protecting consumer privacy but had developed varying techniques for informing consumers and safeguarding their privacy. Google, for example, touted its constantly evolving privacy policy and privacy settings controls in its Google Account feature
- Each company present had differing interests, business models, and approaches to privacy. For example, Twitter is public by default so its privacy compliance needs will differ from those of companies which collect personal information for internal use only. Amazon's representative clearly stated that protecting privacy was critical to meeting its customer expectations. Marked differences existed between paid service and free service views on several points.
- Multiple companies opened with statements that transparency, control, portability, security, and uniformity were paramount concerns for developing appropriate privacy regulations.
- The Committee spent significant time exploring how companies had endeavored to comply with the E.U.'s General Data Protection Regulation (GDPR) in an effort to understand the likely burden on American companies in complying with a similar regulation. Google stated that it had spent "hundreds of years" of human time with a cost "multiple orders of magnitude" greater than millions of dollars to achieve GDPR compliance.
- Interestingly, all companies present agreed that the FTC should be provided additional resources to enforce privacy regulations, but most companies did not go so far as to agreeing that the FTC should have more rulemaking authority when it comes to privacy.

Both the RFC and Google's proposed framework suggest that users should have access to personal data they have provided and the ability to correct or have deleted such data. Because of the January 1, 2020 compliance deadline set in the CCPA and the lead time companies need for the significant compliance efforts required by the CCPA, motivation

is high to take quick action on a federal level.

The RFC has an October 26, 2018 response deadline. If you would like more information regarding U.S. or international privacy laws and regulations, please follow our updates in future on the TMCA or those issued from Dorsey & Whitney LLP's Cybersecurity, Privacy & Social Media industry group.