FIVE QUESTIONS YOU SHOULD BE ASKING AS CONGRESS TAKES ON PRIVACY LEGISLATION

Date: 6 February 2019

U.S. Cyber Law and Cyber Security; Privacy, Data Protection and Information Management; Technology Transactions; and Public Policy and Law Alert

By: Pamela J. Garvie, William A. Kirk, Mark H. Wittow, Peter V. Nelson

Over the past few months, the question of "if" Congress should strengthen privacy protections has increasingly become a matter of "when" and what form the legislation should take. Republican and Democratic congressional leaders have pledged to take action on privacy this year; a number of legislative proposals have already been introduced and others are under development, and this is one of the few legislative areas where bipartisan agreement is possible. While the debate is still in its early stages, its potential implications are significant — namely, the creation of a new federal privacy regime that would be the American answer to the European Union's General Data Protection Regulation ("GDPR") and potentially head off state-by-state regulatory efforts like the California Consumer Privacy Act of 2018 ("CCPA").

This is a development that should be on the radar screen of every organization that handles personal information. The integrated team of privacy and public policy professionals at K&L Gates has developed the following five questions to begin your analysis of the legislative debate and start planning the next steps as it moves forward. More likely than not, privacy is a central concern for your organization, and it will be essential to monitor the action in Congress and engage with policymakers as needed to protect and advance your interests. We can help.

1. DOES THIS IMPACT ME?

The big-tech giants have received most of the media attention so far, but the reality is that a federal privacy law would create new obligations for every organization that collects, uses, processes, stores, or shares personal information. This is an effort of a similar scale and scope as the GDPR and the CCPA. If your organization's activities potentially are covered by either regime, it is likely that the legislation Congress is considering will be relevant too. The bottom line is that the implications of the federal privacy debate cut across industries and sectors.

2. WHAT COULD THIS MEAN FOR MY ORGANIZATION?

It is too early to say what the final privacy legislation will look like, but it is safe to assume that it will entail new obligations for organizations and potentially create new legal exposure and enforcement risk. Some of the key issues under discussion include the following:

- **New Individual Rights and Disclosures**: Policymakers have proposed significant new compliance obligations for organizations. They are expected to require organizations to disclose how they collect, use, process, share, and store personal information and give individuals greater control over their information. New requirements or standards in these areas are expected to emerge, particularly with respect to sensitive personal information and social media.
- **Opt-in vs. Opt-out**: A central issue policymakers are considering is whether the United States should follow the GDPR approach of requiring users to affirmatively "opt-in" to data collection, sharing, and use — not only for sensitive information but beyond. The resolution of this issue could create the need for significant reengineering of Web services and architecture, as well as other compliance changes.
- **Strengthened Federal Trade Commission ("FTC") Authority**: Although the FTC is the federal government's top privacy watchdog, it lacks the authority to promulgate data privacy regulations (leaving the agency to inefficient ex post "regulation" through enforcement actions), has no jurisdiction over nonprofit organizations and common carriers (like wireless companies), and can only impose civil penalties in limited circumstances. The agency's staff headcount and budget have also not kept pace with the scope of its authority as the digital economy has grown. Federal legislation is expected to grant the agency rulemaking authority, expand its jurisdiction and authority to impose fines, and give it additional resources to pursue its mission.
- **Other Enforcement**: In addition to expanding the FTC's ability to impose civil penalties, some policymakers want to give the agency's enforcement authority even more "teeth." Senator Ron Wyden (D-OR), for one, has proposed prison terms of up to 20 years or significant fines — as much as $5,000,000 — for executives of organizations that violate privacy protections, as well as more significant penalties at the corporate level. Further, while virtually all agree that the FTC should be the lead federal enforcement agency, some also support giving state attorneys general authority to enforce the federal law and providing for private rights of action.
- **Preemption**: The urgency of the current debate in Congress is partially a response to last year's passage of the CCPA, which imposes significant new privacy obligations starting in 2020 and is prompting action by other states that could produce an unwieldy "patchwork quilt" of inconsistent requirements. Policymakers in Congress are grappling with the extent to which federal law should take precedence over state statutes like the CCPA, as well as existing federal privacy statutes that apply to specific industries.

3. IS ANYTHING *REALLY* GOING TO HAPPEN?

There is understandable pessimism about the prospects for sweeping legislation under a divided Congress, but the data breaches, unauthorized sharing, and other privacy violations that have dominated headlines for the past few years have led to a high level of public interest and engagement on the issue. In addition, the CCPA's looming 2020 effective date — and the potential for similar initiatives in other states — has united much of the business community around the need for federal legislation. These trends have made privacy legislation a top priority for House and Senate leaders on both sides of the aisle, as well as the Trump administration. As noted above, policymakers are pressing ahead with plans to hold hearings, draft legislation, and move a bill as early as this summer.

Of course, the devil is always in the details, and there is a possibility that these legislative efforts could fall short. Although there is broad interest in privacy legislation among stakeholders and policymakers, there are important differences of opinion about its specifics that could be difficult to reconcile. However, even if the proposals under debate do not make their way into law this year, they will still set a marker for future initiatives — underscoring the importance of the present legislative debate.

4. HOW DOES THIS AFFECT MY EXISTING COMPLIANCE PROGRAM?

With GDPR implementation in the rearview mirror, many organizations are looking toward the CCPA as the next major regulatory milestone. The privacy debate in Congress adds uncertainty to this timeline and could complicate compliance strategies going forward. Federal legislation could preempt the California law entirely, introduce new or additional requirements on top of it and other federal laws, open the door to future rulemaking activities, and prompt responsive action by other jurisdictions — including U.S. states as well as foreign governments.

In view of this, consider the need to monitor developments closely so they do not come as a surprise and can be factored into compliance plans sooner rather than later. In addition, early engagement in the process offers a way to advance priorities and address specific problems before legislation is baked into law.

5. WHAT SHOULD I BE DOING TO PREPARE?

Preparing for changes in the U.S. privacy landscape starts with understanding your organization's exposure to personal information and following the various policy proposals under consideration to develop a clear sense of their potential implications for your business and regulatory compliance strategies. Undertaking this evaluation sooner rather than later preserves the option to engage in the legislative debate to shape the final outcome in a way that advances and protects your interests. The integrated team of privacy and public policy professionals at K&L Gates can assist clients in analyzing the potential impacts of legislation and in developing strategies to influence the privacy debate as it moves forward.

KEY CONTACTS

PAMELA J. GARVIE
PARTNER
WASHINGTON DC
+1.202.661.3817
PAMELA.GARVIE@KLGATES.COM

DANIEL L. FARRIS
PARTNER
CHICAGO
+1.312.807.4375
DANIEL.FARRIS@KLGATES.COM

BRUCE J. HEIMAN
PARTNER
WASHINGTON DC
+1.202.661.3935
BRUCE.HEIMAN@KLGATES.COM

WILLIAM A. KIRK
PARTNER
WASHINGTON DC
+1.202.661.3814
WILLIAM.KIRK@KLGATES.COM

MARK H. WITTOW
PARTNER
SEATTLE
+1.206.370.8399
MARK.WITTOW@KLGATES.COM

