DORSEY
DORSEY+WHITNEY LLP

Jail Time for Executives? Federal Privacy Proposals Have Teeth

2019 will bring significant privacy law changes in the U.S. These changes will require significant compliance efforts by companies operating in the U.S. this year. It is still an open question as to whether those compliance efforts will be in connection with a new federal privacy law or the California Consumer Privacy Act of 2018 (CCPA). Numerous companies and members of Congress are calling for federal legislation. Momentum is building. However, unless legislative action is immediate in the new Congress, it is time for companies to begin efforts to comply with the CCPA, if they have not already done so.

Our previous articles describe the CCPA and highlight some of the federal proposals. Here, we address trends in the recent federal proposals.

Criminal Penalties for Executives

U.S. privacy law observers complain that legal accountability is not strong enough for key management personnel when it comes to privacy violations. Employment termination and civil actions (including derivative suits) are currently available as recourse against management. However, some privacy advocates are pushing for more "teeth" in proposed federal legislation. This push has found its way into a few of the more prominent proposals.

Both Senator Ron Wyden's Consumer Data Protection Act and Intel's Innovative and Ethical Data Use Act of 2018 contain *criminal penalties* for business executives that knowingly certify that their privacy practices comply with the law when that is not true. This prospect represents a significant change in the way that authors of mainstream privacy law proposals are approaching the accountability issue. What is even more interesting, though, is that this concept is included in even *private industry's* proposal for privacy legislation. Intel's global privacy officer and key architect of this draft legislation reportedly stated that this inclusion was to drive "the best privacy protection you can get." If this concept gains traction, executives in the United States will want to take note.

Related Capabilities

- Privacy & Social Media
- Trademark, Copyright + Advertising
- Technology Commerce
- Technology
- California Consumer Privacy Act (CCPA)

Standard of Care

A group of 15 Democratic senators introduced the Data Care Act of 2018 on December 12. This draft legislation represents a markedly different approach from the many other proposals that appear to be mimicking the CCPA and GDPR. Rather than providing companies with the ability to do with data pretty much whatever they please so long as they provide consumers with notice of their data practices and seek consent where required, in the Data Care Act, companies are held to duties of care, loyalty, and confidentiality – establishing a fiduciary duty for companies that process personal information. Advocacy groups like the Electronic Frontier Foundation and the Center for Democracy and Technology back this concept. While most businesses will likely oppose this concept and thus limit its political viability, some elements of such duties are implied in other, more widely accepted, draft legislation.

A key question about creating such duties is who will determine the baseline standard of care. At FTC hearings in December on Competition and Consumer Protection in the 21st Century, for example, a call for the FTC to further enforce privacy protections *before* breaches became a recurring theme. During one of the panels, a panelist called for pre-emptive enforcement through an assessment process and likened such pre-emptive enforcement to issuing speeding tickets – there is no actual harm from someone speeding if they don't cause a collision, but the act of speeding makes the roads more unsafe and collisions more likely. Thus, some panelists argued that to prevent breaches, pre-emptive enforcement of baseline standards, a la speeding tickets, is needed. For this to happen, codified standards for baseline security are needed, and these standards would likely end up being sector-specific. Without a codified standard, it would be up to the courts to determine what constitutes the standard of care. This would create a constantly moving target in an already dynamic environment. Companies should pay attention to this and participate, where possible, in the development of industry security standards – particularly generally applicable frameworks such as the NIST Cybersecurity Framework or the upcoming NIST Privacy Framework as these could become *de facto* baselines.

FTC Authority

A third emerging trend is a call for the FTC to have increased authority to enforce privacy laws. Many of the proposals go so far as granting the FTC rulemaking authority on the issue. Currently, the FTC has some authority to enforce privacy rules under Section 5 of the FTC Act, which grants the agency the authority to investigate unfair or deceptive acts or practices. Thus, many of the FTC's current actions resemble false advertising actions as the FTC holds companies accountable for not following their own privacy policies. It also has some rulemaking authority, such as in connection with the Children's Online Privacy Protection Act. Under many proposals, the FTC's authority would be expanded greatly, and the FTC would receive a new privacy/security enforcement mandate. A recurring theme in the calls for expanding the FTC's authority is to move away from focusing on enforcement after a breach and toward pre-emptive actions.

Also, of note, during last month's FTC hearings, at least one panelist called on the FTC

to do a better job of investigating security vendors' advertising claims. The security vendor space has long been known for significant puffery when it comes to claims of security benefits for various products and, as more companies are relying on security vendor products to establish secure systems in lieu of developing their own tools and processes, the argument is that the FTC should take a more active role in investigating these advertising claims. The FTC could do this without any new authority, and it would be an easy first step in expanding the FTC's role in protecting privacy in the United States. Security vendors, especially startups, should take note of this and work with legal counsel to evaluate their marketing efforts.

Likelihood of Short-Term Action

Given the increased attention to a potential federal privacy law, it may be tempting to delay compliance efforts for the CCPA and other emerging state and local privacy rules. We spoke with David Hoffman, Global Privacy Officer at Intel, who has been working with industry leaders and legislators on developing a federal privacy law for several years, about what he has been seeing in these recent legislative efforts. When it comes to the likelihood of a federal law being passed before state and local rules come into effect, Hoffman said, "there is still considerable work that needs to be done working through the substance of a preemptive federal law. However, if states and municipalities continue to pass non-harmonized privacy laws, the need for a federal framework will make passing a law in the next three years much more likely." So, it may still be a few years before a federal law is passed and companies should not delay in their compliance efforts in connection with the emerging patchwork of state and local regulations.

While the news of large security incidents continues to fill our air waves, the prospect of large fines or jail time is not appealing to executives. Companies may want to participate in the federal legislative process. We would be happy to connect them with leaders in the industry efforts to enact a federal statute and to help with compliance efforts in connection with the CCPA.