Cooley

January 28, 2015

Over the past two weeks, President Obama has made clear that cybersecurity continues to be a concern, and he and the administration are increasing their focus on the issue. President Obama kicked off efforts with a speech at the Federal Trade Commission on January 12, 2015, where he articulated a series of major privacy and cybersecurity initiatives being planned by the administration. These proposed changes follow recent large-scale data breaches at several major retailers and destructive cyberattacks on other US-based entities.

The administration plans to take several steps aimed at addressing cybersecurity and improving privacy for consumers. The first component in the President's plan calls for creating a single national data breach notification law that would be significantly stricter than today's patchwork of state laws. One important aspect of this new law would be a thirty-day period within which a company would need to report a data breach to consumers. The second component of the plan is ensuring that individuals have the right to access their free credit scores. The President noted that companies including JPMorgan Chase, Bank of America, USAA, State Employees' Credit Union, and Ally Financial are a few of the banks, credit card issuers, and lenders that have agreed to participate in the provision of free credit scores so that consumers can more easily tell if they have been a victim of financial fraud. The third component laid out by the President in his plan is to introduce through legislation a Consumer Privacy Bill of Rights, which would outline baseline protections for consumers. The President hopes to introduce this legislation by the end of February. Finally, the President has proposed a Student Digital Privacy Act that would make it illegal to sell students' personal information and would limit the use of such personal information to the academic purposes for which it was collected.

Following up on his plan to protect consumers' privacy, the President announced on January 13 additional cybersecurity steps to be taken to combat cyberthreats at home and abroad. The President proposed legislation that would enable cybersecurity information-sharing in the private sector and between the private sector and the government. Another stated aim of President's proposal is to modernize law enforcement authorities in order to combat cybercrime and to provide law enforcement with additional tools to address cybercrime, such as allowing for the prosecution of the sale of botnets. In addition, the President is again pushing a proposal for a national security breach reporting system. Finally, $25 million in grants would be provided over the next five years to fill a growing demand for trained professionals to obtain education in the cybersecurity field.

The administration proposals led up to last week's State of the Union address that featured cybersecurity and privacy as two prominent issues. Particularly notable was the focus not just on personally identifiable information (PII) but on other information subject to cyberattack. Many commentators and government officials have urged that, in addition to PII, trade secrets and other intellectual property should also be better protected. The President stated, "[n]o foreign nation, no hacker, should be able to shut down our networks [or] steal our trade secrets."

For cybersecurity and privacy issues, as with many other issues, the "devil is in the details." Many aspects of cybersecurity and privacy implicate the interests and concerns of a wide variety of stakeholders. Often, what seems to be a good idea on the surface may turn out to be problematic once the relevant parties attempt to work through the details. As just one example, anyone who has been involved in a data breach understands that investigations of cyber incidents take time and that early release of potentially incorrect information can be problematic. Consequently, some critics of the anticipated breach notification law have argued that thirty days may not be enough time to give notification of a breach in all cases.

To facilitate the President's consumer protection and cybersecurity initiatives, the White House plans on holding a Summit on Cybersecurity and Consumer Protection at Stanford University on February 13, 2015. This will bring together stakeholders from the private and public sector to discuss these complex issues.

Having cybersecurity take "center stage" may mean, at a minimum, that a robust national dialog on the issue will occur. It may also result in overarching national legislation. But, again, the devil is in the details. Stay tuned to see how any such legislation may affect you. Our Privacy & Data Protection practice continues to track these and related legislative developments and can provide you with additional information or insights, tailored to your or your company's needs.

# Key Contacts



| | |
|---|---|
| **Matthew D. Brown**<br>**San Francisco** | **brownmd@cooley.com**<br>**+1 415 693 2188** |
| Adam Ruttenberg<br>Washington, DC | aruttenberg@cooley.com<br>+1 202 842 7804 |
| Randy Sabett<br>Washington, DC | rsabett@cooley.com<br>+1 202 728 7090 |
| Vince Sampson<br>Washington, DC | vsampson@cooley.com<br>+1 202 728 7140 |