President Obama Announces New Federal Data Breach, Student Privacy and Consumer Privacy Legislative Initiatives

On Monday January 12, President Barack Obama announced several new proposals aimed at protecting consumer and student data in the digital age. The proposals will center on three pieces of proposed legislation, addressing corporate responsibilities when data breaches occur, the protection of student information, and consumer control of personal information.

The Personal Data Notification and Protection Act (PDNPA) that the President announced he will be putting forward, for instance, is intended to create a national standard for companies and others to follow in notifying consumers about breaches or losses of their data. Currently, 47 states, plus the District of Columbia, Puerto Rico, the Virgin Islands, and Guam each have their own, sometimes disparate, laws that define how and when corporations are to notify consumers when their personal information may have been accessed or acquired without authorization. In certain cases, a single breach can trigger the notification laws in some states but not others, often leaving corporations to decipher which conflicting requirements may apply to the situation at hand. As President Obama stated, "Right now almost every state has a different law on this and it's confusing for consumers and it's confusing for companies – and it's costly too, to have to comply with this patchwork of laws."

The proposed legislation would set a single national standard for data breaches and, according to the White House, "strengthen[] the obligations companies have to notify customers when their personal information has been exposed." The proposal will call for a 30-day time limit for corporations to notify consumers of a breach. While many corporations have voiced support for a national standard, some question whether the 30-day notification requirement is too short. Currently, those states that impose time limits – whether by statute or administratively – are limited, which provides companies some flexibility in timing to understand the extent of a breach, work with law enforcement, accurately determine the consumers who must be notified, and restore the integrity and security of affected data systems.

The proposed language of the PDNPA has not yet been released, raising other questions about the proposal. This includes whether it will expand the kinds of data breaches or the categories of data to which notice obligations attach; whether a company will be required to notify consumers any time an actual breach occurs or only when an actual breach presents a reasonable likelihood, or some lesser showing, of data misuse or harm to the consumer; and whether the proposed statute will be enforced administratively or through the courts, with possible class action litigation.

In addition to the PDNPA, the President is proposing a Student Data Privacy Act, which would offer significant protections for student data collected in schools. With the predicted rise in the use of Internet-connected and other digital educational technology, there are increasing opportunities for the collection of student data by third-party technology firms. The proposed legislation would place restrictions on the use of student data by such firms. For example, the bill would likely prohibit these companies from either selling the data or advertising to the students based upon the data. This bill is modeled after a recently enacted California law, the Student Online Personal Information Protection Act, which was intended to address similar concerns.

One critical question with each of these bills is whether the President's proposed legislation would preempt the current state laws on these issues. For example, while the PDNPA would almost certainly set a national minimum standard for corporations to follow in response to data breaches, it remains an open question whether states would be free to adopt more stringent requirements for breaches involving their corporations or their residents.

Last, the President announced that a revised legislative proposal for the Consumer Privacy Bill of Rights would be released in 45 days. The Consumer Privacy Bill of Rights was originally proposed in 2012 and would give consumers greater control over what types of personal information may be collected by companies and how those companies can use that data.

The President also announced on Monday that his Administration has obtained voluntary commitments from corporations in the financial, energy, and educational sectors that are designed to protect consumer data. For example, Bank of America and J.P. Morgan Chase have agreed to provide customers with free access to their credit scores – a move that is designed to help consumers more quickly identify possible identity theft. Several large companies active in education technology, including Microsoft and Apple, have pledged to use student data only for authorized purposes.

These announcements follow the passage of several major federal cybersecurity bills at the end of 2014. Those bills mostly focused on increasing national cybersecurity by providing the Department of Homeland Security and Border Patrol with additional tools to protect against cyberattacks.

The President intends to continue to highlight these issues as he further addresses cybersecurity and data privacy issues in his upcoming State of the Union address.

These initiatives are not surprising given the significant number of high profile consumer data breaches that have occurred in recent years and the current patchwork of different state approaches to data regulation. These and other cybereffortsCongress is likely to take up this year may have a significant impact on a wide range of industries, essentially encompassing all companies that touch the collection, processing, storage or use of consumer data. For further information about how these proposals may impact your interests, please contact a member of Ropes & Gray's leading Privacy & Data Security team or your regular Ropes & Gray contact.