President Obama Announces New Privacy and Consumer Protection Initiatives, Highlights Student Privacy

By Mary Ellen Callahan and Heidi Wachs

President Obama announced a package of new privacy and consumer protection initiatives, including three legislative proposals, to enhance student and consumer data privacy at a visit to the Federal Trade Commission. The President discussed the combination of legislation, government and private sector resources designed as a comprehensive approach to address issues of data privacy, data security, identity theft, and education privacy. He also plans to highlight these efforts during the upcoming State of the Union address.

Educational privacy, a subset of data privacy that members of the Privacy and Information Practice have emphasized before, is gaining momentum and attention. After a year with some state-level legislative activity on education privacy, including the passage of a comprehensive student data privacy law in California, President Obama raised the issue to the national stage. The impact of this proposed legislation and attention to student privacy will directly affect not only education institutions and school districts, but also the many private sector companies and organizations whose businesses involve the use of student data.

The three pieces of legislation the President is going to propose are:

**The Student Digital Privacy Act:** This legislation applies specifically to companies and organizations that collect student data. The law will place restrictions on the sale of student data and the use of student data to engage in targeted advertising. However, the law will also contain provisions designed to support the use of student data for research that improves teaching and learning initiatives and products.

**The Personal Data Notification & Protection Act:** The subject of much debate for years, this legislation would create a federal data breach notification law. If passed, the law will establish baseline requirements for when and how companies must notify customers when their personal information has been inappropriately accessed or disclosed. Companies will be required to provide notification within 30 days of discovering the breach.

**Consumer Privacy Bill of Rights Legislation:** In 2012, the Administration introduced the conceptual Consumer Privacy Bill of Rights in an effort to establish guidelines around the use and collection of personal information and the rights of individuals with regards to their personal data. Based on the Fair Information Practice Principles (FIPPs), the new legislation would codify the Consumer Privacy Bill of Rights.

**Action Items and Considerations**

Although the timeline, final content and enactment of these pieces of legislation are uncertain, there are actions clients should consider taking:
- **Conduct a Data Inventory.** Companies, institutions and organizations should have at least a high-level understanding of all personal information being used and collected. There should be frequently updated documentation on where the personal information is stored throughout the enterprise.

- **Create, or review, the breach response and notification plan.** Every organization that collects personal information should have a data breach response and notification plan. Most organizations collect personal information, at a minimum, on their employees. The response plan should include a timeline of anticipated activities such as notifying affected individuals and appropriate authorities, contracting with call centers, and engaging in crisis management as appropriate. Clients with existing plans should review them to ensure that they support compliance with the new legislation's 30-day notification window.

- **Review data collection, handling, and sharing practices.** The Consumer Privacy Bill of Rights will require companies to be much more transparent about their data use and processes than they may be currently. Organizations should be prepared to provide clear and concise notice to those whose data is being collected about its exact purpose and use. In addition, companies will have to be transparent with customers about how and when their data is being used for marketing purposes or shared with third parties. This is especially true with any company or organization handling student data.

- **Review existing programmatic and technical controls.** Both the Consumer Privacy Bill of Rights and the FIPPs establish baseline security requirements, in addition to the FTC’s enforcement actions on data security. Good cybersecurity isn’t achieved with firewalls or anti-virus software alone. Comprehensive data privacy and cybersecurity requires a program that integrates information governance, such as information classification, with technical controls, such as access controls or data loss prevention. Companies should conduct privacy and cybersecurity audits and reviews to assess the current state of their protection of personal information and identify the programmatic and technical controls required to mitigate information-related risk.

---

### Contact Us

**Mary Ellen Callahan, Partner, Jenner & Block**  
Phone: 202.639.6064  
Email: mecallahan@jenner.com  
Download V-Card  
Practices: Content, Media & Entertainment; Litigation; Privacy and Information Governance

**Heidi Wachs, Special Counsel, Jenner & Block**  
Phone: 202.639.6081  
Email: hwachs@jenner.com  
Download V-Card  
Practices: Litigation; Privacy and Information Governance