U.S. President Obama Announces Renewed Focus on Securing Cyberspace and Protecting Consumer Privacy

By Alexander H. Southwell, Eric D. Vandevelde, Ryan T. Bergsieker, Stephenie Gosnell Handler and Adam Chen, of Gibson, Dunn & Crutcher LLP.

In the days leading up to the State of the Union address scheduled for January 20, 2015, President Obama outlined several significant cybersecurity and data privacy initiatives. This renewed focus on cybersecurity comes in the wake of a number of prominent cyber attacks on U.S. companies in recent months that have captured national and international attention, and includes both proposed legislation and executive actions. Several of the initiatives seek to protect American consumers from cyber threats while ensuring privacy and civil liberties. They mark an evolution in the Administration’s approach to cybersecurity and come after years of stalled efforts to pass cybersecurity legislation. Their unveiling establishes cybersecurity and data privacy as focal points of the president’s upcoming State of the Union address and reinvigorated priorities for the Administration.

While politics will shape the final version of these proposals, this article examines, from a legal perspective, the initiatives as an outline of the Administration’s goals in cybersecurity and data privacy.

Proposed Cybersecurity Legislation
President Obama officially announced proposed cybersecurity legislation in a speech on January 13, 2015, at the Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC). The legislation proposal creates primarily of cybersecurity information sharing and law enforcement tools.

Cybersecurity Information Sharing
The proposed legislation would promote enhanced cybersecurity information sharing between the private sector and the government, and seek to increase collaboration and information sharing in the private sector.

News and analysis of data protection developments around the world. For the latest updates, visit www.bna.com

International Information for International Business

WORLD DATA PROTECTION REPORT

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., U.S.A.

VOLUME 15, NUMBER 1 >>> JANUARY 2015
The proposed legislation is intended to reinforce and strengthen existing relationships between the federal government and the private sector. It also would encourage the development of additional private sector-led information sharing and analysis organizations, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The Department of Homeland Security, in consultation with the Department of Justice, the Department of State, and the Federal Trade Commission, would be responsible for developing such guidelines. The Privacy and Civil Liberties Oversight Board, which was created by the USA PATRIOT Act, would be responsible for reviewing the guidelines to ensure they are consistent with constitutional, statutory, and legal requirements. The board also would be responsible for ensuring the guidelines are consistent with the national security, foreign policy, and law enforcement needs of the federal government.

The proposed legislation also would require companies to provide notice to consumers when their personal information has been compromised in a data breach. The notice would be required to be posted on the company’s website and would include information about the nature and scope of the breach, the steps that the company is taking to address the breach, and the steps that consumers can take to protect their information. The proposed legislation also would require companies to provide consumers with a toll-free phone number and a website to assist them in reporting identity theft.

Further, the proposed legislation would require companies to provide a description of the steps that are being taken to address the breach, including the steps that are being taken to prevent similar breaches in the future. The proposed legislation also would require companies to provide consumers with the name and contact information of a compliance officer who can be reached to discuss the breach.

The proposed legislation also would require companies to implement robust security measures to protect the personal information of consumers. The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers.

The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers. The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers.

The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers. The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers.

The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers. The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers.

The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers. The proposed legislation also would require companies to provide consumers with a description of the steps that are being taken to protect the personal information of consumers.
the initiative are already at the forefront of legislative action. The Consumer Privacy Bill of Rights (CPBR), previously proposed in 2012, is revitalized by the recently announced White House initiatives. The CPBR seeks to set clear principles regarding the use of such data, as well as enforce legal frameworks to ensure that companies are held accountable for their data protection practices. The CPBR is intended to bring together stakeholders from the federal government, the private sector, and consumer advocates to develop comprehensive laws and regulations that facilitate these goals and build upon its previous efforts.

The president also announced that the Department of Energy and the Federal Smart Grid Task Force have released a new Voluntary Code of Conduct for utilities and data, including customer energy usage. The code aims to bolster the nation’s abilities to deter, respond to, and recover from cyber attacks. The magnitude of recent cyber attacks on American businesses has heightened the executive branch’s sense of urgency around developing comprehensive measures to protect the nation’s critical infrastructure and ensure national security.

Conclusion

The magnitude of recent cyber attacks on American businesses has heightened the executive branch’s sense of urgency around developing comprehensive measures to protect the nation’s critical infrastructure and ensure national security. The recent announcements indicate that the Administration is likely to continue leading cybersecurity efforts by leveraging new initiatives and collaborations with key stakeholders. The text of the White House’s January 13, 2015, statement on “Cybersecurity Communications Integration Center” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The text of the White House’s January 12, 2015, fact sheet “Safeguarding American Consumers & Families” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families. The text of President Obama’s January 13, 2015, speech at the National Conference on Cybersecurity and Consumer Protection can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The new CPBR will attempt to set clear principles regarding protecting electricity customer data, and data protection.

Smart Grid Customer Data Privacy

In addition to these pieces of proposed legislation, the Administration announced that the Department of Energy and the Federal Smart Grid Task Force have released a new Voluntary Code of Conduct for utilities and data, including customer energy usage. The code aims to bolster the nation’s abilities to deter, respond to, and recover from cyber attacks. The magnitude of recent cyber attacks on American businesses has heightened the executive branch’s sense of urgency around developing comprehensive measures to protect the nation’s critical infrastructure and ensure national security. The recent announcements indicate that the Administration is likely to continue leading cybersecurity efforts by leveraging new initiatives and collaborations with key stakeholders. The text of the White House’s January 13, 2015, statement on “Cybersecurity Communications Integration Center” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The text of the White House’s January 12, 2015, fact sheet “Safeguarding American Consumers & Families” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families. The text of President Obama’s January 13, 2015, speech at the National Conference on Cybersecurity and Consumer Protection can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The new CPBR will attempt to set clear principles regarding protecting electricity customer data, and data protection.

Smart Grid Customer Data Privacy

In addition to these pieces of proposed legislation, the Administration announced that the Department of Energy and the Federal Smart Grid Task Force have released a new Voluntary Code of Conduct for utilities and data, including customer energy usage. The code aims to bolster the nation’s abilities to deter, respond to, and recover from cyber attacks. The magnitude of recent cyber attacks on American businesses has heightened the executive branch’s sense of urgency around developing comprehensive measures to protect the nation’s critical infrastructure and ensure national security. The recent announcements indicate that the Administration is likely to continue leading cybersecurity efforts by leveraging new initiatives and collaborations with key stakeholders. The text of the White House’s January 13, 2015, statement on “Cybersecurity Communications Integration Center” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The text of the White House’s January 12, 2015, fact sheet “Safeguarding American Consumers & Families” can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families. The text of President Obama’s January 13, 2015, speech at the National Conference on Cybersecurity and Consumer Protection can be accessed at http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-creation-cybersecurity-communications-integration-center. The new CPBR will attempt to set clear principles regarding protecting electricity customer data, and data protection.