CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

Privacy and the White House Cyberspace Policy Review

Privacy and the White House Cyberspace Policy Review

Shortly after entering office, President Obama directed a comprehensive "clean-slate" review to assess the United States' policies and structures for cybersecurity. The result was the *Cyberspace Policy Review* ("*Review*") [1]. The *Review* discussed the myriad issues facing the United States in cyberspace in terms of national security, economic interests and civil liberties. Since the release of the *Review*, some in and out of government have called into question the government's ability to protect the nation, the open Internet and privacy simultaneously. CDT strongly believes that all three goals are essential to keep the Internet open, innovative and free.

In particular, CDT plans to track efforts to ensure privacy rights are included in any discussion of a national policy vis-à-vis cybersecurity.

In discussing privacy rights, the *Review* relies on three broad themes. First, privacy is a value to promote. Citing the substantial concerns raised by privacy rights groups, the *Review* notes that all future strategic planning must include protections for individual privacy else much of the substantial benefit derived from advances in information technology will be lost. Second, privacy rights must be clearly enumerated. Absent a clear legal framework, privacy rights are extremely vulnerable to advances in technology. Thus, clear policies that detail privacy rights are necessary. Third, any plan to protect privacy rights requires melding both technology and policy. Without a coordinated effort to develop polices that incorporate advancements into technology, loss of privacy could become an unintended consequence.

Extracted from the *Review* and the *President's Remarks on the Review* [2], the Action Items that develop from these themes are offered to supplement the Review's broader Near and Mid-Term Action Plan ("Plan") for the incoming cybersecurity policy official.

[1] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[2] http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Action Items to Enhance Privacy from the Cyberspace Policy Review

1) Create a National Dialogue on Cybersecurity and commitment to privacy and civil liberties guaranteed by constitution

“The United States needs to conduct a national dialogue on cybersecurity to develop more public awareness of the threat and risks and to ensure an integrated approach toward the Nation’s need for security and the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law.” (p. i)

2) Ensure That Federal Government Will Not Monitor Private Networks in Pursuit of Cybersecurity.

“Let me also be clear about what we will not do. Our pursuit of cybersecurity will not -- I repeat, will not include -- monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be -- open and free.” (Presidential Remarks)

3) Hire a Privacy Officer at NSC (and/or EOP)

“Designate a privacy and civil liberties official to the NSC cybersecurity directorate.” (p.vi)

“Other options include: facilitating regular engagement of government civil liberties and privacy advisors on policy matters for cybersecurity or designating a dedicated privacy and civil liberties officer within the NSC (or, more broadly, the EOP) to engage with the private-sector civil liberties and privacy community, an oversight board, and government civil liberties and privacy officers.” (p. 9)

“To ensure that policies keep faith with our fundamental values, this office will also include an official with a portfolio specifically dedicated to safeguarding the privacy and civil liberties of the American people.” (Presidential Remarks)

4a) Draft a policy strategy for privacy in authentication technologies.
4b) Encourage privacy enhancing technologies for authentication

“Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.” (p. vi)

“The Federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies.” (p. 33)

"Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy." (p. 38)

5) Reconstitute the Privacy and Civil Liberties Oversight Board

"It is important to reconstitute the Privacy and Civil Liberties Oversight Board (PCLOB), accelerate the selection process for its board members, and consider whether to seek legislative amendments to broaden its scope to include cybersecurity-related issues." (P. 9)

6) Build engagement mechanisms for civil liberties and privacy advisors on cybersecurity

"Other options include: facilitating regular engagement of government civil liberties and privacy advisors on policy matters for cybersecurity or designating a dedicated privacy and civil liberties officer within the NSC (or, more broadly, the EOP) to engage with the private-sector civil liberties and privacy community, an oversight board, and government civil liberties and privacy officers." (p. 9)

7) Develop incident response sharing mechanisms that protect privacy

"The ICI-IPC should develop clear, enforceable rules for timely reporting of incidents by departments and agencies to enable an effective and efficient interagency response. Departments and agencies are uneven in their incident reporting outside their own boundaries. The overall federal response would benefit from immediate reporting of significant events across a wider range of departments and agencies having incident response roles." (p. 24)

8) Ensure intrusion detection policy and mechanisms protect privacy

"The Federal government should improve its ability to provide strategic warning of cyber intrusions and attacks to the President. The Federal government should continue to leverage the Nation's long-term investments in the fundamental development of cryptologic and information assurance technologies and the necessary supporting infrastructure. . . . Any new authorities would need to be consistent with the protection of civil liberties and privacy rights." (p. 25)

9) Define privacy objectives for future infrastructures

"The movement of data across jurisdictional boundaries presents challenges for law enforcement, the protection of privacy and civil liberties as defined by different countries, and liability decisions in he event of data or network breaches." (p. 33)

"[W]e will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that's why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives." (Presidential Remarks)

10) Establish global policy standards to protect privacy rights and civil rights.

"Work with international partners to develop policies that encourage the development of a global, trusted eco-system that protects privacy rights and civil liberties and govern appropriate use of law enforcement activities to protect citizens and infrastructures." (p. 34)

11) Ensure privacy protection in information sharing regimes.

"Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and mutual arrangements that will improve economic and security interests while protecting civil liberties and privacy rights." (p. 38)

12) Develop international standards to protect privacy of data used in cloud computing.

"The movement of data and services to third-party network-based servers, referred to as the "cloud," introduces new policy challenges for the private sector and governments around the globe. The movement of data across jurisdictional boundaries presents challenges for law enforcement, the protection of privacy and civil liberties as defined by different countries, and liability decisions in the event of data or network breaches." (p. 32)