August 20, 2013

The Honorable Denis McDonough
Chief of Staff
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

The Honorable Kathryn Ruemmler
Counsel
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear Mr. McDonough and Ms. Ruemmler:

The undersigned organizations represent numerous sectors within the technology industry. Our industry is continuously developing and delivering innovative products and services that improve the lives of people around the world in many ways. New products and services, fueled by the Internet, serve as vehicles for social, cultural, political, and economic empowerment and transformation.

We appreciate the opportunity to participate in the discussions surrounding privacy and civil liberties that the Administration has convened regarding the scope and operation of the U.S. government's surveillance programs. Discussions about national security must be kept separate from conversations about commercial privacy issues, as the policy considerations in these two areas are distinct.

As a follow up to the meeting at the White House on August 6, 2013, we offer the following recommendations to the Administration and Congress. These are the most critical recommendations, which would address important privacy and civil liberties concerns while also fostering technology innovation and economic growth. We look forward to continued discussions with the Administration on the following issues.

Recommendations

1. Implement appropriate transparency with respect to national security programs;

2. Support reforms to the Electronic Communications Privacy Act that would enhance privacy in law enforcement investigations; and,

3. Promote policies that allow for unimpeded cross-border data flows such as the U.S.-EU Safe Harbor Framework.

We discuss each of the above recommendations in detail below.

Implement appropriate transparency with respect to national security programs

Just as the Administration has observed significant consequences to the government's national security efforts from the recent disclosures, the technology sector is facing significant repercussions. One study estimates that the U.S. cloud computing industry alone could lose up to $35 billion during the next three years.[1]

To have a deliberate policy discussion it is important that we separate fact from fiction. President Obama's August 9, 2013, announcement that he has directed the intelligence community to make public as much information about these programs as possible is a necessary first step. The NSA memo released that same day, "The National Security Agency: Missions, Authorities, Oversight and Partnerships," was also a necessary step.

We are encouraged that a website will be created to serve as a hub for further transparency. We urge that the information shared publicly through this website will include assurances that the information collected by the government is properly secured. Further, the website should also detail the scope of the government's access to information; the means by which this information is obtained; the level of oversight in connection with the mechanisms determining access; and transparency into the government access orders that are made to commercial entities.

In this regard, we also encourage the government to revisit limitations on what private companies can disclose about the orders they receive, recognizing that a lack of transparency on this subject may lead consumers to overestimate the scope of these intelligence programs and, thereby, undermine public trust in both industry and the government's efforts. In particular, companies should be allowed to report the number of orders they receive pursuant to U.S. national security or intelligence gathering and surveillance programs, and the number of users or accounts that are the subject of the orders. Further, we recommend that the government disclose similar information relating to the orders.

Implementing such steps to increase transparency can assist in reestablishing trust, both domestically and globally. Measures taken to be more transparent with respect to government information collection, now and in the future, should be pursued globally.

---

[1] Castro, Daniel, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?" The Information Technology & Innovation Foundation, August 2013. http://www2.itif.org/2013-cloud-computing-costs.pdf

The additional action items that President Obama announced may further the goal of increasing public trust in the government's national security and intelligence programs. We are eager to review any recommendations as to how Section 215 of the Patriot Act can be improved. We also are eager to see how giving a greater voice to civil liberty concerns will be implemented in the Foreign Intelligence Surveillance Court.

We urge the Administration to provide the newly established Review Group on Intelligence and Communications Technologies the necessary tools to conduct a thorough and balanced review. This Review Group is being tasked with assessing, among other things, whether the U.S. government's technological information collection capabilities appropriately account for policy considerations such as unauthorized disclosure and the need to maintain public trust. We look forward to the preliminary report from this Review Group within 60 days, along with the final report by the end of 2013. We hope that the Administration will take full advantage of the insights that industry can provide as it develops these reports, as well as industry's expertise in connection with any planned reforms.

Support reforms to the Electronic Communications Privacy Act that would enhance privacy in law enforcement investigations

We urge the Administration to support updating the Electronic Communications Privacy Act (ECPA). ECPA was a forward-looking statute when Congress enacted it in 1986. It specified standards for law enforcement access to electronic communications and associated data, affording important privacy protections to subscribers of emerging wireless and Internet technologies. Technology, however, has advanced dramatically since 1986, and ECPA has not kept pace with this innovation. The statute has not undergone a significant revision since it was enacted in 1986. The standards in the law are outdated and are not interpreted consistently. These standards need to be simplified and provide clearer privacy protections for users.

Bipartisan legislation, sponsored by Senators Leahy and Lee, would update ECPA and generally, would require law enforcement to obtain a warrant for the content of all stored electronic communications.[2] We urge the Obama Administration to support efforts to pass a clean ECPA bill and oppose efforts to include carve outs to the warrant requirement, which would weaken the privacy protections the bill seeks to establish.

Promote policies that allow for unimpeded cross-border data flows such as the U.S.-EU Safe Harbor Framework

One of the most negative consequences of the recent disclosures would be if it were to result in increased barriers to global cross-border data flows. The free flow of data is critical to the continued growth of our global economy, and such free flow is recognized as one of the most important principles of international trade.

We are already seeing longstanding and effective cross-border data mechanisms being questioned in light of the recent disclosures about the U.S. government surveillance programs. Officials in the EU are now questioning whether they can "trust" the U.S.-EU Safe Harbor

[2] S.607, available at http://www.gpo.gov/fdsys/pkg/BILLS-113s607rs/pdf/BILLS-113s607rs.pdf.

framework, which allows for the transfer of information from the EU to the U.S. for participating companies.[3] Many U.S. companies rely on this mechanism to lawfully transfer data from the EU to the U.S. and its continued operation is a top priority for the technology sector.

Recent statements by government officials in the EU indicate that the Safe Harbor may be in jeopardy, and we urge the Administration to engage with EU officials to ensure that the Safe Harbor continues to be a viable mechanism for cross-border data flows from the EU to the U.S.

Also, the facilitation of cross-border data flows is a critical element in two important trade agreements currently being negotiated -- the Trans-Pacific Partnership and the Trans-Atlantic Trade and Investment Partnership.

We applaud the USTR for recognizing that the maintenance and expansion of cross-border data flows is a vital component of the trade discussions around the world, and we urge the Administration to continue to engage with foreign officials to ensure that cross-border data flows continue to facilitate economic growth and opportunity.

A number of multilateral fora in which the U.S. government participates may be appropriate venues to engage with the international community on preserving cross-border data flows while addressing privacy and civil liberties concerns. Both the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) forum have long recognized the importance of cross-border data flows and have facilitated initiatives to find common ground among different privacy regimes.

We encourage the U.S. government to identify opportunities to build on the work of these fora to foster interoperability between privacy regimes. In addition, these fora could provide appropriate venues for work on increased transparency globally for government collection of data.

Again, thank you for the opportunity to participate in these important discussions and we look forward to continuing to engage with you on these issues.

Sincerely,

BSA | The Software Alliance
Computer & Communications Industry Association (CCIA)
Information Technology Industry Council (ITI)
The Internet Association
SIIA – Software & Information Industry Association
TechNet

cc: Members of Congress

[3] See July 19, 2013 statement, of Viviane Reding, European Commission Vice President, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm; and July 24, 2013, statement of the Conference of German Data Protection Commissioners, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.