Information Technology Industry Council

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

The Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Testimony of
Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

March 19, 2014

Privacy and Civil Liberties Oversight Board Public Hearing

Testimony of ITI's Dean C. Garfield

March 19, 2014

I am Dean Garfield, president and CEO of the Information Technology Industry Council, or ITI, a U.S.-based global trade association representing more than 50 of the world's most dynamic and innovative companies in the information and communications technology (ICT) sector.

I appreciate the opportunity to appear before the Privacy and Civil Liberties Oversight Board (PCLOB) today and thank you for inviting me.

PCLOB, as an independent government agency charged with ensuring that the privacy and civil liberties of individuals are protected, is in a unique position to be a driving force in effectuating change to the surveillance framework in this country.

Business Impact

The ongoing revelations about data collection by the National Security Agency (NSA) are having a significant economic impact on the technology sector. In addition to addressing the economic impact in my comments today, I will also discuss the potential long-term implications for innovation and Internet governance on the global economy. Finally, I will offer up some thoughts on solutions.

The United States has been a leader in nearly every part of the technology sector. Public and government responses around the world to the NSA disclosures put this leadership at risk. The erosion of the public's trust and protectionist regulatory proposals from foreign governments are alarming developments.

While we can talk about specific programs and authorities such as Section 215 or Section 702, it is the totality of the revelations that have brought us to where we are today—an environment where U.S. technology companies are facing uphill battles to keep or secure business in overseas markets.

"Made in America" is no longer viewed as positive for customers of U.S. online services. Many ITI member companies are experiencing increased levels of concern about government access to data, specifically access by the U.S. government. Other governments, of course, engage in online surveillance, but the impression being fueled globally in response to the NSA disclosures is that the U.S. government is the source of the problem, with U.S. companies seen as either aiding government surveillance, or particularly vulnerable to it.

The potential losses are tangible, demonstrable, and widespread. In the short term, the resulting commercial losses will likely reach the tens of billions of dollars. One study from the Information Technology & Innovation Foundation anticipates the revelations could result in as much as a $35 billion loss to the U.S. cloud computing industry over the course of three years. Other studies, including by Forrester, suggest the losses could be even higher over a longer period of time.

Broader Implications

The potential adverse economic impact here in the U.S. could be even more significant and lasting if other governments enact legislation to force localized data storage and production of technology. Such forced localization measures would also disrupt the current Internet governance model that to date has ignited and sustained the incredible success of the Internet as a global platform for innovation and economic productivity.

These problematic policy proposals are spreading across the globe and are putting the open Internet of today at risk. We are facing the possibility of a Balkanized Internet, and global innovation will certainly suffer. Brazil, for example, is considering a legislative proposal that could lead to the requirement that certain data be stored in that country. Brazil has also taken steps aimed at ensuring that all government communications, including email, are managed by local companies.

The revelations have also received significant attention in the European Union (EU). One of the most critical data transfer mechanisms that many U.S. companies in numerous sectors rely on to transfer data from the EU to our nation is in jeopardy. Government officials in the EU are now questioning whether the U.S.-EU Safe Harbor Framework should continue to operate. Similarly, a number of European nations are proposing to establish country-specific clouds.

These types of proposals and requirements would be highly disruptive to business operations. They risk creating network architecture inefficiencies that would hinder the performance of ICT services. They also have the potential to Balkanize open platforms, including the Internet, that are key to continued transformative innovations and global commerce.

Solutions

The U.S. government must take the lead to repair the erosion of public trust and the acceleration of forced localization and other onerous policies that would Balkanize the Internet and other open platforms. Economic and commercial interests must be part of the discussion around government surveillance, coequal to the factors governments globally now in the information age need to consider, including individual privacy, economic prosperity, and national security.

While reforms are being considered here in the United States, we also urge the administration to actively engage on this issue globally, and at the highest levels.

International government-to-government dialogue is critical to prevent harmful policies that will impact our economy.

ITI has worked with its member companies to arrive at several consensus recommendations about how to reform our surveillance programs to consider both the national security needs of our nation as we know them, with the dire need to restore confidence in the "Made in America" brand. While our recommendations are not unique to Section 702, our proposals can be applied across the board to a range of intelligence programs.

The recommendations I outline below largely derive from a set of seven global principles that ITI has developed with the Software & Information Industry Association (SIIA). We believe these principles should guide government surveillance policies around the world. Among other imperatives, these principles highlight the need for greater transparency and oversight in connection with how intelligence-gathering programs operate. I also ask that our seven global principles be submitted for the record along with my testimony. Our recommendations, as well as the principles, are guided by a recognition that we don't know what we don't know on national security, and by a realization that privacy and security do not sit on opposite ends of a spectrum. It is possible to advance both.

Transparency

As recognized in the January 2014 PCLOB report, "transparency is one of the foundations of democratic governance." In furtherance of this ideal, companies that make up the technology sector are committed to informing their users and the public about requests received from governments around the world for law enforcement and intelligence purposes. Companies should be able to provide more information about such orders. The administration's recent decision to allow companies to disclose certain information is certainly a step forward. Greater transparency, however, should be permitted and legislation enabling such disclosures is desirable. Specifically, companies should be permitted to disclose the number of government orders for information made under specific legal authorities, including, but not

limited to, separate disclosures for Section 215 of the USA Patriot Act, Section 702 of the FISA Amendments Act, and various National Security Letter statutes. Also, companies should be permitted to disclose the number of individuals or accounts, including accounts of business customers, impacted by the orders received as well as the type of information that is sought by such orders.

In addition, as appropriate, the U.S. government should supplement the annual reporting that is already required by law with information similar to what companies should be permitted to disclose: the total number of orders under specific authorities for specific types of data, and the number of individuals or accounts affected by each. Basic information about how the government uses its various law enforcement related investigative authorities has been published for years without any apparent disruption to criminal investigations. Further, the provision of such data to the public on a time-delayed basis and in aggregate form should not compromise any ongoing investigation.

An additional transparency measure we would recommend relates to the legal decisions of the Foreign Intelligence Surveillance Court (FISC). The legal decisions of the FISC are not routinely disclosed to the public. These decisions, however, involve constitutional questions and interpretations of legal authorities pursuant to which the U.S. conducts its surveillance activities. These decisions should be released publicly, as appropriate, to enable an informed public discourse about the court's rulings, and to better guide future congressional oversight and policymaking. This type of transparency can also yield greater public trust in the government's surveillance programs, their oversight, and the process utilized by the government to gain access to user data.

Oversight

FISC proceedings operate in a non-public forum and the U.S. government is the sole party appearing before the judges. An additional party should be appointed or consulted in appropriate cases to assist the FISC in evaluating the issues at hand. Additional parties would be an advocate for the privacy and civil liberty considerations implicated in court proceedings.

Rebuilding Trust: Cryptography

Steps should be taken, using a transparent, public process, to restore public trust in the central role that the National Institute of Standards and Technology (NIST) plays in developing standards and guidelines to protect federal information and information systems, and industry at large.

Recent news reports describe in general terms the efforts of the NSA to defeat cryptographic protections for surveillance purposes. The reports suggest this effort went beyond the use of specially designed high-speed computers to crack encryption codes and involved the NSA in an attempt to introduce weaknesses into the encryption standards followed by hardware and software developers worldwide.

For nearly 20 years, the technology and user communities have welcomed the involvement of the NSA, as one of many stakeholders, in the work of developing cryptographic standards because it brings one of the most knowledgeable and experienced code-writing institutions to the vital task of protecting information from unauthorized access. The public, the technology sector, and the government all have an interest in the creation and widespread use of the strongest possible cryptographic standards. Regardless of the accuracy of these reports, the mere suggestion that the NSA has used its participation in the cryptography development process to introduce weaknesses into cryptographic standards has created a crisis of trust in the technology community. Some security firms have issued advisories to their customers to avoid using algorithms that might contain weaknesses.

We further appreciate NIST's history of extensive collaboration with the world's cryptography experts to support robust encryption. NIST has reopened public comment on some specific standards and stated clearly: "If vulnerabilities are found in these or any other NIST standards, we will work with the cryptographic community to address them as

quickly as possible." This initiative is an important step toward regaining trust in NIST's commitment to strong, robust, cryptographic, and other standards that have been vetted by experts globally.

The facts alleged in the news accounts should be investigated and the separate roles played by NIST and the NSA in cryptographic standards should be reaffirmed.

Rebuilding Trust: Collection

In addition to the transparency and other measures outlined above that are designed to increase public trust, with regard to specific statutory authorities and the collection programs currently in operation, I urge that the public be assured that such collection is not indiscriminate. If reforms are necessary to ensure that such collection is not indiscriminate, they should be implemented. Avoiding indiscriminate collection is critical to public trust and to ensure an open Internet where individuals can take advantage of all that technology has to offer.

Conclusion

We need to restore "Made in America" as positive. It is imperative that the necessary steps be taken by Congress and the Administration to restore trust in the innovative products and services that ITI member companies provide, and to maintain the open and borderless Internet that has served to the benefit of so many individuals, companies, and countries around the world.

Thank you for this opportunity to appear before you today. I will be happy to answer any questions you may have.