Information Technology Industry Council

"Examining Recommendations to Reform FISA Authorities"

Testimony of

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

Before the

U.S. House of Representatives
Judiciary Committee

February 4, 2014

"Examining Recomendations to Reform FISA Authorities"
Testimony of ITI's Dean C. Garfield
House Judiciary Committee
February 4, 2014

Mr. Chairman, Ranking Member Conyers, and members of the Committee, I am Dean Garfield, president and CEO of the Information Technology Industry Council, or ITI, a U.S.-based global trade association representing 55 of the world's most dynamic and innovative companies in the information and communications technology (ICT) sector. I want to thank you, Mr. Chairman, for scheduling this extremely important and timely hearing – important for the reasons that I will outline shortly and timely because bipartisan congressional action on surveillance reform this year is critical to the continued innovative and competitive success of our sector in global markets.

The ongoing revelations about data collection by the National Security Agency (NSA) are having a significant economic impact on our sector, aside from the substantial societal implications that have been so much in the news. I discuss below the economic impact, as well as the potential long-term implications on the global economy for innovation and Internet governance, and offer our thoughts on solutions.

We live in a world where reality is quickly outpacing even our imagination. Today consumers can purchase a watch that is also a phone and a biometric device that monitors your heart rate. We can purchase cars that can slow down on their own to avoid accidents and also alert you to avoid an accident. We have access to three-dimensional printers that one day will produce organs and limbs to expedite transplants. These innovations are not only cool—they are potentially both life-saving and world changing. Further, these inventions rely on an innovation ecosystem that is global in nature, largely because of an Internet governance model that is open, integrated, and borderless. The tech sector is committed to sustaining both because they have served this nation and our world well.

Business Impact

The United States has been a leader in, and major economic beneficiary of, practically every part of the technology sector. For example data analytics, according to information technology research and advisory firm Gartner, will generate more than 4.4 million jobs worldwide between 2012 and 2015, including more than 1.9 million new IT positions in the U.S. And, according to a study by the International Data Corporation, cloud computing will create almost 14 million jobs worldwide from 2011 to 2015, including nearly 1.2 million new positions in the U.S. and Canada. Public and government responses from around the world to the NSA disclosures put that job creating potential at risk. The NSA disclosures, by creating a misimpression of the U.S technology sector, are eroding trust in U.S. companies and in the security of data they hold. It is well established that: (a) data security is not a question of server location but rather depends upon the mechanisms and controls in place to safeguard the data; and (b) the data held by U.S. companies are as secure as data held anywhere else in the world. U.S. tech companies, like tech companies globally, view data integrity and security as their first priority.

Nonetheless, damage is being done. "Made in America" is no longer viewed as positive for customers of U.S. online services. Indeed, almost every ITI member company is 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, translating into lost American jobs. One recent 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. Let me take it one step further -- 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 have the potential of pushing the now-open Internet into a Smoot-Hawley protectionist death spiral, with disruptive global impact on international trade and commerce. We are facing nothing short 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 Brazil, and has 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), placing in jeopardy 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. Government officials at the European Commission and in EU Member States are now questioning whether this mechanism -- 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 proposal and requirements would be highly disruptive to business operations, create network architecture inefficiencies that would hinder the performance of ICT services, and Balkanize open platforms, including the Internet, that are key to continued transformative innovations and global commerce.

Solutions

It is critical the U.S. government take the lead to reverse the erosion of public trust and the acceleration of forced localization and other onerous policies that would Balkanize the Internet and other open platforms.

We need a public policy course correction, and it must begin here in Congress. In fact, Mr. Chairman, this hearing is particularly helpful in highlighting that 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 Congress works to develop appropriate measures to improve surveillance polices, 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.

Both the Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board have made recommendations relating to the nation's surveillance programs. And President Obama recently outlined policy measures he supports.

We are encouraged by the building momentum to reform our surveillance policies, which now must translate into congressional action.

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

The 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, whether it is referred to as a special advocate or a public advocate, should be appointed in appropriate cases to assist the FISC in evaluating the issues at hand. This additional party would be an advocate for the privacy and civil liberty considerations implicated in the 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 should be reaffirmed.

Rebuilding Trust: Section 215

In addition to the transparency and other measures outlined above that are designed to increase public trust, there is an additional step that would provide greater certainty about how the U.S. government designs and implements the surveillance programs it operates.

This step involves Section 215 of the Patriot Act. There is a great deal of uncertainty surrounding what type of surveillance is authorized by Section 215 of the Patriot Act. Uncertainty leads to distrust, as does indiscriminate collection of private sector data by the government. Any collection of private sector data by the government must have the appropriate legal basis. In addition, especially given the number of technology tools that exist today, the collection of private sector data need not be indiscriminate.

We urge Congress to re-examine Section 215 with a focus on the extent to which national security interests are actually being advanced under existing practices, and to consider, as part of that examination, domestic and international implications, the implications on the perception of independence of the U.S. tech sector, significant economic costs, and the impact on existing Internet governance models. These same considerations are also important in assessing whether the private sector should store meta-data, rather than the U.S. government.

Conclusion

Mr. Chairman, we need to restore "Made in America" as a positive description of U.S. cloud services. The first step forward begins here. We at ITI are ready to work with this Committee and your colleagues on both sides of Capitol Hill, as well as 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.

-30-