



Submission to the Privacy and Civil Liberties Oversight Board (PCLOB)
Notice: Hearings: Surveillance Programs

Docket Number: PCLOB 2013-0005

October 24, 2013

The undersigned technology trade associations represent more than 500 U.S. and foreign-based companies that span the information and communications technology (ICT) sector spanning infrastructure, computer hardware, software, telecommunications, consumer electronics, and information technology, e-commerce and Internet services. Our member companies operate globally.

We appreciated the opportunity to meet with the members of the Privacy and Civil Liberties Oversight Board (PCLOB) last month. As our members discussed at the meeting, the recent revelations relating to the U.S. intelligence programs have impacted the technology sector both domestically and internationally.

Around the world, there is mistrust over the security of hardware and software produced by the technology sector. Concerns about U.S. government access to privately held user data by U.S. companies is eroding trust in U.S. ICT products globally, and encouraging governments to adopt localization requirements that threaten the competitiveness of U.S. ICT products and services, or that could close off foreign markets entirely. The revelations could serve as the pretext for protectionist measures in foreign markets that are designed to promote domestic industries within such foreign markets.

The impact of this lack of trust is real. A number of recent reports predict the extent to which the U.S. technology industry will lose revenue as a result of the revelations. For example, one report anticipates that the revelations could result in as much as a $35 billion loss to the U.S. cloud industry over the course of three years.[1]

While it is too soon to know the business losses that will result, the revelations have severely

[1] Castro, Daniel, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?" *The Information Technology & Innovation Foundation*, August 2013, accessed October 23, 2013, http://www2.itif.org/2013-cloud-computing-costs.pdf.

exacerbated long-standing issues for U.S. companies doing business overseas relating to U.S. government access to data stored with U.S. service providers. The U.S. government, aware of the difficulties that U.S. providers face on these issues, issued a document in 2012 that, among other things, attempts to dispel perceived misconceptions about how and the extent to which the U.S. government may gain access to certain data.[2]

With the revelations over the course of the last few months, the concerns among potential customers of U.S. service providers have grown significantly. Our members have reported lost and delayed contracts over the last several months, based on concerns about data residing on servers in the U.S. and the potential for U.S. government access to that data. Further, specific feedback suggests that these types of concerns are expressed in business-to-business transactions in almost half of the transactions with potential partners. At a minimum, U.S. companies are facing increased scrutiny and higher costs when doing business overseas.

Business losses are not the only economic indicator to measure how the revelations might have a financial impact on U.S. companies. Policy and regulatory actions that have been proposed in some jurisdictions in reaction to the reports would require information technology companies to incur significant costs in order to serve those markets. Brazil is considering a legislative proposal that would require data collected in Brazil to be stored locally.[3] Such a requirement would compel technology companies doing business in Brazil to build data centers in Brazil. This would come at a great financial cost. It has been reported that it costs 40% more in Brazil to build a data center than it would to build one in the U.S.[4] Building a data center comes at a significant cost – often hundreds of millions of dollars.[5]

In addition to the financial cost, a local data center requirement would also create network architecture inefficiencies that would hinder the performance and launch of new services. Localization requirements result in the delay of U.S. or other companies offering new services in the host country, which would thwart that country's economic development and innovation goals. We also note that Brazil's proposal has the potential to negatively impact Brazil's economy. Companies providing ICT services may decide to invest in other countries in Latin America in order to avoid legal risks in Brazil, and some companies already installed in Brazil may decide to leave. This flight of businesses could prevent Brazil from having access to the widest range of

---

[2] "Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States," *U.S. Department of State*, accessed October 23, 2013, http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf.

[3] See "Letter to Ministers of the Brazilian Government," *Information Technology Industry Council*, August 5, 2013, accessed October 23, 2013, http://www.itic.org/dotAsset/2a6d7008-9c61-4f7c-917a-5fe4ad493527.pdf.

[4] Sooraj Shah, "Cost of Building a Data Center in Brazil is 40 Percent More than the US," *Computing*, September 20, 2013, accessed October 23, 2013, http://www.computing.co.uk/ctg/news/2295802/cost-of-building-a-data-centre-in-brazil-is-40-per-cent-more-than-the-us.

[5] Kenneth Brill, Johnathan Koomey, John Stanely, Bruce Taylor and Pitt Turner, "A Simple Model for Determining True Total Costs for Data Centers," *Uptime Institute*,*Inc.*, accessed October 23, 2013, http://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/%28TUI3011B%29SimpleModelDeterminingTrueTCO.pdf.

affordable and leading-edge technologies available and from taking advantage of the increase in competitiveness and reduction in costs provided by the Internet.

The revelations have also received significant attention in the European Union, placing in jeopardy one of the most critical data transfer mechanisms that many U.S. companies rely on to transfer data from the EU to the U.S. in the technology sector as well as other industry sectors. 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.[6] Were the Safe Harbor no longer an available data transfer mechanism, an alternative transfer mechanism would need to be arranged, or data flows would cease. Either scenario would be highly disruptive to business operations.

Global customer and policy responses, such as the ones discussed above, demonstrate that the current perceptions of U.S. surveillance practices are putting U.S. businesses at a competitive disadvantage in international markets. The Administration's responses to date are further undermining public trust, and are accelerating the push for forced localization and other onerous policies that have the potential to balkanize open platforms, including the Internet, that are key to continued transformative innovations and global commerce.

The solutions we propose below are guided by three principles. First, as the recently retired chairman of the Joint Chiefs of Staff Adm. Mike Mullen has pointed out, a "strong economy and strong national security are inextricably linked."[7] Second, security and privacy are not on opposite sides of the spectrum: both are priorities and security can be advanced in a privacy-protective manner. Third, restoring trust, both domestically and internationally, must be a driving force of these efforts.

PCLOB, established as an independent agency within the executive branch, has been tasked with ensuring that this second principle is fully implemented. Security and privacy should not be perceived as mutually exclusive. A recent report noted that government policies enacted in the name of "cybersecurity" could, if not designed to provide both strong security and privacy, impede the global flow of information technology products and services, harming not only information technology firms and vendors, but also importing countries.[8]

---

[6] See "Informal Justice Council in Vilnius," *European Commission*, July 19, 2013, accessed October 23, 2013, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm; and "Conference of German Data Protection Commissioners," *The Federal Commissioner for Data Protection and Freedom of Information*, July 24, 2013, accessed October 23, 2013. http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.

[7] "Group of Distinguished Defense, Economic and Foreign Policy Leaders Identify the National Debt as the Single Greatest Threat to U.S. National Security," *Peter G. Peterson Foundation*, December 4, 2012, accessed October 23, 2013, http://www.pgpf.org/Issues/Fiscal-Outlook/2012/12/120412-Coalition-for-Fiscal-and-National-Security-Announcement.

[8] Allan Friedman, "Cybersecurity and Trade: National Policies, Global and Local Consequences," *Brookings Institution Center for Technology Innovation*, September 2013, accessed October 23, 2013, http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf.

As outlined in PCLOB's enabling statute, PCLOB's mandate in connection with measures to protect the nation from terrorism is to:

> *advise the President and the departments, agencies and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered.*[9]

In connection with PCLOB's current study of U.S. counterterrorism surveillance programs, and with PCLOB's ongoing work to ensure that privacy and civil liberty concerns are appropriately considered in connection with counterterrorism efforts, we make the following recommendations.

The measures outlined below would promote an appropriate culture of transparency surrounding the government's intelligence-gathering programs – without national security risks. Indeed, promoting appropriate transparency surrounding intelligence-gathering is not a goal limited to the U.S.; it should be pursued internationally.

I. Information about Orders

Transparency is a core value of the technology sector. The companies that make up the sector are committed to informing their users and the public about requests received from governments around the world for law enforcement and intelligence purposes. The existing limitations on what private companies can disclose about the orders they receive undermine public trust in the industry and its compliance with the legal regime in various countries. Absent a verifiable security reason not to do so, companies should be able to provide more information about such orders.

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.

II. Foreign Intelligence Surveillance Court

President Obama has committed to working with Congress to improve the public's confidence in the oversight conducted by the Foreign Intelligence Surveillance Court (FISC). Specifically,

[9] 42 USC 2000ee(d).

President Obama has stated that steps can be taken to make sure civil liberties concerns are raised in appropriate cases by appointing an adversary to challenge the U.S. government's position. We urge that any such steps provide a meaningful opportunity for civil liberties concerns to be considered in FISC proceedings.

An additional step that can be taken to increase FISC transparency would be the declassification of FISC opinions where appropriate. A body of law has been, and continues to be developed, within the FISC. Providing appropriate access to the legal basis for court findings will improve public understanding of the factors that court takes into account in its rulings. Moreover, the appropriate declassification of FISC opinions can help inform the broader debate by ensuring effective review and scrutiny of the interpretation and implementation of key FISA authorities. This type of transparency can also yield greater public trust in the government's programs and in the process utilized by the government to gain access to user data.

In addition to the transparency measures outlined above, the following additional steps are recommended.

III. Cryptography

Recent press reports describe in general terms the efforts of the National Security Agency (NSA) to defeat cryptographic protections for surveillance purposes. The reports suggest that this effort went beyond the use of specially designed high-speed computers to crack encryption codes and involved the agency in an attempt to "introduce weaknesses into the encryption standards followed by hardware and software developers around the world."[10]

For nearly 20 years, the technology and user community has 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.[11] Some security firms have issued advisories to their customers to avoid using algorithms that might contain weaknesses.[12]

---

[10] Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *The New York Times*, September 5, 2013, accessed October 23, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0.

[11] Nicole Perlroth, "Government Announces Steps to Restore Confidence on Encryption Standards," *The New York Times*, September10, 2013, accessed October 23, 2013, http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.

[12] Kim Zetter, "RSA Tells Its Developer Customers: Stop Using NSA- Linked Algorithm," *Wired*, September 19, 2013, accessed October 23, 2013, http://www.wired.com/threatlevel/2013/09/rsa-advisory-nsa-algorithm/.

We appreciate that the National Institute of Standards and Technology (NIST) has issued a public statement reiterating its mission to develop standards and guidelines to protect federal information and information systems, and industry at large, using a transparent, public process. 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."[13] 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 these news accounts should be investigated and it may be appropriate for PCLOB to make recommendations in the area of cryptographic standard setting. We recommend that the Administration reaffirm the separate roles played by NIST and NSA in cryptographic standards.[14]

IV. Data Retention

We take this opportunity to address any proposals that might be made to limit government collection of data by imposing data retention requirements on private sector companies. It is unclear what privacy or security issue such proposals would address. We point out that such requirements could represent a step backward for privacy, given that they would mandate the retention of the same, or perhaps even an increased volume of information relative to what the NSA has been criticized for collecting. Data retention requirements would not only shift responsibility for housing such data to private companies, but would impose unnecessary and counterproductive costs on companies as well, by forcing them to store data that they have no business reason to retain. Costs of a data retention program include data storage centers, systems retrieving data upon government request, and technical expertise for maintaining these systems. The diversion of scarce engineering, legal, and managerial resources to government-mandated data retention represents a real opportunity cost that would inhibit innovation in new products and services. Such mandates would likely result in a preference for ICT services in overseas markets where these burdensome mandates do not exist. It would represent a threat to the global competitiveness of the U.S. technology sector.

V. Modernizing Legal Assistance Processes

International efforts around evidence collection for terrorist and other law enforcement investigations have been a driving component of recent government surveillance concerns. One mechanism pursuant to which such evidence is collected is the mutual legal assistance treaty (MLAT) process. MLATs are treaties between two or more countries that define processes and timelines for law enforcement cooperation. Through an MLAT to which the U.S. is a signatory, a foreign government can ask the U.S. government for help in obtaining evidence from entities in the United States.

---

[13] "Director Cybersecurity Statement," *National Institute of Standards and Technology*, accessed October 23, 2013, http://www.nist.gov/director/cybersecuritystatement-091013.cfm.

[14] Computer Systems Laboratory Bulletin, Computer Security Roles of NIST and NSA, February 1991, accessed October 23, 2013, http://csrc.nist.gov/publications/nistbul/csl91-02.txt.

The U.S. government should seek to modernize and streamline treaty-driven processes for mutual legal assistance, to ensure that lawful foreign assistance requests contain consistent requirements and can be reviewed in an efficient manner. In addition, guidance on submission requirements should be easily understood and publicly available.[15]

Moreover, the U.S. government should institute a program to promote the use of treaty-driven processes by other countries that might otherwise seek to obtain information directly from companies (U.S.-based or otherwise) outside the well-established treaty processes and potentially in violation of current U.S. law.

VI. Oversight

In its examination of the U.S. government's intelligence gathering programs, we urge that PCLOB pay particular attention to the oversight mechanisms that are in place in connection with these programs. For example, we ask that you review the structure of the FISC and determine whether improvements can be made in that process.

VII. Technology

As PCLOB examines counterterrorism programs currently in place, as well as future proposals, we urge you to consider how technology tools can be utilized to protect the integrity and confidentiality of information collected and maintained as part of properly authorized surveillance activities and to better address certain privacy and civil liberties concerns.

In closing, we appreciate the opportunity to provide you with these recommendations as PCLOB develops findings and recommendations in connection with its work to ensure that the nation's counter-terrorism initiatives sufficiently protect privacy and civil liberties. We look forward to continuing on open dialogue with PCLOB.

* * *

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

---

[15] See "ICC policy statement on Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures," *International Chamber of Commerce*, December 9, 2012, accessed October 23, 2013, http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/mlat/.