Before the
Privacy and Civil Liberties Oversight Board
Washington, D.C.

In the matter of	)
July, 9 Public Workshop	)
Docket No. 2013-0004	)
	)

COMMENTS OF
THE COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

1 Introduction

In response to the Privacy and Civil Liberties Oversight Board (PCLOB) workshop on July 9, 2013 and the related call for comments, the Computer and Communications Industry Association (CCIA) submits the following statements.

CCIA is an international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.[1]

The time is ripe for PCLOB to finally begin the work it was intended to do. It has overcome numerous obstacles standing in the way of its creation, and the current crisis is both the exact eventuality the board is meant to avoid, had it been operating, and a situation where its expertise is desperately needed. CCIA would like to take this opportunity to welcome the board members and wish them the best in their endeavors.

In these comments, CCIA suggests two related areas in which the PCLOB can use its influence to improve both national security law itself as well as the process by which the government constructs surveillance policy. In general, PCLOB should attempt to position itself as the body within the administration but outside of the surveillance community which has the expertise and the clearances to convincingly argue against overbearing surveillance programs. In addition, while using the tools

[1] A complete list of CCIA's members is available online at http://www.ccianet.org/members.

and rhetoric of civil liberties and constitutional law are obvious routes for PCLOB, the board should also look at incorporating other convincing arguments for limiting surveillance, including those of commerce, foreign relations, and international Internet governance.

2 Righting the Balance Within the Government

American democracy has always been about the vocal and sometimes even strident competition between ideas. In the days of the drafting of the Constitution and its subsequent enactment by the states, the actions of the Continental Congress included careful compromise between contrary interests and vociferous public debate, such as in The Federalist Papers. Today that competition is evident in many functions of our government. The political parties working in Congress compete with one another, the Congress, the Executive, and the Judiciary form a system of careful checks and balances, and within the Executive branch the various departments and agencies use the interagency process to advance their own positions.

In our modern day, however, there is a striking absence of public debate on the topic of surveillance, particularly with regard to terrorism and national security. These topics are among the very few in which there in an inherent barrier to mere participation. That barrier is the system of classification and security clearances. The modern US administrations have used their power to classify larger and larger amounts of information in the name of national security. While the number of people given security clearances has exploded in the past decade,[2] those clearances are given out to support the intelligence community, not to oppose it. They end up in the national security related government bodies or for defense related contractors.[3]

When nearly all of the information about a surveillance program (sometimes including the fact that it exists) is hidden behind a classification, it limits the people that are able to participate in the conversation. Because employees at the non-defense related agencies generally have less cause to seek security clearances and therefore receive them much less frequently than do their counterparts within the national security agencies, conversations about the propriety of surveillance programs are likely one-sided. In addition, there can also be a

[2]Steven Aftergood, *Number of Security Cleared Personnel Grew in 2012*, Secrecy News, April 15, 2013, at http://blogs.fas.org/secrecy/2013/04/2012_clearances/.

[3]For some sense of who is given security clearances, *see* Office of the Director of National Intelligence, 2012 Report on Security Clearance Determinations (2012).

The repercussions of this can be seen in the fall out from the recent leaks about NSA surveillance programs. Around the world, people are migrating away from US-based Internet services because privacy is based on trust and US companies are perceived as being complicit with US surveillance authorities.[4] This result is not a surprise and representatives of the Commerce Department should have been in a position to raise the concern as a reason to narrowly tailor spying authorities. Similarly, the State Department has for years been advocating around the world for Internet freedom and for maintaining the multi-stakeholder method of Internet governance that has worked so well to date. In the wake of the recent revelations, however, many authoritarian countries have renewed their calls for state control of vital Internet resources such as the domain name system.[5] Had the leaders of the relevant State Department offices been aware of the now-leaked systems, this point of view could have been discussed and incorporated into the planning of the programs.

While one answer to these problems is to greatly reduce the amount of information about the surveillance programs hidden behind classification (and CCIA is pushing for greater transparency in that area),[6] it is unlikely that all the important details can or should be declassified. This is a problem that PCLOB has the potential to address. Board members, who all have top secret security clearances and the mandate to carefully inspect and oppose overarching surveillance, are well positioned to be briefed on proposed surveillance requests and orders from the FISA Court and provide a wide range of contrasting ideas in order to clearly articulate the costs of surveillance decisions. In doing so, PCLOB should seek to use whatever processes are available to it, including in the interagency process and direct consultation with relevant agencies. CCIA strongly recommends that PCLOB advocate within the administration for the kind of access that would make this role feasible to play.

[4] *See, e.g.*, John Naughton, *Edward Snowden is not the story. The fate of the internet is.*, The Guardian, July 27, 2013, at http://m.guardiannews.com/technology/2013/jul/28/edward-snowden-death-of-internet.

[5] Josh Peterson, *NSA surveillance leaks damage Obama administration's Internet freedom agenda*, The Daily Caller, June 25, 2013, at http://dailycaller.com/2013/06/25/nsa-surveillance-leaks-damage-obama-administrations-internet-freedom-agenda/.

[6] Press Release, Computer and Communications Industry Association, CCIA, Others Ask For More Transparency On Surveillance Practices (July 18, 2013)

3 Broadening the Range of Arguments

Privacy and civil liberties are inherently important rhetorical positions from which to stand up against overbearing government surveillance, but they are not the only ones. There are also important economic, trade, and Internet governance reasons to control government surveillance. These goals will help American companies both at home and abroad, as well as support Administration policy in trade negotiations that involve data flows and issues of Internet freedom and Internet governance. All of these concerns are inextricably bound together with our country's policy on online surveillance.

Companies that provide online services know that user trust is of the utmost importance, particularly when the nature of those services makes switching to a competitor as easy as typing a different URL into a browser. The recent leaks regarding the NSA have led to users the world over feeling like their trust has been broken, and resulted in calls internationally for users to switch to only locally owned online services.[7] Some countries have again turned to ideas such as local hosting requirements, in which online services that store data for users are forced to keep that data in the country in which the user lives.[8] These requirements would completely undermine the work that the Commerce Department and the United States Trade Representative have engaged in for a number of years. Requirements like these would also work to counter some of the greatest advantages that the Internet brings. By placing data around the world based on where it is most efficient, fastest, or cheapest, companies can lower costs, improve services, and even help the planet by using less power to cool their server farms.

There are non-economic issues that the NSA revelations have brought to the forefront as well. For much of the past years the State Department has been advocating abroad for Internet freedom, often coming into conflict with more authoritarian regimes who are seeking international opprobrium for their own acts of censorship on the web. Unfettered access to information is one of the great gifts of the Internet and it has the potential to raise the impoverished and the victims of dictatorships. The past few years have seen a new growth in countries pushing for greater government

[7] *See, e.g.*, Posting of Gerd Leonhard to Harvard Business Review Blog, http://blogs.hbr.org/cs/2013/07/a_call_to_boycott_us_tech_plat.html (July 16, 2013, 10:00 EST).

[8] Amy Armitage, *One lesson from the NSA scandal: Find out where your cloud provider's data centers are located*, GigaOm, June 16, 2013, at http://gigaom.com/2013/06/16/cloud-security-depends-on-geography/.

control of the Internet, predominantly within the UN's International Telecommunications Union, but also with other intergovernmental bodies both within and outside the UN system. Programs such as PRISM and others leaked recently affirmatively harm US efforts in these areas. Ironically, they give cover to governments that are truly authoritarian who can now point to US programs and claim that censorship and surveillance are global norms. They also alienate countries that were "on the fence" about supporting the US in its Internet freedom campaign by creating a trust deficit that will take years if not longer to overcome.

4 Conclusion

An effective Privacy and Civil Liberties Oversight Board was vitally needed in the past decade, but without that it is vitally needed now. There are existential questions at stake, for civil rights and civil liberties but also for the future of the Internet itself as a global platform for expression and commerce.[9] The United States must work to overcome the trust issues caused by the NSA's international spying efforts and a strong showing by the Board would do much to begin that process. By using all of the available arguments and finding a voice to push back against the overreaches of the national security establishment, this moment can become a catalyst for greater checks against government surveillance, saving the Internet from balkanization and preserving civil liberties and American businesses.

[9] Naughton, *supra*, note 4.