Statement of

Edward J. Black

President & CEO of

The Computer & Communications Industry Association

Before the

Senate Judiciary Committee

"Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

1 Introduction

Chairman Leahy, Ranking Member Grassley, members of the Judiciary Committee, thank you for the opportunity to offer testimony today on the surveillance authorities of the National Security Agency and how those authorities are affecting the Internet and the global trade in services online. CCIA is a 40-year old international nonprofit association representing a broad cross section of computer, communications and Internet industry firms. Our members employ more than 600,000 workers and generate annual revenues in excess of $200 billion.

This testimony will outline the promise of and the challenges to the open Internet, as well as some changes in law that will help preserve the civil liberties of Americans and the vital commerce of the Internet services sector both in the U.S. and in markets around the world. I am proud to announce in that context that CCIA supports the USA FREEDOM Act offered by Chairman Leahy and Representative Sensenbrenner. There are a few areas where we have some suggestions to improve the bill and we look forward to working with the Chairman and his staff on those points. Finally, this testimony will offer some suggestions for addressing the disparity between U.S. citizens and foreigners in a global age on a global network.

It is important to step back from the current controversy to provide context. In 1997 the United States government issued what has been widely hailed as a prescient and insightful policy statement that laid the foundation of the U.S. government's approach to the Internet. A task force, led by Ira Magaziner, produced the first major review of Internet policy and global commerce in 1997. In the Framework for Global Electronic Commerce, the White House put forward five principles to guide the development of the new digital economy. These principles enshrined an extremely successful approach to Internet policy that has seen the Internet grow from a medium with approximately 100 million

users in 1997 to nearly 3 billion Internet users today. The policy statement also identified what was the most crucial variable determining whether the Internet lived up to its potential as both an economic and social medium: public trust.

> If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce.[1]

If the above quote seems rudimentary, it is. However, it is also easy to take for granted what has been achieved since 1997 in creating a more secure online environment for commerce and communication. It is even easier to discount how easily decades of progress in creating user trust in the fidelity of their online conversations and transactions can be eroded. Revelations about the NSA's surveillance programs have had global repercussions and threaten to undermine the very trust upon which the current success and future growth of the Internet depend.

The fallout has harmed individual U.S. companies, the competitiveness of the United States economy, and the evolution of the Internet itself. It is difficult to overemphasize how deeply felt have been the reverberations of these revelations in discussions of Internet governance, trade, and freedom around the world. Here in the United States we have been focused understandably on the rights and liberties of Americans, questions of rule of law, and public opinion across the country. While these are critical issues, it is important that the Committee also concern itself with the fact that the behavior of the NSA, combined with the global environment in which this summer's revelations were released, may well pose an existential threat to the Internet as we know it today, and, consequently, to many vital U.S. interests, including the U.S. economy. That is why a number

[1] President William J. Clinton and Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce (1997), *available at* http://clinton4.nara.gov/WH/New/Commerce/read.html.

of large Internet companies earlier this week released a set of principles calling for an end to bulk collection, better oversight and transparency, and protection for free flow of information.[2] Of particular note, these principles were addressed to governments around the world, not just here at home, because this is a problem that will take all of us to fix.

2 Economic Security

The members of the committee are no doubt familiar with the great commercial benefits the open Internet provides. It allows small-and-medium-size businesses to access markets and customers well beyond their reach in the brick and mortar world, lowers costs along the entirety of global supply chains, increases efficiency in business from the Fortune 500 down to the smallest mom-and-pop shop, and is the catalyst for the online services marketplace, one of the greatest economic drivers in the country today.

As an example of the immense economic benefit of the Internet, the Boston Consulting Group conducted a study in 2012 analysing the economic promise of the Internet economy.[3] The study predicts that the Internet economy in the G-20 will reach $4.2 trillion by 2016. Another study, conducted by the McKinsey Global Institute, estimates that 21% of GDP growth over the past 5 years is attributable to the Internet and that 2.6 jobs are created for every job lost.[4] And, perhaps more telling, the same study estimates that 75% of the economic value of the Internet accrues to traditional sectors of the economy in the form of greater efficiency and expanded market access.

[2] Global Government Surveillance Reform, *available at* http://reformgovernmentsurveillance.com/.

[3] Boston Consulting Group, The $4.2 Trillion Opportunity: The Internet Economy in the G-20, March 2012, *available at* https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf.

[4] McKinsey Global Institute, Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011, *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

The U.S. government has even taken notice. A recent comprehensive report from the U.S. International Trade Commission (ITC) noted, "digital trade continues to grow both in the U.S. economy and globally" and that a "further increase in digital trade is probable, with the U.S. in the lead." In fact, the report also shows, U.S. digital exports have exceeded imports and that surplus has continually widened since 2007.[5] As traditional manufacturing and lower-skill service sector jobs migrate overseas, the Internet, and the innovative ecosystem that it has spawned, is becoming increasingly important to our global economic competitiveness. As a result, the economic security risks posed by NSA surveillance, and the international political reaction to it, should not be subjugated to traditional national security arguments, as our global competitiveness is essential to long-term American security. It is no accident that the official National Security Strategy of the United States includes increasing exports as a major component of our national defense strategy.[6]

The NSA's practices have clear impacts on the business of the U.S.-based Internet companies. So much of online commerce today is fundamentally based on trust. If users are going to turn over very sensitive information such as the contents of an inbox, to a company providing an online email or other cloud service, they need to have trust in the idea that the company will act as a responsible steward of that data. So much of the promise of the Internet is reliant on that trust, as the Magaziner report made clear 16 years ago.[7]

The images portrayed in the press of Internet companies happily working with the NSA to turn over vast troves of information about users, while almost entirely untrue, nevertheless harmed the trust of users. We have seen the effects both here in the U.S. and around the world in both public rhetoric and the bot-

[5] U.S. ITC, *Digital Trade in the U.S. and Global Economies, Part 1* (2013), at xix, *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

[6] The White House, *National Security Strategy of the United States* (2010), at 32, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[7] *Supra*, note 1.

tom line. Contracts, particularly at the enterprise and government levels, are being cancelled and there are calls to somehow limit the amount of information sent to companies within the U.S. The European Union is even seriously reconsidering the EU - U.S. Safe Harbor Agreement that permits U.S. companies to collect information about European citizens. All of these efforts have an obvious effect on commerce in a sector of the U.S. economy that has shown some of the best performance in the recent economically difficult times.

Revelations about NSA surveillance of foreign users of American service providers, however, have made that natural commerce much less fruitful. Even worse have been the discussions since the first revelations. The White House almost immediately began emphasizing the legal protections afforded to American citizens under the current system. Others in Congress and the press have continued to emphasize this line of argument. It is important to emphasize how harmful this approach is to companies trying to do business around the world. Congress cannot expect American companies to successfully export information services if the protections their customers receive are weaker than the protections provided by the foreign competition. Last week Cisco announced their latest quarterly earnings are lower than expected because of a lack of trust of an American company abroad.[8] American cloud companies also report that both governmental and enterprise purchasing of U.S. cloud services in Europe have declined.

The NSA's efforts to undermine international encryption standards have also made us economically weaker. Those same standards the NSA subverts are used by people around the world to bank and shop safely online. Weaker encryption can be used by hackers to break passwords, conduct espionage, steal identities, and create mayhem. By decreasing the effectiveness of cryptography,

[8]Richard Waters, *Cisco cites emerging markets backlash on NSA leaks for sales slump*, Financial Times, Nov. 13, 2013.

the NSA is singlehandedly creating cybersecurity threats at a time when our Congress has been debating how to shore up our cyber defenses. Furthermore, this is at odds with the NSA's other stated mission: protecting the security of American networks. As Matthew Green, a noted encryption expert at John Hopkins University noted, The risk is that when you build a back door into systems, youre not the only one to exploit it.... Those back doors could work against U.S. communications, too.[9]

With these affects in mind, it would be dangerously myopic to separate the economic effects of widespread Internet surveillance from its security impacts.

3 Soft Power

The Internet's value obviously cannot be summed up in just dollars and cents. It is impossible to place a monetary value on the ability for people around the world to connect with each other, exchange ideas, debate politics, and experience foreign cultures. This is the Internet's greatest value and it may do more for national security than all the surveillance the government could muster. It is sometimes said that no two countries that both have a McDonald's have ever gone to war.[10] Although this analogy might overstate the causal mechanism behind peace, it is certain that unfettered Internet access, and the international commercial and economic interdependence that flows from it, makes international military conflict more costly and therefore less likely.

U.S. national security increasingly depends as much on this "soft power" in addition to traditional hard power. It is important to recognize the dramatic effect these revelations have had on our international diplomatic sway,

[9] Jeff Larson, Nicole Perlroth, and Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, ProPublica, Sep 5, 2013, *available at* http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[10] Thomas Friedman, The Lexus and the Olive Tree, (Farrar, Strauss, and Giroux 1999).

particularly in regards to the future of Internet governance.

Even before the revelations in the *Guardian*, *Washington Post*, and other papers this summer, the open Internet was in trouble. Most people associate the World Conference on International Telecommunications (WCIT) treaty conference of last year with the first attempts to wrest control of the Internet away from the bottom-up multi-stakeholder organizations that have kept it running for years, but the efforts go back even further. Numerous governments – both well-meaning and repressive – have long believed that all Internet problems could be solved, if only they were in charge.

These efforts have escalated since this summer's revelations. The U.S. government position of supporting the multi-stakeholder model of Internet governance has been compromised. We have heard increased calls for the ITU or the United Nations in general to seize Internet governance functions from organizations that are perceived to be too closely associated with the U.S. government, such as the Internet Corporation for Assigned Names and Numbers (ICANN). This is unfortunate because ICANN is one of the best examples of an independent multi-stakeholder organization. Furthermore, the Internet governance regime that ICANN has cultivated has subjugated political concerns to economic and technical decisions, which, in turn, has allowed the Internet to grow from an obscure medium largely known only to academics 20 years ago, to a tool utilized by nearly 3 billion people today.[11] ICANN and the other multi-stakeholder governance groups have also seen it necessary to move themselves further away from U.S. government control.[12]

Finally, we have been faced with a series of proposals for modifications of the engineering structure of the Internet, such as requirements that companies

[11] 2.749 billion individuals are using the Internet, according to the ITU's 2013 ICT data, *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

[12] *See Montevideo Statement on the Future of Internet Cooperation*, ICANN, *et al.*, (2013), *available at* http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm.

host all citizens' data physically in a particular country rather than where it is most efficient or cost effective. These demands are simply digital protectionism wrapped up in the cloak of privacy protection, but they are enabled by the perception U.S. government's actions. We have unfortunately seen these demands from places as diverse as the EU, Brazil, and Indonesia.

Losing this international diplomatic battle and turning over control of the Internet to politicians and bureaucrats from around the world would have disastrous consequences for the future growth and vitality of the Internet. Given that nearly half of the world voted against the U.S.'s position on the future of Internet governance at the WCIT last December[13] – before the NSA revelations were made public – ceding more rhetorical ammunition to our political enemies is detrimental to the U.S.'s diplomatic ability to protect the Internet.

The timing for this situation could not be worse. The next year will see a large number of events at which Internet governance will be a topic of discussion. Some of these, such as the ITU Plenipotentiary Conference, the World Summit on the Information Society ten year review, and the World Telecommunications Development Conference, are occurring on a set schedule but will be considerably more focused on these questions than they may otherwise have been. Others like the Internet governance meeting taking place in Brazil next year, and the new focus on governance emerging at both the UN's Commission on Science and Technology for Development and in the General Assembly, are directly a result of the NSA's actions, particularly with reference to non-U.S. citizens. We already know that there will be many countries at these meetings seeking to usurp the governance of the Internet and give it to organizations like the International Telecommunications Union. This damage to the U.S.'s reputation on governance and the potential for adverse results in international

[13]WCIT 2012, *Signatories of the Final Acts* (December 2012), *available at* http://www.itu.int/osg/wcit-12/highlights/signatories.html.

fora will take hard work and a lot of time to overcome. It is a damage that will persist unless deep, fundamental change is undertaken.

Furthermore, it is important to recognize that there is no "status quo" option in this conversation. The world is already reacting to make the NSA's programs less effective. If the Unites States comes across as stubborn or unwilling to engage on this topic, particularly where it comes to the data of foreigners, not only will the practical value of this surveillance be lessened, we will have contributed directly to the further fracturing of the global Internet.

To their credit, many within the U.S. government have seen this threat and responded, particularly within the State Department, which has made Internet Freedom a major policy initiative. Former Secretary Clinton and her staff should be applauded for their work evangelizing the open Internet. Unfortunately they have been unintentionally undermined by the actions of others in the national security establishment. Through a posture that seems to treat Americans only as sources of data, albeit ones with laws protecting them, and foreign nationals as merely sources of data alone, the NSA programs have greatly harmed the credibility of American calls for Internet freedom, multi-stakeholder governance, and the free flow of information in large portions of the world.

4 Transparency

Transparency in the use of surveillance authorities is fundamentally important. Without knowledge of what the government is doing, citizens have no means of judging whether and how to change the law. Companies who receive government demands are unable to be truthful with their users about the extent of surveillance that is happening. Finally, laws interpreted in secret courts and left generally unchallenged cannot form the basis for a healthy democracy. Transparency has therefore been a focus for the companies in the Internet services

marketplace since the first revelations and is reflected in the principles released earlier this week.

Transparency, therefore, must be a multi-pronged effort. It should involve as many avenues for getting information out to people as is feasible. The executive branch, the FISA courts, and the companies themselves all have a duty, and must be allowed the ability, to release information about surveillance programs.

The companies in particular have a great need to share this kind of information. A breakdown of what companies receive surveillance orders, and how many, will help develop the national debate surrounding surveillance in our country. In addition, companies have a unique need to inform their users publicly about how many requests they actually get from the government, particularly after the allegations made this summer. In addition, those numbers should be as precise as is feasible, because the tendency today is to be skeptical of companies that look like they are hiding something. Precision in these numbers will help combat these concerns.

Not all companies are developing transparency reports, but all of them should be encouraged to. Any company, whether U.S. based or foreign, that receives orders from any government to turn over or take down information should be releasing aggregate numbers of such demands. It will only be once we can learn the full impact of surveillance on our online services that we can make informed decisions.

Government also has an obligation to share with its citizens the laws that affect them on a day-to-day basis. The interpretations of the law, the procedures used by the surveillance authorities, and the number of times those authorities have been invoked are all vital pieces of information. This is not only true of the U.S. government, of course. Governments around the world should be encouraged to reveal this information, and if the U.S. takes this first step it will

be in a much greater position to demand the same of other countries.

The committee will no doubt hear that transparency of the sort here suggested will cause undue damage to the security of the nation. These transparency proposals are, however, no different than those permitted for years under criminal statutes. Transparency reporting in the criminal context is even enshrined in the Wiretap Act. There have been little to no complaints from law enforcement indicating organized crime has learned to evade surveillance because of such transparency. Indeed, if anything we are seeing increased demands for data under criminal statutes year over year. It would be a mistake to let vague warnings about terrorism deter the full development of transparency in this area, particularly when that obfuscation erodes our economic security.

The Surveillance Transparency Act of 2013, recently introduced by Senator Franken and the topic of a hearing last week, would go far to create the sort of transparency that will inform the public and help the companies set the record straight. That is why CCIA has also publicly supported Senator Franken's bill and why we are glad to see that Chairman Leahy has included that language in his bill.

5 Protection for Americans

Federal laws addressing under what circumstances the government may collect Americans' data for national security investigations are badly in need of reform. Many of them were understandably written in a culture of fear and since bolstered by the ever-present invocation of terrorism. What has been forgotten is the fact that one of the greatest contributors to national security is a strong

economy.[14] Today, Americans fear government intrusion more than terrorism.[15] The time has come to adjust our priorities.

One area of national security surveillance programs needing modification is the bulk collection of metadata. Despite statements by some that imply collection of metadata is not intrusive of privacy, there is a great deal that can be learned about a person if you can see a list of who they call or with whom they email. Medical conditions, religious affiliation, sexual identity, and more are all reasonably easily deduced from this sort of metadata. The government emphasizes, when discussing its metadata program, that there are many controls in place to protect the data once it is collected and housed by the NSA, but that provides little comfort. Even if the current administration's intentions are completely noble and without reproach, once the data is collected, it can be used in the future. Information, it is said, wants to be free. A corollary is perhaps that databases want to be used.

As we now know, the NSA seeks to use this sort of metadata to build a model of the social networks of Americans.[16] To store details on who we speak to and who we associate with runs into direct conflict with not just the Fourth Amendment but also the First. The Supreme Court recognized this fact as far back as 1958, when they decided NAACP v. Alabama. Justice Harlan, in denying the State of Alabama the right to peer into the NAACP's membership rolls, recognized the "vital relationship between freedom to associate and privacy in one's associations."[17] This is just one of the reasons why the principles released this week took aim so directly at bulk collection, calling on governments

[14] *See, e.g.*, Alice M. Rivlin, *National Security Depends on a Strong American Economy*, Brookings Institute (2010), *available at* http://www.brookings.edu/blogs/up-front/posts/2010/12/30-security-economy-rivlin.

[15] Pew Research Center for the People & the Press, *Few See Adequate Limits on NSA Surveillance Program*, Pew Research Center (2013), *available at* http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

[16] James Risen and Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times, Sep. 28, 2013.

[17] NAACP v. Alabama, 357 U.S. 449 (1958).

to "limit surveillance to specific known users for lawful purposes, and should not undertake bulk data collection of Internet communications."[18]

The USA FREEDOM Act would directly address this issue. It is good to see that it would address collection not just under Section 215 of the USA PATRIOT Act but also under a range of other authorizations including pen register/trap and trace provisions and National Security Letters. We know from official releases by the Director of National Intelligence that bulk collection of Internet metadata had been ongoing up through 2011 under the FISA pen register/trap and trace provisions. While we don't know precisely whether bulk collection of Internet metadata continues under other authorities at the moment, it is also encouraging that the bill seeks to prohibit all forms of bulk collection, for Internet and phone calling records.

Our laws protecting Americans must also be modified with regard to the operations of the Foreign Intelligence Surveillance Court. Right now the court issues its orders *ex parte*, with only the government in the room. While this works for criminal warrants, defendants in a criminal trial have the ability to challenge any improper warrants at trial. There is usually no such opportunity under FISA. That is why an institutional opponent should be created to intercede at the FISC, particularly in cases where the Court is grappling with novel questions of law and would be well served by hearing multiple sides of an argument.

It is important that such an advocate have the knowledge and the resources to properly represent the alternative viewpoints necessary to provide counsel to the FISC. In particular, we hope that the office will have access to technological expertise, as well as legal, as the NSA's programs are technologically complex and many in the FISC system have admitted that there is not enough knowledge

[18] Global Government Surveillance Reform, *available at* http://reformgovernmentsurveillance.com/.

to fully comprehend them. Senator Blumenthal's FISA Court Reform Act of 2013 is an excellent starting point and we are encouraged to see it included in Chairman Leahy's bill.

6 Foreigners Abroad

Despite the fact that the modern Internet is a global, interconnected medium, U.S. national security policy continues to operate on the presumption that U.S. citizens online deserve protection from unwarranted surveillance while others do not. While the U.S. began this great experiment, today's Internet is an international platform for innovation and communications. The network hosts commerce, politics, and love letters of billions from all corners of the globe – a fact reinforced as more of the developing world come online.

The short-sighted position that only a fraction of those users deserve privacy protections poses very real dangers for the future of the Internet. If foreign users are not provided any baseline assurances about the privacy of their personal information, communications and associations, then America's role as the world leader in Internet innovation and digital commerce is threatened. This is especially true going forward, as the fastest growing Internet markets are foreign and many major U.S. Internet companies are already attracting more users and reaping more revenue from abroad than they do at home.

Solving these problems will need the development of new legal paradigms. Old rules focused only on citizenship or location are anachronistic when it comes to the Internet. We do not yet have all the answers, but we must cease distinguishing Internet users in such a way if we wish our American companies to succeed globally. Furthermore, given that the Internet is global platform, Americans should have baseline assurances about their privacy when using non-US Internet platforms and services as well. The principles released this week

by major Internet companies focuses on this issue and calls for a framework for handling requests across jurisdictional boundaries, such as strengthened Mutual Legal Assistance Treaties (MLATs). If we don't change our rhetoric and seek new solutions to these problems, we will face a Internet surveillance arms race to the bottom that will almost certainly diminish the future commercial and social promise of the Internet as a global communications medium.

7 Conclusion

The Internet today is at a crossroads. The tool for commerce, expression, and communications so many of us have been building for a few decades now faces threats of balkanization, censorship, and being co-opted for the purposes of mass surveillance. This is not a sacrifice that should be made lightly. The companies that CCIA represents are in many ways the stewards of their users. There is a great responsibility to protect the trust given to them, and to work unceasingly toward a free and open Internet that will benefit everyone. The discussion that we are having today is one example of that larger goal.

This committee and Congress in general has the opportunity to have an incredible effect on the future of the Internet. It seems clear that for a long time our government has made choices impacting the Internet with only security fears in mind. This committee, right now, finally has the opportunity to right that wrong. I truly hope it does so. I thank you for the opportunity to testify on this crucial issue and look forward to answering your questions.