Before the
Review Group on Global Signals Intelligence Collection and Communications Technologies
Washington, D.C.

In the matter of	)
September 4 Request for Comments	)
	)

COMMENTS OF
THE COMPUTER AND COMMUNICATIONS INDUSTRY
ASSOCIATION

1 Introduction

In response to the Review Group on Global Signals Intelligence Collection and Communications Technologies' (Review Group) call for comments on September 4, 2013, the Computer and Communications Industry Association (CCIA) submits the following statements.

CCIA is an international, nonprofit association representing a broad cross section of computer, communications and Internet industry firms. CCIA remains dedicated, as it has for over 40 years, to promoting innovation and preserving full, fair and open competition throughout our industry. Our members employ more than 600,000 workers and generate annual revenues in excess of $200 billion.[1]

As an industry association, CCIA speaks on behalf of the industry as a whole. We do not, however, speak directly on behalf of our member companies, some of whom will probably submit comments of their own. The suggestions we provide below are our interpretations of what will be best for the entire industry going forward.

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

Over the past few months, the Internet industry has been deeply affected by the emerging national conversation on the NSA's surveillance powers. The Internet is one of the greatest communication technologies ever developed and it reaches people around the world, enabling them to talk to one another, exchange views, discuss politics, and conduct commerce. CCIA's members offer services that facilitate all of that communication. Those services, however, rely on the trust of the users, because in so many cases personal information is stored and used by these companies. If users do not trust a particular online service, using a different one is as easy as typing a different domain name.

This is why one of CCIA's major goals is promoting public policies that increase user trust. Unfortunately, the revelations about NSA spying have done exactly the opposite. Users both in the US and around the world are worried today that their governments are inappropriately spying on their communications and are looking for assurances that this is not the case. To remedy this situation, CCIA offers a number of suggestions in these comments, including procedural methods to improve the standing of the Foreign Intelligence Surveillance Court, and substantive changes to the law that are needed to restore trust in both government and the Internet ecosystem.

2 Transparency in the FISC

As Supreme Court Justice Louis Brandeis once wrote, "Sunlight is said to be the best of disinfectants."[2] The National Security Administration's (NSA) programs are shrouded in secrecy, and companies that receive FISA demands are generally barred from even acknowledging receipt, which would shed light on the volume and nature of FISA activities. Bringing its actions into public view will reinforce and protect the legitimacy of democracy, foster trust in US businesses, and force the NSA to think carefully about the number of requests it makes of private companies.

Secrecy in surveillance law can appear to make sense at first. In theory, letting the public know too much about surveillance may harm its effective-

[2]Louis D. Brandeis, *What Publicity Can Do*, Harper's Weekly, Dec. 20, 1913.

ness. In truth, however, sweeping transparency is not only possible without compromising security, it is vital for the nation. Over the past few months we have seen the government and the Foreign Intelligence Surveillance Court do exactly that, as they have released past court opinions. This is an excellent start, but it is also only a start.

As a basic minimal step, the government should also begin allowing companies to report aggregate numbers of requests that they receive from authorities. The national security arguments here remain vague[3] and the benefits of transparency are enormous. Because aggregate data reporting is legal in the criminal context and a number of companies already report such numbers,[4] there is an example from which to draw information about this sort of transparency. Despite years of such practice, there have been no claims of adverse impact on criminal investigations (even against coordinated and sophisticated adversaries such as organized crime). In fact, the sheer increase in the volume of government demands served on CCIA members and others in the industry suggests that those services are still fruitful sources of intelligence. Reporting requirements about numbers of orders are even statutorily mandated in some circumstances by federal law in the Wiretap Act.[5]

Reporting this data is also vitally important for business reasons both in the US and around the world. In the wake of revelations about NSA demands for users' data, companies have had serious problems with user trust. Many users have come to the conclusion that their data is no longer safe. Being unable to report how often the government makes such demands only exacerbates the distrust. We cannot know for sure, but it is very likely that if aggregate numbers were published, many would be comforted by the simple knowledge of the limited scale of the surveillance. Having a specific

[3] *See generally* Response of the United States to Motions for Declaratory Judgment by Google Inc., Microsoft Corporation, Yahoo! Inc., Facebook, Inc., and LinkedIn Corporation, Nos. 13-03, 13-04, 13-05, 13-06, and 13-07 (FISA Ct. Sep. 30, 2013).

[4] *See, e.g.*, Google Transparency Report, http://www.google.com/transparencyreport/, Facebook Global Government Request Report, https://www.facebook.com/about/government_requests, Microsoft Law Enforcement Request Report, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

[5] Wiretap Act, 18 U.S.C. 2519 (2013).

number to point to is probably better than whatever is imagined based on vague news reports.

Transparency is also vitally important as we begin to use our democratic processes to examine possible substantive changes to our national security surveillance law. While legislators have been given some opportunities to be briefed on the topic, the people they work for remain in the dark. Until the citizens know much more about the surveillance being conducted on them, in their name and with their tax dollars, there cannot be the truly informed public discussion that is so vital right now.

CCIA also supports a process for reviewing and declassifying the decisions of the Foreign Intelligence Surveillance Court (FISC). The Administration has now begun a long overdue process of releasing select opinions concerning significant statutory and constitutional issues. Haphazard release of selected opinions only risks making things worse, however, as the public can have no way of knowing what is in the unreleased opinions and why they were not selected for release.

Important economic interests would also be advanced by further declassification of FISC opinions. Companies thrive best when the rules they operate under are clear, stable, and well understood by all the people who might be subject to them. Secret opinions interpreting surveillance laws fail all of those tests. If fledgling companies seeking seed financing will be subject to laws that can be enforced in unpredictable and devastating ways, the market for financing such companies will dry up. Certainty in the law is the best way a government can encourage entrepreneurship and enable businesses to grow.

To overcome this problem, the government should undertake two actions. First, older FISC opinions should continue to be released with minimal redaction. Second, there should be a process to ensure contemporaneous release of FISC opinions upon disposition, consistent with the need to protect national security, but with a presumption of publication. Only by having the interpretations of the law made public can the FISC function properly and the surveillance it authorizes retain its legitimacy. There can be no room for secret law in a healthy democracy.

Only once these steps are taken can the public begin to reestablish trust, both in the online services they use and in the government that is protecting them. The Review Group should start the country toward that important reconciliation by making these recommendations to the Director of National Intelligence and the President.

3 Structural Reforms to the FISC

Improving the transparency of the Foreign Intelligence Surveillance Court is necessary, but not sufficient, to solving today's problems. The Court needs structural reform to retain legitimacy and help companies that are the recipients of orders. The inclusion of an opposing counsel that would represent the interests of providers and subjects of FISA demands in cases involving significant statutory or constitutional interpretations would ensure that the FISC is fully apprised of the arguments that would be marshaled both in support of and in opposition to the government's position.

Having such a counsel would transform the FISC from a one sided affair – in which the judges themselves admit they are completely at the mercy of the government to explain the very program that they are asking the court to approve – into a much more adversarial process that would serve to protect the privacy of Americans much better than the current system. An institutional adversary that would litigate weighty legal issues before the FISC would help inform the judges, encourage self-restraint by those seeking surveillance, provide an opposing point of view to counter the claims of the government, and could (if they possessed the right experience) provide much-needed, objective technological expertise for the court – something the court would undoubtedly benefit from given rapid technological change.

This sort of reform to the FISC is vitally important from a commercial perspective as well. Large companies who receive orders from the Court often fight the orders that they feel are over-broad or illegal, on behalf of their users. Doing so inevitably requires the expenditure of significant human and monetary resources. Small companies, however, do not generally have the necessary resources to fight those battles and are therefore left with an

uncomfortable decision on either side – to turn over data on users when it seems inappropriate, or risk the entire company in defying the government.[6] An institutional adversary would help give companies at least a basic assurance that there are appropriate checks and balances around the issuance and oversight of FISA demands. Smaller companies could therefore better trust that their users are properly protected without expending massive resources.

4 Protections for Americans

While transparency and procedural fixes are required, there is a need to begin a reexamination of the substantive surveillance laws in our country. Any suggestion for substantive change is tentative today because a lack of transparency means that it is impossible to form firm conclusions when weighing the costs and benefits of our current system. However, there are sufficient grounds today to say that a high-level policy review of key provisions is needed. Many have already concluded how best to do so and their arguments are persuasive in some areas. Some of those are presented here, but necessary details are still lacking.

There are concerns with how the NSA is using section 215 of the USAPATRIOT Act as a means of gathering vast amounts of metadata to later analyze for connections. Even the original author of the law has said that this use was not what was intended when the law was written.[7]

The privacy impacts of collecting this sort of information are far from negligible. While some argue that the information involved is only metadata, and therefore deserving of less protection, the reality is that there is much that can be learned about a person through looking at a list of who they call, email, or otherwise associate with, not to mention whatever other pieces of information the NSA has been able to gather through the use of section 215.

[6] *See, e.g.*, Nicole Perlroth, *As FBI Pursued Snowden, an E-Mail Service Stood Firm*, N.Y. Times, Oct. 2, 2013.

[7] Jim Sensenbrenner, Op-Ed., *How Obama Has Abused the Patriot Act*, L.A. Times, Aug. 19, 2013.

It is time to call for an exploration of the important questions raised by this practice. The nation must now decide if the national security benefits of mass collection outweigh the privacy harms, and whether the collection authority under section 215 should be modified. While considering that balance, it will be important to take into account the chilling effects that can arise from broad-based surveillance, even if only of metadata. Such effects could lead to considerable adverse effects to online commerce, a young industry that has been a great engine of the economy even during uncertain times.

Section 702 of the FISA Amendments Act is the other area of the law that may benefit from careful examination. This provision has been the subject of considerable controversy this summer, including when the PRISM program was originally billed as a "backdoor" directly into the servers of many major online service providers.[8] While further reporting corrected that initial image and showed that PRISM was instead more likely the name for a database that held information collected from those companies under authorized process, to a large degree that damage to companies' reputations was already done.[9] The law as it currently stands has some worrisome aspects that bear careful consideration for their impacts on the privacy of Americans and their commercial implications.

One procedure that the press reported was used by the NSA is the gathering of Americans' communications in the process of targeting a foreigner, keeping that communication, and returning to read it later without first obtaining a warrant.[10] This sort of "loophole" has implications for companies that offer online services. Warrantless interception of Americans' online content is an issue of great concern in today's marketplace. Problems with the Electronic Communications Privacy Act have for a number of years permitted the government to read Americans' emails and other online message

[8] *See* Glenn Greenwald, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, June 6, 2013.

[9] *See* Dominic Rushe, *PRISM scandal: tech giants flatly deny allowing NSA direct access to servers*, The Guardian, June 6, 2013.

[10] James Ball, *NSA loophole allows warrantless search for US citizens' emails and phone calls*, The Guardian, Aug. 9, 2013.

for criminal investigations, all without a judge's approval.[11] People who store data online want to know that their information will be kept safe from government intrusion unless a judge has signed off on it. That is why a coalition of companies, public interest groups, and academics is working to have Congress amend ECPA.[12] This loophole in section 702 may similarly be an area that deserves study.

These are just a few suggestions for ways in which the Administration might go about assuring the trust of Americans in both the government and the online services that so many of them use every day. Considering changes along these lines will increase confidence while still maintaining important investigatory resources to allow NSA analysts to do their difficult and important jobs. The Review Board should make their recommendations with this in mind.

5 Protections for Non-Americans

These surveillance programs are not confined to having purely domestic impacts. We must as a country look carefully at the international implications of our actions. It is important to realize that American Internet companies who do business online do not distinguish or care about whether potential users and customers are American. People around the world today, however, are very concerned about what happens to their data when they choose to use a US-based service. Companies would like to say that they are good stewards of privacy, but the fact remains that companies with a presence in the US will be subject to turning over users' data to the government regardless of how hard they fight it. This is already having the effect of turning away customers and potential customers, and may someday have the effect of turning away companies themselves.

Even in a noncommercial sense, we cannot continue to act as if Americans are the only ones affected by the NSA's actions in this area. In a globalized world and on a global network, it is simply untenable to treat those who

[11] Electronic Communications Privacy Act, 18 U.S.C. 2703
[12] Digital Due Process Coalition, http://digitaldueprocess.org/.

by whatever fortune were born outside our borders as if they have no rights whatsoever. They are no less deserving of privacy than Americans are. America's legitimacy abroad and our place in the global conversation about Internet governance are also dangerously at stake. Some may say that other countries are being hypocritical and that "everyone does the same," but at the end of the day perception of this matter for the US government and companies may be as important as reality.

While the courts have consistently held that the Fourth Amendment does not protect foreigners abroad, the judiciary's interpretation of our civil liberties set a floor and not a ceiling. As a starting point, the administration could look to the International Covenant on Civil and Political Rights, to which the United States is a signatory, which contains language on citizens' rights to privacy.[13] While the Covenant does not contain precise enough language to base a policy on, it may be a suitable basis to begin from. There is no reason why these proposed protections must make finding and tracking terrorists impossible (and indeed nobody would wish such an outcome), of course, but basic privacy restrictions can live appropriately alongside security.

6 Conclusion

The people within the intelligence community who implement these laws are hard-working civil servants tasked with a difficult job and to whom the country has given great tools. The intelligence community as a whole, however, has shown that they will use every tool given to them, sometimes beyond its breaking point. That is why it is so important to make sure that those tools are appropriate, balanced, and overseen by both officials from all three branches of government. It is to that end that CCIA respectfully offers these comments.

[13] International Covenant on Civil and Political Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.