Computer & Communications Industry Association

Tech Advocacy Since 1972

Questions for the record to

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 Klobuchar:

Q: Mr. Black, in your testimony, you discuss the importance of allowing companies to disclose the demands they receive from the Government for bulk collection of customer data. Why is this level of transparency important? Can you provide some concrete examples of the way this would help these companies?

A: As in many other industries, consumer trust is vital to Internet services companies such as our members. Users today want to know how and why data about them is shared, because data today can reveal so much about a person. That is why CCIAs members and nearly every other company operating online today have privacy policies detailing what information they collect, how it is used, and with whom it is shared, so that consumers who want to be informed can do so. In fact, in a poll conducted recently by Benenson Strategy Group and American Viewpoint on behalf of CCIA, 65% of respondents reported that they read privacy policies as a means of understanding their privacy online better. What is good for the consumer is even better for the citizen, as citizens cannot simply choose to live under a different surveillance regime with a simple click. Without this kind of transparency, there can be no larger conversation about the ongoing use of surveillance in our country.

Trust is also the more parochial answer to your question. There are those who now presume that Silicon Valley and Ft. Meade are simply two sides of the same coin. We know that this does not represent the truth. Transparency about the numbers of requests will give customers data instead of speculation to base their decisions on. In this it is also essential that the data be as exact as possible. In a situation where suspicion is as high as it is right now, hiding behind large ranges of numbers in transparency reporting risks doing as much damage as reporting no numbers at all. The question will always be what do they have to hide?

Q: Is there an alternate arrangement that could be made between the government and these companies to allow rapid access to necessary data while not engaging in bulk collection?

A: With due respect, Senator, we believe that where the data lives at the end of the day is the wrong question. If the NSA is going to be engaging in three-hop contact chaining using this information, they will be sweeping in information about millions of Americans. The government has claimed that this sort of information carries no privilege of privacy under the Fourth Amendment. Whether or not that is true – and we are finally starting to see the judiciary come directly into contact with this idea and finding it repugnant to the Constitution – we should be asking ourselves whether large-scale analysis of information about Americans communications is something a democratic government should be engaging in.

Wherever the data lives, the fact will remain that the bulk phone records analysis program presents a grave risk to Americans privacy, and produces dubious national security benefits, as was pointed out last month by both Judge Leon of the DC District Court, and the Presidents own Review Group Report.

2 Grassley:

Q: In your prepared testimony you criticized U.S. national security policy for operating on the presumption that U.S. citizens online deserve protection from unwanted surveillance, while others do not. What new legal protections do you suggest U.S. law recognize for foreign terrorists abroad? For example, do you believe the government should be required to get a warrant to spy on a terrorist sitting in an internet caf in Europe or Asia? Shouldnt our government be doing everything within the current law it can to fight terrorists, as opposed to giving them new legal rights?

A: CCIA does not yet have concrete suggestions for the protections due to non-US citizens, but we do believe this subject should be one that Congress closely contemplates. Your question, Senator, focuses exclusively on what terrorists must be hiding abroad and the implications of giving them legal rights. What your questions ignores, however, are the billions of non-terrorists living their lives abroad. Billions of ordinary people over whom our government claims great power through its indiscriminate surveillance. Billions of potential customers for American Internet companies, along with the global customers of American products being sold online, who may now have second thoughts. Swiss data hosting providers, to provide an example, are experiencing growth in the hundreds of percent per year as companies migrate away from US-provided products. Cisco, on its most recent earnings call, made clear that it is seeing a dramatic decrease in sales in the very countries who are most upset about the Snowden disclosures. A recent survey of purchasing intention made clear that US-sourced products already face a significant competitive disadvantage due to the surveillance disclosures. If we continue to treat all foreigners as fair game for unlimited surveillance, US-based companies will not be able to sell to them. The source of our national security flows not only from surveillance, but also from the vitality of our economy, and our current choices on how we treat non-nationals is damaging our economic competitiveness and therefore our national security. Many leading members of Congress have long called for more cost / benefit analysis in evaluating government programs. Here, we are pointing out that there are massive economic and security costs to sweeping worldwide surveillance, that need to be, and have not yet, been fully understood.

The danger is not just to trade, but also to the idea of the open Internet as a vehicle for democracy and freedom around the world. Some of our members recognized this when they wrote the Global Government Surveillance Princi-

ples, particularly the principle of Respecting the Free Flow of Information. In response to the NSAs blanket surveillance of people from around the world, there have been calls to disrupt the non-geographical nature of the Internet by forcing data to live in certain places. These calls directly challenge the idea of a borderless Internet and threaten the free flow of data.

Nobody has suggested, and nor would we ever suggest, that surveillance is not appropriate over some small percentage of the worlds people. Even other countries agree with this fact. Of course the NSA must be able to analyze and track actual terrorists who aim to inflict imminent damage upon the United States. However, that does not mean that some measure of due process for the people of the world against our overwhelming ability to gather information on them cannot exist. Surely the country that put men on the moon, invented the technical underpinnings of the Internet, and created the Marshall Plan is capable of the vision required to meet this challenge.