

United States Senate

WASHINGTON, DC 20510

January 9, 2014

President Barack Obama
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear Mr. President:

We write with regard to the report of the Review Group on Intelligence and Communications Technologies, issued in December 2013. As members of the Senate Select Committee on Intelligence, we commend the Review Group for its thorough report and thoughtful recommendations, and we urge you to consider those recommendations seriously as you continue your own evaluation of potential reforms to U.S. surveillance programs. The Review Group was tasked with six priorities, the first of which was “Protecting The Nation Against Threats to Our National Security.” The Review Group’s report clearly emphasizes this priority while also taking into account other important priorities like protecting the privacy and civil liberties of U.S. citizens while respecting and strengthening the rule of law.

We wish to highlight some of the Review Group’s recommended reforms with which we agree and for which we have been advocating for some time, particularly the group’s recommendations dealing with reform of government surveillance conducted under Section 215 of the USA PATRIOT Act.

First, we wholeheartedly agree with the Review Group that as a general rule, “the government should not be permitted to collect and store mass, undigested, non-public personal information about US persons for the purpose of enabling future queries and data-mining for foreign intelligence purposes.” Accordingly, the Review Group recommends the termination of the storage of bulk telephony metadata under Section 215 of the PATRIOT Act, and a transition to a system in which phone companies provide specific customers’ records to the government only when the government has a demonstrated need and an appropriate court order or emergency authorization.

The Review Group’s recommendations would enable the government to collect the phone records of individuals connected to terrorism by directing specific queries to telecom providers, instead of collecting the phone call records of huge numbers of law-abiding Americans. This was the intent of the original USA PATRIOT Act and is consistent with a legislative proposal that was first included in the Senate-passed version of the USA PATRIOT Improvement and Reauthorization Act (S. 1389) in 2005, which was passed by unanimous consent. A version of this proposal has been included in multiple pending bills that we all support; a stand-alone proposal introduced by Sen. Udall (S. 1182), bipartisan comprehensive surveillance reform legislation introduced by Sen. Wyden (S. 1551), and the bipartisan and bicameral surveillance reform legislation introduced by Sen. Leahy and Rep. Sensenbrenner (S. 1599).

Critics of the Review Group’s proposal for Section 215 reform make several arguments in opposition to such reform. Each of these arguments is flawed, and we will address them in turn.

In the past, NSA officials have claimed that they need to acquire huge amounts of phone records in order to identify people in contact with suspected terrorists. But, as the Review Group suggests, telecom

providers already retain their customers' phone records, and the records of anyone in contact with a suspected terrorist can already be obtained using regular Foreign Intelligence Surveillance Court orders. Additionally, the Review Group notes that the government currently only collects a fraction of the call data maintained by telecoms. Having the government go directly to the carriers with specific FISA Court orders or emergency authorizations, instead of searching a gigantic but still incomplete database of Americans' telephone calls, would dramatically reduce the total volume of information held by the government, but the universe of information available for these terrorism-related searches would increase significantly.

Telecom providers generally already hold this information for at least 18 months to comply with FCC regulations, and some companies hold data longer for their own business purposes. This proposal could therefore be implemented without requiring telecom providers to hold data for a longer period of time than they normally do, which, we understand, is a primary concern of the telecom providers themselves. Frankly, the NSA has not demonstrated that there is any need to require the telecom providers to hold data for longer than they normally would. Indeed, the NSA has never adequately explained how it determined that it should hold bulk telephony metadata in its own database for five years, as it currently does, nor has the NSA explained why it now believes that a three-year retention period under the Section 215 program would be sufficient in the future. We have asked intelligence community officials on numerous occasions to identify examples of cases in which they have derived unique value from NSA's bulk metadata collection program using records that were no longer held for normal business purposes by the telecom providers. We have yet to receive an answer.

NSA officials have also stated that analysts need to be able to access the phone records of suspected terrorists in a timely manner. We agree. As the Review Group stated, while "there might be problems in querying multiple, privately held databases simultaneously and expeditiously...it is likely that those problems can be significantly reduced by creative engineering approaches." Again, we agree, especially because the NSA already deals with these issues in the records it currently receives from carriers.

Some have raised valid privacy concerns about the retention of customer records by telecoms. Again, we see no reason to require telecoms to retain customer records any longer than they do currently. And we believe the way to restore Americans' constitutional rights is to end the practice of vacuuming up the phone records of huge numbers of innocent Americans every day and permit the government to obtain only the phone records of people actually connected to terrorism or other nefarious activity. As you know, the NSA performs queries of the bulk telephony database when there is a reasonable articulable suspicion about a target. Adding a layer of court review to these queries will not substantially overwhelm the FISA Court, or inhibit the speed of an investigation. Only 288 "selectors" were queried by the NSA in 2012, and the law already allows for emergency authorizations under urgent circumstances.

Finally, we agree with the Review Group's conclusion that "information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders." We have yet to see any evidence that the bulk phone records collection program has provided any otherwise unobtainable intelligence. The Intelligence Community notes that the massive collection of phone records under Section 215 has provided some relevant information in a few terrorism cases, but it is still unclear to us why agencies investigating terrorism do not simply obtain the specific information they need directly from phone companies as the Review Group suggests.

Mr. President, we agree with your recent comment that "just because we can do something doesn't mean we necessarily should." While it might be more convenient for the NSA to collect phone records in bulk

rather than directing individual queries to the various phone companies, convenience alone does not justify the collection of the personal information of millions of ordinary, innocent Americans, especially when the same or more information can be obtained in a timely manner using less intrusive methods.

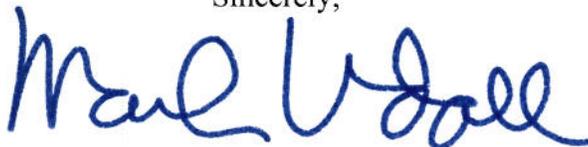
In addition to reforms to the Section 215 bulk telephony metadata collection program, we urge you to seriously consider a number of other key reforms identified in the Review Group's recommendations, such as:

- Requiring probable cause to search through the contents of communications collected under Section 702 of the FISA Amendments Act to find information about U.S. persons. This recommendation echoes a reform we have advocated to prohibit intelligence agencies from using collection authorities aimed at foreigners to conduct warrantless searches for the phone calls and emails of individual Americans. Currently, a gap in the law known as the "backdoor searches" loophole permits the government to make an end run around traditional constitutional warrant protections.
- Creating a "Public Interest Advocate" to represent privacy interests before the FISA Court. We have advocated legislation to create a similar authority to present an opposing view in cases where the FISA Court is called upon to interpret U.S. surveillance laws or the Constitution. We also support a process for making significant FISC decisions public, and thereby reducing the government's reliance on a secret body of surveillance law.

While we have served on the Intelligence Committee for varying lengths of time, all three of us can attest that our nation's intelligence professionals are overwhelmingly dedicated and patriotic men and women who make real sacrifices to help keep our country safe and free. We believe that they should be able to do their jobs secure in the knowledge that their agencies have the trust and confidence of the American people. This trust has been undermined by overly intrusive domestic surveillance programs and misleading statements made by senior officials over a period of many years. Your Review Group recognized that the way to rebuild this public trust is to reform surveillance law and end the dragnet surveillance of ordinary Americans in a way that preserves intelligence agencies' ability to collect information that is actually necessary for the preservation of American security.

If you or your administration determines that legislative changes are needed in order to accomplish these goals, we stand ready to work with you to provide the legislative assistance you need. However, we believe you have the authority to make many of these changes now, and we urge you to do so with reasonable haste to protect both our national security and the personal rights and liberties of U.S. citizens. We look forward to working with you and our Senate colleagues to achieve this.

Sincerely,



Mark Udall
U.S. Senator



Ron Wyden
U.S. Senator



Martin Heinrich
U.S. Senator