# Opening Statement of Senator Feinstein
## Judiciary Committee Hearing on President's Review Group on Intelligence and Communications Technologies
## Tuesday, January 14, 2014

Thank you, Chairman Leahy.

I'd like to welcome the panel and appreciate their being here today. For the information of other Members, the Intelligence Committee met with three of the Review Groups members in a hearing last week – Mr. Sunstein, Mr. Swire, and Mr. Stone. It's good to see you again, along with Michael Morell and Richard Clarke.

I noted then, and want to re-iterate now, that there are a number of constructive recommendations in their report, in particular with respect to the need to improve the security clearance process, better protect information in the government's hands, and strengthen whistleblower protections for Intelligence Community employees.

Many of these provisions, as well as measures providing for additional transparency into intelligence collection programs where possible, are included in the FISA improvements legislation and the Fiscal Year 2014 intelligence authorization bill reported favorably by the Senate Intelligence Committee last fall with strong bipartisan votes. (The FISA Improvements bill passed 11-4 and FY 14 Intelligence Authorization bill passed 13-2.)

However, I am concerned by a number of other findings and recommendations in the report, and want to repeat briefly some of my concerns and some of what we discussed last week.

First and foremost is the recommendation to replace the current NSA call records program operated under the Business Records provision of FISA with one where the

phone companies or a private third party hold the records and the government must go to the FISA Court each time it seeks to query this data.

The Intelligence Committee looked at this approach in our deliberations concerning the NSA program both before and after the program was leaked to the media and found that it likely would increase significantly the cost of the program to taxpayers (at least in the short-term); require new statutes be passed to, among other things, compel private parties to store the metadata and new network infrastructures to be developed for the government to receive and process the data; cause a delay of up to several days in the government's ability to obtain information in response to a query; and do precious little to enhance privacy protections, as the data would still be stored, but by one or more private entities that are not subject to the same oversight and accountability requirements as NSA.

Moreover, it should say something that this alternative approach is strongly opposed not only by the telecommunications providers but also by privacy groups who oppose requiring the telecom companies to hold and search this data.

The Review Group acknowledges in their report that there has been no finding of any "official efforts to suppress dissent or any intent to intrude into people's private lives without legal justification." Last week, members of the Review Group testified to the Senate Intelligence Committee that their report has been misunderstood by the media and that they believe the NSA program has value and should be maintained, albeit in a different form.

Significantly, in an op-ed published in the *Washington Post* on December 27th, one member of the Review Group, Mr. Morell, wrote to "correct the record" and stated that the NSA program "would likely have prevented 9/11. And it has the potential to prevent the next 9/11." In fact, Mr. Morell calls for an expansion of the program.

When I raised this op-ed with the three Review Group witnesses, they agreed with Mr. Morell's comments, and I hope to ask all the panelists today to say for the record whether they believe the 215 program may have been able to alert the government to the 9/11 plot, and that it could prove instrumental in thwarting a future attack.

Let me note here two other areas that we discussed last week.

First is the Review Group's recommendation number 15, which matches a section in the SSCI FISA Improvements Act. We both believe that the NSA should have additional, limited statutory authority to continue surveillance when a known counterterrorism target outside the United States travels to the United States. Under current law, NSA must stop surveillance that has been lawfully conducted, either under Section 702 of FISA or under Executive Order 12333, until the government can go to the Court for an individual warrant under Title I of FISA. That process can take days, and occurs precisely when the individual may be in position to carry out an attack.

Secondly, the Review Group's recommendations 7 through 10 address public transparency with respect to the government's use of national security letters, FISA orders, and similar tools used in national security investigations. Recommendation 9 in particular states that companies who receive national security letters or FISA orders and produce information as a result should be allowed to periodically disclose to the public information on the numbers of requests and related general information. A number of technology companies, including Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo, and others, have sought this authority – not to disclose specifics of whose account information is being sought any why, but to provide general statistics so they can publicly describe and defend their cooperation with the government.

The companies have noted that they are losing business to foreign competitors because of suspicions about the extent of their cooperation with the government. I know Sen. Franken has introduced legislation to provide companies with the authority

they seek and I'd like to work with Sen. Franken to increase transparency in this area because I believe it is possible to do so in a way that still protects national security.

Thank you, Mr. Chairman, for the opportunity to make these opening remarks.