Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing on the Report of the President's Review Group
on Intelligence and Communications Technologies
January 14, 2014

Today, we will hear from the President's Review Group on Intelligence and Communications Technologies. This is the first time they have appeared together publicly since their ground-breaking report was released last month.

The Review Group's report addresses some of the weightiest issues that we will confront in the coming years. Technology will continue to advance in ways we cannot even imagine. More and more data will be created by all of us as each day passes. When should our government be allowed to collect and use that data? To what extent does the massive collection of data improve our national security? And what will the answers to these questions mean for privacy and free expression in the 21st century?

All three branches of government are grappling with whether to allow the NSA's dragnet collection of Americans' domestic phone records to continue, and we are finally doing so with full public participation in that debate. The Review Group makes an important contribution to this conversation. While we must always consider ongoing threats to national security, the report urges policymakers to consider all of the risks associated with this and other intelligence activities: the risk to individual privacy, to free expression and freedom of association, to an open and decentralized Internet, to America's relationships with other nations, to trade and commerce, and to maintaining the public trust.

The most critical factor in deciding whether to conduct any particular intelligence activity is an assessment of its value. This is particularly important in evaluating the phone records program conducted under Section 215 of the USA PATRIOT Act. As I have said repeatedly, I have concluded that this phone records program is not uniquely valuable enough to justify the massive intrusion on Americans' privacy.

The Review Group likewise concluded that the program has not been essential, saying: "The 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." And a few pages later: "Section 215 has generated relevant information in only a small number of cases, and there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony meta-data program."

In addition to the concerns about the utility of this program, I also question its constitutionality. Although the Review Group report is careful not to make a legal judgment about the program, it acknowledges the ramifications of the extraordinarily broad legal theory on which the program is based. The report explains that nothing in Section 215, as interpreted by the FISA Court, would preclude the mass collection of Americans' personal information beyond phone records. In

addition, one member of the Review Group has publicly concluded that the program as currently constituted violates the Fourth Amendment.

The privacy implications of this sort of massive surveillance in the digital age cannot be overstated, and the Review Group's report provides some valuable insights. Some argue that there is nothing wrong with the NSA's program because it is "just collecting metadata." But the report reminds us that keeping a record of every phone call an individual has made over the course of several years "can reveal an enormous amount about that individual's private life." It further explains that in the 21st century, revealing private information to third party services "does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life." The report appropriately questions whether we can continue to draw a rational line between metadata and content. This is a critically important question given that many of our surveillance laws depend upon the distinction between the two.

These insights are also important as we take up reforms to the National Security Letter statutes. Using NSLs, the FBI can obtain detailed information about individuals' communications records, financial transactions, and credit reports without judicial approval. Recipients of NSLs are subject to permanent gag orders. Senator Durbin and I have been fighting to impose additional safeguards on this controversial authority for years – to limit their use, to ensure that NSL gag orders comply with the First Amendment, and to provide recipients of NSLs with a meaningful opportunity for judicial review. The Review Group report makes a series of important recommendations to change the way National Security Letters operate. These recommendations have not generated the same attention that other issues have, but they should.

The report also recommends creating an institutional Public Interest Advocate at the FISA Court, a proposal that I strongly support. I am concerned that merely allowing for an amicus to participate at the FISA Court from time to time will neither improve the substantive outcome of the proceedings, nor rebuild public confidence in the process.

I suspect none of us on this Committee agrees with all of the report's recommendations, but we are privileged to hear directly from this distinguished panel today. They have written a thoughtful report worthy of careful consideration, and I applaud the members of the Review Group for their public service.

The stakes are high. This is a debate about Americans' fundamental relationship with their government – about whether the government should have the power to create massive databases of information about its citizens. I believe strongly that we must impose stronger limits on government surveillance powers – and I am confident that most Vermonters, and most Americans, agree with me. We need to get this right.

# # # # #