JOINT TESTIMONY OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE DEPARTMENT OF JUSTICE

Robert S. Litt, General Counsel, Office of the Director of National Intelligence

J. Bradford Wiegmann, Deputy Assistant Attorney General, National Security Division, United States Department of Justice

Senate Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

November 13, 2013

Good afternoon Chairman Franken, Ranking Member Flake, and distinguished members of the Subcommittee. We appreciate this opportunity to appear before you today to discuss the Intelligence Community's efforts to increase transparency concerning certain intelligence collection activities under the Foreign Intelligence Surveillance Act (FISA). We will also offer some initial views on S.1621, the Surveillance Transparency Act of 2013.

The Administration's Efforts To Increase Transparency of FISA Activities

Recent unauthorized disclosures have sparked an ongoing public dialogue about intelligence collection activities, particularly those conducted under FISA. Increasing transparency regarding how some of these activities are conducted is important to ensuring that this dialogue is grounded in facts. As we have publicly explained over the last several months, bulk collection of telephony metadata under the business records provision of FISA (known as Section 215), and other collection activities targeting non-U.S. persons overseas under Section 702 of FISA, are authorized by law, have been approved by the FISA Court, and have been overseen by all three branches of our government. The extensive information we have released to the public about these activities over the last several months demonstrates the rigorous oversight under which these programs operate.

We recognize the public interest in understanding how the Intelligence Community uses the legal authorities provided by Congress to conduct surveillance and gather foreign intelligence. It is appropriate for Congress to examine whether these legal authorities, as implemented by the Executive Branch, strike the appropriate balance between privacy and national security. We welcome the opportunity to discuss ways to make more information about intelligence activities conducted under FISA available to the public in a responsible way. At the same time, we are mindful of the need not to disclose information that our adversaries could exploit to evade surveillance and harm our national security. There is no doubt that the recent unauthorized

disclosures about our surveillance capabilities risk causing substantial damage to our national security, and it is essential that we not take steps that will increase that damage.

In keeping with this balance, in June the President directed the Intelligence Community to make as much information about the Section 215 and Section 702 programs available to the public as possible, consistent with the need to protect national security and sensitive sources and methods. Since then, the Director of National Intelligence has declassified and publicly released substantial information in order to facilitate informed public debate about these programs. Among other things, the Government has declassified and disclosed the primary and secondary orders from the FISA Court that describe in detail how the bulk telephony metadata collection program operates and the important restrictions on how the data collected under the program are accessed, retained, and disseminated. We have also declassified and released to the public numerous FISA Court opinions and orders concerning the two programs, including detailed discussions of compliance issues that have arisen during the programs' history and the Government's responses to these incidents. We have also released extensive materials that were provided to the Congress in conjunction with its oversight and reauthorization of these authorities.

Our efforts to promote greater transparency through declassification and public release of relevant documents are not yet complete. We will continue to declassify and release more information, while carefully protecting information that we cannot responsibly release because of national security concerns. These ongoing declassification efforts are an important means of enhancing public confidence that the Intelligence Community is using its legal authorities appropriately, which has unfortunately become increasingly necessary in the wake of confusion, concerns, and misunderstandings caused by the recent and continuing unauthorized disclosures of classified information.

As part of our ongoing efforts to increase transparency, the Director of National Intelligence has also committed to providing annual public reports that include nationwide statistical data on the Intelligence Community's use of certain FISA authorities. Specifically, for each of the following categories of FISA and related authorities, the Intelligence Community will release to the public the total number of orders issued during the prior twelve-month period and the number of targets affected by these orders:

- FISA orders based on probable cause (Titles I and III and Sections 703 and 704 of FISA).
- Directives under Section 702 of FISA.
- FISA Business Records orders (Title V of FISA).
- FISA Pen Register/Trap and Trace orders (Title IV of FISA).
- National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. § 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709.

This information will enable the public to understand how often the Intelligence Community uses these authorities nationwide, how many persons or entities are targeted by these efforts, and how these figures change over time. The Director of National Intelligence has concluded that providing this information on a nationwide basis is an acceptable course in light of the goal of public transparency, without unduly risking national security.

We also understand the concerns that specific companies have expressed as to their ability to inform their customers of how often data is provided to the Government in response to legal process. In light of those concerns, we have authorized companies to report within certain ranges the total number of federal, state, and local law enforcement and national security legal demands they receive on a nationwide basis, and the number of user accounts affected by such orders. This allows companies to illustrate that such process affects only a tiny percentage of their users, even taking all of that process together, and thus to refute inaccurate reports that companies cooperate with the Government in dragnet surveillance of all of their customers. At the same time, this approach avoids the disclosure of information to our adversaries regarding the extent or existence of FISA coverage of services or communications platforms provided by particular companies.

The scope of the voluntary disclosures by the Executive Branch concerning sensitive intelligence collection activities carried out under FISA is unprecedented. We hope that the information we have released, and will continue to release, will allow the American public to understand better how our intelligence collection authorities are used. We also hope the public will see the rigorous oversight conducted by all three branches of government over our intelligence activities, which helps to ensure that those activities protect national security, balance important privacy considerations, and operate lawfully.

Preliminary Views on S.1621, the Surveillance Transparency Act of 2013

Turning to S.1621, we have reviewed the bill with both transparency and national security concerns in mind, and we share the goal of the legislation of providing the public with greater insight into the Government's use of FISA authorities. Many of the bill's provisions are consistent with the steps we have taken to report more information to the public while protecting intelligence sources and methods. Other provisions, however, raise significant practical or operational concerns, as we shall explain. We hope that we can work with you to find common ground on this bill, and we would be happy to provide technical assistance to address the concerns we have identified.

Section 2

Section 2 of the bill includes enhanced reporting requirements for the use of FISA authorities pertaining to electronic surveillance, pen register and trap and trace devices, business records, and Title VII. Some of these reporting requirements we fully support, but others would be difficult if not impossible for the Government to implement.

We support the provisions requiring reporting of the total number of applications made for orders pursuant to Titles I, IV, and V of FISA, including reporting on the total number of such orders granted, modified, or denied. Likewise, we support the provisions requiring reporting of the total number of directives issued under Section 702 and orders granted under Sections 703 and 704. And for each of these authorities, we would support provisions requiring the Government to report the number of targets affected by such orders, information we have already committed to provide.

We have significant concerns, however, about provisions that would require reporting exact numbers or estimates of the number of individuals and of U.S. persons whose information is acquired from surveillance conducted pursuant to these authorities but who are not themselves targets of the surveillance. We can compile and report statistics concerning the *targets* of FISA collection activities, but it would be difficult if not impossible to do so for individuals whose communications or information may be incidentally collected.

Identifying the number of persons who are "subject to surveillance" under FISA would require reviewing, in detail, all of the information we collect and then manually determining every unique person who is party to an intercepted communication. That is, we would have to review all of the communications collected concerning a foreign intelligence target and attempt to determine who else is involved in each communication and whether each such individual is someone who has already been counted or, instead, is a new individual communicating with the target, which will often be an impossible task. Moreover, doing so would run contrary to the culture and mission of the Intelligence Community, which is to discover among the communications acquired those of foreign intelligence value and disregard those that hold no such promise. What's more, we would then have to determine which of those individuals are U.S. persons—although often there is no reliable way to determine that and attemping to do so would further detract from the privacy of the person incidentally collected.

Many communications acquired under FISA are never reviewed by analysts or at least do not become the focus of any attention. When analysts do review them, they focus on identifying material that is of foreign intelligence value. It would be difficult if not impossible to count the number of persons whose communications may have been incidentally obtained in this context, let alone attempt to identify which of those individuals were U.S. persons, as the bill would require. The same is true of collection via the FISA-authorized pen register/trap and trace program, which collects metadata associated with telephone calls or electronic communications of a target .

Moreover, attempting to identify the numbers of persons or U.S. persons whose communications or information may be incidentally collected would, in practice, have a privacy-diminishing effect directly contrary to the aims of this bill. Attempting to make this determination would require the Intelligence Community to research and review personally identifying information solely for the purpose of complying with the reporting requirements, even if the information has

not been determined to contain foreign intelligence. Such an effort would conflict with our efforts to protect privacy.

In sum, reporting on numbers of targets is feasible; it is consistent with our efforts to protect privacy; and it provides information that is valuable and relevant to the public, i.e., the numbers of individuals whom the Government has purposefully sought to monitor. Reporting on numbers of individuals affected by incidental collection is operationally difficult, if not impossible, and attempting to do so would require otherwise unnecessary intrusions on personal privacy. We therefore strongly urge that the bill's disclosure requirements only apply to the number of individuals who are targets of intelligence collection, and not to the number of individuals whose communications may have been incidentally collected.

Section 3

Section 3 of the bill would amend FISA to allow a person (including a company) who received a FISA order to disclose to the public every six months, among other things, the total number of orders or directives received under each specific FISA authority, the percentage or total number of orders or directives complied with, in whole or in part, and the total number of individuals, users, or accounts whose information of any kind was produced to the Government, or was obtained or collected by the Government, under an order or directive received under that specific authority.

We recognize the importance of allowing companies to provide transparency to their customers, and we have taken steps to allow them to do so. The Government has agreed to permit companies to report, in certain ranges, the aggregate number of criminal and national security-related orders they receive from federal, state, and local government entities combined. We have also agreed to permit companies to report the number of user accounts affected by such orders. We believe that those measures will serve the overriding interest of the public: these measures will show that the sum total of all such process affects only a tiny fraction of the companies' user accounts. At the same time, the aggregated nature of such disclosures minimizes the potential harm to national security. We could support legislation that would mandate such disclosures as a matter of law.

We do have significant operational and national security concerns with the detailed, company-by-company disclosures that the bill, as currently written, would authorize regarding legal demands for interception of communications. More detailed company-by-company disclosure threatens harm to national security by providing a roadmap for our adversaries on the Government's surveillance capabilities relating to services or communications platforms offered by any particular company. This information would be valuable to our adversaries, who could derive a clear picture of where the Government's surveillance efforts are directed and how its surveillance activities change over time, including when the Government initiates or expands surveillance efforts involving specific providers or services that adversaries may have previously

considered "safe." There is a limit to how much we can say about this in an open hearing, and we would be happy to provide more detailed information in a classified setting. But the basic point is straightforward: disclosing information in a manner that would permit our adversaries to deduce our specific collection capabilities and shortcomings would harm national security by allowing those adversaries to switch providers and services in order to avoid our surveillance. .

Already, our Intelligence Community knows that our adversaries purposely gather such information to assess our capabilities and evade surveillance. Providing them the information on our collection capabilities that they are working so hard to gather could significantly and irreparably harm our intelligence collection efforts. So, while we fully support nationwide, aggregate disclosure in the interests of transparency, as well as certain generic company-level reporting, we are concerned that the bill's provisions requiring more detailed company-specific disclosure would pose a risk to national security.

As we have explained, the Intelligence Community has carefully considered how to disclose FISA statistics in a way that will educate the public while protecting sources and methods associated with FISA collection activities. We believe that the nationwide statistics the Government has committed to provide, and the more general data the Government has authorized companies to disclose, strike the right balance. This level of reporting would demonstrate how various FISA authorities are used by the Government in the aggregate and also allow the public to see, in general, the number of subscriber accounts that are accessed through all forms of legal process, without compromising our national security authorities.

Again, thank you for the opportunity to appear before you today. As we said at the outset, we are entirely supportive of the goal of the Surveillance Transparency Act, to increase public understanding of the ways in which we use our legal authorities to conduct surveillance and oversee that use to ensure that it complies with the law. While we have concerns about some of the specific provisions, we look forward to continuing to work with the Subcommittee on improving this important transparency legislation. We would be pleased to answer any questions.