Senator Grassley's Questions for the Record from

Senate Committee on the Judiciary

"Hearing on the Report of the President's Review Group on Intelligence and Communications Technologies"

January 14, 2014

Questions for the President's Review Group on Intelligence and Communications Technologies

1. Application of the Privacy Act to Non-United States Persons

The Review Group's report recommends that the intelligence community apply the Privacy Act of 1974 to non-U.S. persons. This is currently the policy of the Department of Homeland Security (DHS). However, a former Director of the National Counterterrorism Center wrote that he "spent literally years negotiating for access and retention to certain DHS data about non-U.S. persons and often the Privacy Act protections posed significant practical obstacles." He further wrote that this recommendation "should be read with extreme skepticism as it would likely do far more harm than good."

a. Why would extending such a policy across the intelligence community would do more good than harm? Specifically, what are the benefits of such a policy for the United States?

b. What effect would implementation of this recommendation have on information sharing about suspected foreign terrorists within the U.S. government? What is the basis for this conclusion?

Our recommendation would apply the Privacy Act of 1974 to non-U.S. persons in the same limited way as the Department of Homeland Security has done for several years. Notably, the Privacy Act would apply to "mixed" systems of records, which are systems of records where U.S. persons already have access and correction rights under the Privacy Act. For these "mixed" systems, the agency already must have in place an established procedure for responding to the limited number of access and correction requests that are made in practice. The additional administrative burden of responding in the same fashion to requests from both U.S. and non-U.S. persons, based on our interviews with those who have administered these systems, would be small.

The differential treatment of U.S. persons and non-U.S. persons under the Privacy Act has been a recurring source of concern from allies, notably including member states of the European Union, which has made a right to access a principal issue in data privacy negotiations to date. These negotiations, in turn, have been closely linked in statements by E.U. officials to negotiations for the free-trade agreement known as the Trans-Atlantic Trade and Partnership. By providing the same access rights both to citizens and non-citizens, as is the practice in the E.U., the recommendation addresses an important ongoing issue in negotiations with our leading trading partners in

Europe. Addressing this issue is consistent with the Presidential Policy Directive 28, which takes steps to treat non-U.S. persons similarly to U.S. persons where feasible.

Based on our briefings from multiple agencies, we believe the recommendation would not have a major impact on information sharing about suspected foreign terrorists. As noted in our report, the Privacy Act's requirements do not apply to classified computer systems or to law-enforcement sensitive/investigative information. We were informed that the FBI already applies the Privacy Act in the same manner for national security investigations as it does for other records covered by the Act. In addition, our recommendation creates an exception provision, so that it would not apply where an agency "provides specific and persuasive reasons not to do so."

2. Recommended Changes to the Section 215 Bulk Metadata Program

The Review Group's report recommended that metadata collected pursuant to the Section 215 program no longer be held by the NSA, but rather be stored with the communications providers or a third party, and that the government be required to obtain an order from the FISC before querying the metadata.

a. What effect would implementation of the recommendation that NSA no longer hold the metadata have on the FBI's ability to use the metadata, especially in cases when speed is important? What is the basis for this conclusion? Do you know, for example, whether third parties maintain the data in the same format, or have the same searching capabilities as the government?

When we met with the NSA, we were informed that it was not uncomfortable with this alternative and that its principal concern was the reluctance of the service providers to bear this responsibility. As we note in the Report, there will be transitional issues in moving from the existing system to one or another of the alternatives, and those issues deserve careful attention, but we believe that they can be managed and that the resulting program will operate efficiently. Our Report discusses relevant concerns and notes an alternative.

b. Please describe in detail the basis for the conclusion in the report that creative engineering approaches could help provide the government with similar functionality to search the metadata if it were to be held by a third party.

See our response to 2a. Given the extraordinary technological capacities of the NSA, we believe that problem can be managed if the NSA is asked to do so.

c. How much would implementing this recommendation cost the government if it were to pay for third parties to hold the metadata? What is the basis for this conclusion?

As we note in the Report, we recognize that there are costs involved. In the grand scheme of things, however, these costs seem reasonable and justified, relative to the alternative. The protection of individual privacy and the promotion of public trust are important goals.

d. What is your assessment of the privacy risks if third parties were to hold the metadata? What is the basis for this conclusion?

There are always privacy risks, regardless of who holds the metadata. Laws and processes should be in place to minimize those risks. The special risk in this context, however, is the risk that the government itself might misuse the data. Because government is so powerful, and is thus uniquely capable of doing great harm, that risk is at the very core of our constitutional protection of privacy. As our history teaches, the special concern in this context is that in the future, misguided government officials might use this data for illegitimate political ends. That particular risk – which threatens the integrity of our democracy – is much greater when the data is held by the government than when it is left in private hands.

e. What do you believe is a reasonable period of time for the government to transition to and implement a system in which third parties hold the metadata?

We did not offer an opinion on that question. In our judgment, the transition should take place as expeditiously as reasonably possible.

f. What effect would implementation of the recommendation that the government obtain a court order have on the FBI's ability to use the metadata, especially in cases when speed is important? What is the basis for this conclusion?

Consistent with standard practice, we recommend an exception to the requirement of a court order whenever speed is of the essence and the need to obtain a court order would seriously impair the FBI's ability to fulfill its responsibilities. We therefore think this should have no effect

on the FBI's ability to use the metadata in an appropriate manner.

g. In developing this recommendation, did you consider the government's experience during the period when the FISC required it to obtain court approval for queries of the metadata? What was that experience? For example, did you consider the length of time that it took for court approval during that period, how that increased time affected investigations, and whether that process led the government to forgo queries that it might otherwise have made if it had not needed a court order?

We recognize that, during this unusual period, the process was slow. This was no doubt due to the fact that the FISC was unaccustomed to dealing with such orders. We are hopeful that this would not be a problem once the process is regularized. After all, the FISC deals regularly with requests for court orders for other types of foreign intelligence surveillance, including order under section 215, and ordinary courts deal every day with search warrant requests in an expeditious and efficient manner. There is no reason why the FISC cannot do the same.

3. Metadata (for Director Morell only)

Director Morell, you testified that that there is "quite a bit of content in metadata" and that there is not "a sharp distinction between metadata and content."

a. For clarification, under the Section 215 telephony metadata program, as your report stated, metadata "does not include the content of calls," correct? In other words, the information that is collected under this program includes only the telephone numbers that originate and receive the calls, and the date and time of the calls. It does not include, for example, the identity of the subscriber or caller, or any of the words they may have spoken during the conversation.

b. Director Morell, does your testimony on this point presuppose the government querying the metadata and then marrying it with other information? If so, isn't the government only permitted to take these steps when it has a reasonable and articulable suspicion that a phone number is connected to terrorism? Can the government learn anything about a specific individual's private life merely by collecting this metadata, if it is never queried or combined with other information?

3. Question Regarding Metadata and Content (per the Committee's request, this question was answered specifically by Mr. Morell):

Senator Grassley is correct in noting that the telephony metadata held by NSA under Section 215 of the Patriot Act – by itself – does not contain content. The

Senator is also correct in noting that for that metadata to reveal content, it would have to be married with other data.

The point I (Mr. Morell) was trying to make is that it is possible to go from the seemingly innocuous metadata under 215 to highly personal information with very little effort, thus creating a potential risk to privacy and civil liberties. For example, an individual, acting inappropriately, bringing together metadata under 215 and only the internet, could easily reveal the identity of the caller and the identities of individuals and entities that he/she called – and with that information learn a great deal about the caller, his/her life, and lifestyle.

4. National Security Letters

The Review Group's report recommended that National Security Letters ("NSLs") should only be issued upon a judicial finding, and only when there are "reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect against international terrorism or clandestine intelligence activities."

However, according to the comments of the Judiciary transmitted to the Committee by Judge Bates through his letter of January 10, 2014, this recommendation could "increase the FISC's annual caseload severalfold." He further stated that "the sheer volume of new cases…would transform the FISC from an institution that is primarily focused on a relatively small number of cases that involve the most intrusive or expansive forms of intelligence collection to one primarily engaged in processing a much larger number of more routine, subpoena-type cases."

The FBI issues more than 20,000 NSLs each year for data such as telephone subscriber information, as well as banking and credit-card records. The data does not include phone call content. FBI Director James Comey said that NSLs are "a very important tool" that is "essential" to the work of the FBI. He also stated that adopting this recommendation would "actually make it harder for us to do national security investigations than bank fraud investigations."

a. What benefit will be achieved by requiring the FISC to review all NSLs, given the relatively low relevance standard that the group recommends?

As the Supreme Court has long recognized, the requirement of a court order is essential to mitigate the inherent risks of allowing persons engaged in the "competitive enterprise of ferreting out crime" to decide for themselves when a search is appropriate. That is, quite simply, why the Constitution ordinarily requires search warrants. In the absence of a persuasive reason not to require a judicial order, judicial involvement should presumptively be the preferred process. This is why section 215 requires court orders when the government seeks to obtain information from third parties in circumstances quite similar to those for which NSLs are used. Moreover, experience shows that there have been significant problems in the past with the use of NSLs, problems that demonstrate the need for judicial oversight.

b. What effect would implementation of this recommendation have on both the operation of the FISC and the FBI's ability to investigate national security cases? What is the basis for this conclusion?

As we note in the Report, this recommendation would add substantial new responsibilities to the work of the FISC. Additional judges – or magistrate judges – would be needed. Beyond that, we do not see any reason why giving this responsibility to the FISC – a responsibility it already has in the implementation of section 215 – would be in any way unreasonable.

c. What effect would implementation of this recommendation have on the FISC's budget and additional judges required? What is the basis for this conclusion?

See the response to question 4b.

d. Why does it make sense for the FISC to pre-approve NSLs when courts do not pre-approve grand jury subpoenas? In either case, if a criminal prosecution results, doesn't a defendant have the opportunity to challenge the use of these investigative tools if they are used unlawfully or improperly?

Grand jury subpoenas are typically designed to enable criminal prosecutions. When such prosecutions take place, there is an opportunity for judicial review of the legality of any subpoenas. In addition, the grand jury subpoena process is not classified. There is thus considerable opportunity for public oversight. NSL are classified. Criminal prosecutions in which the details of NSLs are revealed are extremely rare. For the most part, it is a secret process. This is, for the most part, appropriate. But it is why there is a greater need for independent judicial review of the process. Section 215 provides the more appropriate analogy than grand jury subpoenas, and Congress wisely recognized in section 215 the need for judicial orders.

5. Special Advocate

In your report, you recommended that an institutional privacy advocate should be appointed to represent the public's interest before the FISC. As set forth in this recommendation, the advocate could intervene in any case without permission from the presiding judge. However, the comments of the Judiciary transmitted to the Committee by Judge Bates warned against such an approach, for a variety of reasons.

h. What effect would implementation of this recommendation have on the FISC's budget and additional judges required? What is the basis for this conclusion? – As noted in our transmittal letter, we did not explore the budgetary and related questions raised by our various recommendations, and offered those recommendations subject to budgetary constraints.

i. What effect would implementation of this recommendation have on both the operation of the FISC and the FBI's

ability to investigate national security cases? What is the basis for this conclusion?

We believe that the recommendation would have no adverse effects. Our recommendation is designed only for cases raising serious questions of law, and in such cases, an adversary process is typically an important safeguard.

j. Do you agree with the comments from the Judiciary that in the vast majority of matters before the FISC, involving an advocate in the process would be both unnecessary and counterproductive? Why or why not?

We do not disagree with this statement (though the word "vast" might be a bit too strong). In the majority of cases, the relevant issues are relatively routine, and a public advocate would not be necessary.

k. Do you agree with the comments from the Judiciary that in the vast majority of matters before the FISC, involving an advocate in the process would result in more protections for suspected foreign terrorists than U.S. citizens? Why or why not? Do you believe this is desirable? Why or why not?

We agree that in most matters, an advocate would not be necessary or desirable. We do believe that for serious questions of law or policy, involving an advocate would not result in "more protections" for suspected foreign terrorists than for Americans. An adversary process would, in such cases, fit with our traditions.

l. Do you believe that FISC judges are capable of accurately assessing whether a matter requires the involvement of the special advocate? What is the basis for this conclusion?

We would not question the ability of the FISC judges in any way, but we believe that in our system, judges should not decide whether important interests or values should receive representation. That is the job of people whose interests or values are at stake. For this reason, we would not give the judges the power to decide that question.

m. Do you agree with the comments from the Judiciary that involving an advocate in the process could actually result in the court receiving less information on which to make a decision, because the government might be reluctant to share sensitive information with an institutional advocate and would no longer be bound by the heightened duties associated with *ex parte* practice? Why or why not?

There might be a risk of such an unintended outcome, for the reasons outlined in those comments, but when serious legal questions are involved, we believe that the risk is outweighed by the value of having an adversary proceeding.

6. For each of the above-mentioned recommendations, as well as all others listed in the report, please list the stakeholders or interested parties with which you discussed the recommendation, very briefly summarize the feedback the stakeholders or interested parties provided, and indicate whether the stakeholder or interested party (a) agreed with the recommendation or urged its adoption, and why; or (b) disagreed with the recommendation or urged that it not be adopted, and why.

The Review Group no longer exists, and hence we no longer have an available staff, but the full list of the people with whom we met can be found in our report. The public comments we received are also publicly available, and the oral comments we received in our various meetings were consistent with the written comments that are publicly available.