

January 3, 2017

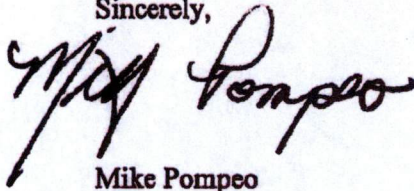
Senator Ron Wyden  
Senator Martin Heinrich  
U.S. Senate Select Committee on Intelligence  
211 Hart Senate Office Building  
Washington, D.C. 20510

Dear Senators Wyden and Heinrich:

Thank you for your letter dated December 23, 2016. As requested, I have completed your Prehearing Questions, and I have enclosed my responses.

I look forward to appearing before your committee on January 11<sup>th</sup>.

Sincerely,

A handwritten signature in black ink that reads "Mike Pompeo". The signature is written in a cursive, slightly slanted style.

Mike Pompeo

Enclosure

**Prehearing Questions for the Honorable Mike Pompeo upon his nomination  
to be the Director of the Central Intelligence Agency**

**Senators Wyden and Heinrich**

**Collection Authorities**

The Committee's questions reference your January 2016 op-ed in *The Wall Street Journal* in which you wrote: "Congress should pass a law re-establishing collection of all metadata, and combining it with publicly available financial and lifestyle information into a comprehensive, searchable database." Please answer the following additional questions.

- Please clarify whether "collection of *all* metadata" was a reference to bulk collection of metadata. If so, what kinds of metadata do you believe should be collected in bulk and entered into a "comprehensive, searchable database"?

I was referring to metadata of the type collected under the then-existing program that was available for review under procedures and conditions reviewed and approved by federal judges.

As noted in the op-ed, I was generally referring to additional publicly available data on the internet or other public databases that can provide important clues in identifying those who would seek to harm America. If confirmed, I will defer to policymakers, including the Congress, on whether it would be appropriate to collect metadata and publicly available data, the exact information to be collected, who would collect such information and appropriate restrictions. I note that such activity would be the responsibility of the FBI or other appropriate organizations. I note also that the Intelligence Community has, for many decades, applied restrictions to minimize information collected on U.S. persons, including in some cases, restrictions carried out under the approval and supervision of federal judges. I believe such minimization requirements are both appropriate and necessary.

- Do you believe metadata for telephony and electronic communications should be treated equally under the law, or should there be more restrictions on the collection of one type of metadata vs. the other?

These are very important questions that merit thorough study. There are a wide variety of constitutional, statutory, and other regulatory rules governing the treatment of different types of metadata. These range, to just name a few examples, from Fourth Amendment considerations, to the Foreign Intelligence Surveillance Act (including items like Pen Register/Trap and Trace provisions), to Federal Communications Commission rules on subscriber data.

If confirmed, and such issues were relevant to the CIA mission, I will consult with legal experts on the appropriate treatment of metadata to include examining the specific metadata at issue, the reasons for collection, and the governing legal framework. The CIA's data collection should always be driven by its statutory mission.

- Please clarify "*publicly available* financial and lifestyle information." What constitutes "publicly available information"? Does it include information provided by or purchased from third parties?

My op-ed was designed to provide general thoughts on the types of information that may be helpful in protecting the country. I did not set forth a specific list of items, but in general was referring to publicly available information, not information purchased by third parties. However, to the extent there is publicly available relevant intelligence information that may be obtained in full compliance with all privacy laws, such information should be considered as appropriate, if necessary to protect the country.

- Please clarify "*comprehensive, searchable database.*" Which U.S. government departments and agencies, as well as federal, state, local and/or tribal entities, should have access to the database or to information derived from the database? What restrictions, if any, do you believe should be placed on searches of the database and dissemination of the results of such searches, whether to U.S. intelligence and law enforcement entities or to foreign governments? How long should the information in the database be retained?

My op-ed was designed to provide general thoughts on the types of information that may be helpful in protecting the country. I did not propose a full legislative framework that would govern exact access to such information, the restrictions on searches and dissemination, or retention timeframes. I am aware that intelligence agencies, including the CIA, are subject to Attorney General guidelines and detailed rules governing the access to and handling of U.S. person data.

- Please provide additional detail on the role of the CIA with regard to the "comprehensive, searchable database," specifically whether, in your view, the CIA should have direct access to the database, whether the CIA should conduct or request queries of the database, whether information from the database should be disseminated to the CIA, and what restrictions, if any, should apply to the CIA's use of information from the database.

My op-ed was designed to provide general thoughts on the types of information that may be helpful in protecting the country. I did not propose a full legislative framework that would govern exact access by CIA to such information, the restrictions on searches and dissemination, or restrictions on use of information. I am aware that intelligence agencies, including the CIA, are subject to Attorney General guidelines and detailed rules governing the access to and handling of U.S. person data. Any such program for collection would be governed by rules and law set forth by policymakers that account for the full spectrum of interests and, with respect to U.S. persons, the CIA would be expected to participate only to the extent it was fulfilling its statutory mission set.

- The CIA's minimization procedures with regard to Section 702 of FISA state: "CIA personnel may query CIA electronic and data storage systems containing

unminimized communications acquired in accordance with section 702 of the Act. [REDACTED] Such queries must be reasonably designed to find and extract foreign intelligence information. CIA will maintain records of all such queries, including but not limited to United States person names and identities, and NSD and ODNI will review CIA's queries of content." Other than the requirement that the query be "reasonably designed to find and extract foreign intelligence information," do you believe there should be any limitations on CIA queries of U.S. persons for purposes of reviewing the content of communications? What limitations and reporting requirements do you believe should apply to U.S. person queries of Section 702-derived metadata?

In this context, a "query" involves using a name, phone number, email address, or other term to isolate communications with that term within a larger pool of data that an agency has already lawfully collected. It is important to note that queries do not result in the additional collection of any information.

The Attorney General and the Foreign Intelligence Surveillance Court (FISC) have reviewed and approved CIA's minimization procedures, including its limitations on queries, finding the procedures consistent with FISA and the Fourth Amendment. Those minimization procedures require that "Any United States person identity used to query the content of communications must be accompanied by a statement of facts showing that the use of any such identity as a query term is reasonably likely to return foreign intelligence information, as defined in FISA." I understand that as part of Section 702's extensive oversight, the Department of Justice and the Office of the Director of National Intelligence review all of CIA's U.S. person queries of Section 702-acquired content to ensure each query satisfies the legal standard articulated in the question. Any compliance incidents are reported both to Congress and the FISC.

In terms of U.S. person queries of Section 702-derived metadata, the DNI is required to make publicly available an annual report that provides -- among other things -- a good faith estimate of the number of U.S. person queries of Section 702-derived content and Section 702-derived metadata.

I believe the outlines of this program to be appropriate to perform the CIA's mission and safeguard fundamental rights.

If confirmed, I will be happy to discuss any specific proposals and their potential effects on CIA's ability to discover and analyze threats once I have been briefed on the Agency's efforts in this area.

- Section 702 of the Foreign Intelligence Surveillance Act prohibits "reverse targeting" of U.S. persons. As CIA Director, what policies would you adopt with regard to nominating targets of Section 702 collection in order to guard against reverse targeting?

I understand there are already Agency policies to prohibit CIA officers from "reverse targeting" U.S. persons and persons inside the United States. If confirmed, I intend to continue those policies. As part of Section 702 oversight, DOJ reviews all nominations for compliance with the targeting procedures and the statutory requirements, including the prohibition against reverse targeting (ODNI reviews a sample).

Bi-monthly reports documenting the results of each review are submitted to Congress as part of the semiannual reports required under 50 USC 1881f. Any compliance incidents discovered in the course of DOJ and ODNI's oversight are reported to the FISC pursuant to Rule 13(b) of the FISC's Rules of Procedure and to Congress in the semiannual reports.

- What differences, if any, do you believe should exist with regard to CIA access to, queries of, and use, dissemination and retention of U.S. person communications collected pursuant to Executive Order 12333 as compared to communications collected pursuant to Section 702?

I understand that all collection and use of U.S. person information is governed by law and policy. The collection of communications under Section 702 occurs under the important, but relatively narrow, circumstances where the communications of a foreign national located abroad may be obtained with the assistance of a U.S. service provider, subject to the jurisdiction of the FISC. The types of targeting and minimization procedures required by Section 702 are generally appropriate to that collection activity because Section 702 collection involves such limited range of collection techniques and because the involvement of U.S. service providers may implicate U.S. person communications to a greater degree in the event of error.

Because CIA activities under E.O. 12333 are strictly focused on collection activities abroad, with very limited exceptions, there is a smaller risk that these activities could implicate U.S. person communications compared with collection under Section 702. Additionally, CIA's E.O. 12333 activities involve a far greater variety of collection techniques, and often occur under circumstances where the collection opportunity is limited, costly, risky, and fragile. Thus, compared with Section 702 collection, the CIA's collection activities under E.O. 12333 require a far greater degree of agility and flexibility to obtain intelligence of sufficient timeliness and reliability. For these reasons, the CIA's access to, queries of, use, dissemination, and retention of U.S. person communications under E.O. 12333 are appropriately governed by broader and more flexible guidelines, compared with those required under Section 702.

- Executive Order 12333 states that the CIA may conduct surveillance within the United States "for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance." How would you ensure that any implementation of this authority does not adversely affect U.S. persons' civil liberties or otherwise result in CIA surveillance of U.S. persons?

Under E.O. 12333, the CIA may not engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance. Surveillance conducted for those purposes is governed by procedures established by the DCIA and approved by the Attorney General, after consultation with the DNI. In addition, activities that constitute "electronic surveillance" within the meaning of FISA, 50 U.S.C. 1801(f), are subject to the separate statutory requirements set forth at 50 USC 1805(g).

In order to protect the privacy and civil liberties of U.S. persons, these activities are limited in extent and duration to those necessary to accomplish the purpose of the activity and not directed at the communications of a particular person. With respect to testing or training, any information obtained in the course of activity should be retained and used only for purposes of the particular testing or training activities and destroyed as soon as practicable. With respect to countermeasures, any collected information should be used only to protect against unauthorized surveillance or disseminated only to appropriate agencies for enforcement of federal statutes prohibiting such unauthorized surveillance. If confirmed, I intend to continue these protections for the privacy and civil liberties of U.S. persons.

- Do you believe the CIA should be authorized to monitor U.S. persons' social media activities? If so, under what circumstances and subject to what limitations? What legal authority would provide the basis for such monitoring?

The CIA may already collect information related to the social media activities of U.S. persons only in furtherance of its authorized functions, and in accordance with the Constitution, federal statutes, and presidential directives. The collection, retention, and dissemination of information concerning U.S. persons may be undertaken only in accordance with Attorney General-approved procedures.

### **PPD-28 and Foreign Partners**

The Committee's questions reference the statement in your *WallStreet Journal* op-ed that Presidential Policy Directive-28 "bestows privacy rights on foreigners and imposes burdensome requirements to justify data collection." Please answer the following additional questions.

- What do you see as the possible costs to bilateral relationships, including bilateral intelligence relationships, to eliminating or modifying PPD 28?

The effect of eliminating or modifying PPD 28 will depend on the specific countries involved and the specific nature of any changes. Some countries, for example, have intelligence laws in effect that are somewhat more liberal than the restrictions in PPD 28, and those countries might not object if the U.S. modified PPD 28 to be more in line with their own laws. Other nations might be concerned about a modification to PPD 28 and seek a bilateral agreement with respect to its citizens.

- **Concerns about U.S. surveillance activities have led to litigation in Europe that prompted the Court of Justice of the European Union to strike down the Safe Harbor Agreement (which was the legal basis for companies' transfers of data between the EU and the U.S.). As CIA Director, would you support reforms to U.S. surveillance programs in order to address these developments?**

**These issues affect multiple agencies, as well as the private sector. If confirmed, I will engage with our partners inside and outside of government to ensure we have a holistic understanding of concerns related to U.S. surveillance programs before undertaking changes or reforms, if those are determined to be necessary and applicable.**

- **Is it ever appropriate for U.S. person information, collected in bulk by a foreign partner, to be obtained, used and disseminated by the Intelligence Community? If so, what limitations should be applied?**

**I understand that, in full compliance with law and Attorney General guidelines, it may be appropriate for CIA to collect information in bulk. To the extent U.S. person information is involved, CIA follows regulations and Attorney General-approved guidelines in handling of such information. If a foreign partner furnishes U.S. person information, I understand that information would also be handled pursuant to CIA regulations and Attorney General-approved guidelines. At times, U.S. person information may be highly relevant to protection of the country, such as a case where a U.S. person abroad is engaged in armed hostilities or planning for attacks to kill Americans.**

#### **Economic espionage**

- **According to the CIA's policies and procedures related to signals intelligence:**

***"The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and US. business sectors commercially. Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage."***

**How will you ensure that CIA collection and analysis is not used to advance the competitive advantage of U.S. companies and business sectors in which members of the administration, their families and associates, have an interest?**

**I understand there are already Agency policies to prohibit CIA officers from collecting or disseminating information purely to provide a U.S. business with a competitive advantage. If confirmed, I look forward to learning more about these policies and evaluating their effectiveness.**

### Encryption

- In your *Wall Street Journal* op-ed, you wrote that “the use of strong encryption in personal communications may itself be a red flag.” Are there any circumstances in which the use of strong encryption could be a basis for surveillance, particularly of U.S. persons?

CIA is prohibited from conducting electronic surveillance inside the United States, except in limited circumstances. The CIA may conduct electronic surveillance of a U.S. person, who is located outside the United States, if there is probable cause to believe the U.S. person is an agent of a foreign power and upon obtaining a warrant by the Foreign Intelligence Surveillance Court.

In my view, a U.S. person’s use of strong encryption would not be sufficient by itself to establish probable cause that the person is an agent of a foreign power. However, if CIA has reason to believe that a named U.S. person has been in contact with known or suspected terrorists, viewed or posted violent extremist propaganda online, expressed a desire to conduct a Homeland attack, and recently started using encrypted communications, his or her use of those communications should be considered in the course of the FBI investigation into the person.

### Interrogation

- The FY 2016 National Defense Authorization Act prohibited any interrogation techniques not listed in the Army Field Manual (AFM). Do you agree that, under current law, the use of interrogation techniques not authorized by the AFM, including the CIA’s former “enhanced interrogation techniques,” is illegal under any circumstances?

Section 1045 of the National Defense Authorization Act for FY2016 provides that no individual in U.S. custody may be subjected to any interrogation technique or approach that is not authorized by and listed in the Army Field Manual. Executive Order 13491 contains a similar requirement thus rendering the use of such techniques by the CIA illegal. Other statutes, including the Detainee Treatment Act of 2005, the Torture Statute, and the War Crimes Act, would prohibit certain interrogation techniques, alone or in combination.

- If you are confirmed and you are directed by President Trump to authorize interrogation techniques that are not authorized by the Army Field Manual and are therefore illegal, how would you respond?

I will never consider taking action inconsistent with the law. I also do not accept the hypothetical premise to this question. I have no reason to believe that President Trump will direct me not to follow the law and I will follow the law. I have no expectation of receiving any directions that do not comply with law.