Senate Select Intelligence Committee
Responses to Questions for the Record for Mr. John Demers,
Nominee for Assistant Attorney General for National Security, Department of Justice
Hearing on October 31, 2017

QUESTIONS FOR THE RECORD FROM SENATOR RON WYDEN

Section 702 of FISA

1. In 2015, the Department of Justice issued a memorandum entitled "Restriction Regarding the Use of FISA Section 702 Information in Criminal Proceedings Against United States Persons."

   a. **Do you believe there should be any restrictions on the use of information obtained from Section 702 other than as evidence in criminal proceedings, i.e. as part of criminal *investigations* or as part of administrative or civil investigations or proceedings?**

   RESPONSE: As I was not involved in the drafting of this 2015 policy, I am not aware of what factors the government may have weighed when deciding its scope, and thus am not in a position to assess whether that scope should be changed. Should I be confirmed, I would expect to be briefed further on Section 702, including on the development and implementation of this policy.

   b. **The 2015 policy includes an exception for "transnational crime." Do you support this exception and, if so, what would be included as a "transnational crime."**

   RESPONSE: See response to Question 1(a) above.

2. Section 702 of FISA prohibits the government from targeting a person reasonably believed to be located outside the United States "if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." Both the foreign target and the U.S. communicant can be the subject of repeated queries and disseminated reporting, and Section 702-collected information on either the foreign target or the U.S. communicant can be used in criminal and other proceedings.

   a. **Assuming the government has a purpose for targeting the foreign target, are there any limits to how extensively the government can query, disseminate and use 702-collected information on the U.S. communicant, relative to the overseas target, before the current statutory prohibition on "reverse targeting" applies?**

   RESPONSE: As I understand it, determining whether a particular known U.S. person has been reverse targeted through the targeting of a Section 702 target necessitates a fact specific inquiry that would involve consideration of a variety of factors. For example, as the Privacy and Civil Liberties Oversight Board noted in

its 2014 report, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little reporting about the Section 702 target, that might be an indication that reverse targeting may have occurred.

b. **If the answer above is no, would you support a change to the law that would require the government to consider the relative extent of queries, dissemination and use of 702-collected information in making a reverse targeting determination?**

RESPONSE: As noted above, under existing law I understand that a reverse targeting determination is a fact-specific inquiry that would involve consideration of a variety of factors. The Privacy and Civil Liberties Oversight Board has found no intentional misuse of Section 702 authority. Nonetheless, should I become aware of instances of reverse targeting through the Division's oversight function, I would conduct a root-cause analysis and consider a variety of approaches to ensure it did not reoccur.

Encryption

3. When the government mandates that companies weaken the encryption of the products used by the American public, it comes at serious cost to the security of Americans. Moreover, recent events such as the Office of Personnel Management breach and election-related Russian hacking have demonstrated that weak encryption is a serious national security problem. **If you are confirmed as Assistant Attorney General for the National Security Division, what will be your position with regard to policies or legislative proposals to permit the government to mandate weaknesses in strong encryption?**

RESPONSE: Encryption is important to enable the government, the private sector, and our citizens to safeguard private information and strengthen our personal and national security. However, it also poses serious challenges for law enforcement's ability to protect public safety by providing child molesters, terrorists, spies and other criminals with a more confidential way of communicating. I know that the Department of Justice and the FBI have expressed serious concerns, across Administrations, about their inability to obtain electronic information pursuant to lawful court orders because of encryption and other technological issues. If I am confirmed, I would work with all interested stakeholders, including Congress and the private sector, to come up with solutions to this challenge.

4. Under Section 702 of FISA, the government can direct an electronic communications service provider to provide "assistance necessary to accomplish the acquisition."

a. **Does this provision authorize the government to direct a provider to circumvent or weaken the encryption of the provider's product or to insert surveillance-enabling software into a customer's device?**

RESPONSE: Section 702(h) authorizes the Attorney General and Director of National Intelligence to direct an electronic communications service provider to provide "all information, facilities, or assistance necessary to accomplish the" Section 702 acquisition. This language is very similar to that found in Title I of FISA. I do not know whether section 702(h) could be used in the manner you describe, and determining the appropriate scope of such "information, facilities, or assistance" that is "necessary to accomplish the acquisition" in particular cases would involve a fact-based inquiry and could vary based on different service providers and different technologies. A provider is always free to challenge the lawfulness of a directive under this section or to require the Government to file a motion to compel.

b. **If the answer above is yes, should the FISA Court be informed of any such directive?**

RESPONSE: The FISA Court would be provided a Title VII directive for review if a service provider challenged the lawfulness of a directive as permitted under Section 702(h)(4), or if the Government filed a motion to compel a provider's compliance with a directive as permitted by Section 702(h)(5).

Media

5. On July 12, 2013, the Department of Justice released a Report on Review of News Media Policies. **Which aspects of that Review do you agree with and which would you advise be modified?**

RESPONSE: I have not had occasion to review the Department's Report on Review of News Media Policies during the prior Administration, so I am not in a position to comment on whether I would support or propose to modify any policies adopted as a result of that review. As I said at my confirmation hearing, I believe that issuing a subpoena to a journalist is not a decision to be taken lightly and should be a last resort or close to a last resort.

Enemy combatants

6. **Can a U.S. person who is arrested in the United States be held as an enemy combatant?**

RESPONSE: Federal courts have rendered different opinions on the question whether, and if so when, a U.S. person arrested in the United States may be held as an enemy combatant in the conflict with al Qaeda, the Taliban, and associated forces, and the Supreme Court has not addressed the issue. I have not examined this issue closely, but would do so if the question arises. As I stated at my confirmation hearing, my predisposition is that Americans ultimately be tried in Article III courts.

Other

7. Section 4 of PPD-28 calls on each Intelligence Community element to update existing or issue new policies and procedures to implement principles for safeguarding all personal information collected through SIGINT. Those policies and procedures are currently posted publicly by the ODNI.

   a. **Do you support the continuation of these policies?**

   b. **Please describe any modifications you would make to these policies.**

   RESPONSE to 7(a) and 7(b): I have not had occasion to review the policies and procedures adopted pursuant to PPD-28 or to discuss their basis and investigative impact with the Intelligence Community, so I am not in a position to comment on the substance of the policies.

8. **Are there any circumstances in which an element of the Intelligence Community may not conduct a warrantless search for a U.S. person of communications that have been collected pursuant to Section 12333? If so, please describe.**

   RESPONSE: Rules governing U.S. person information collected pursuant to Executive Order 12333 are set forth in guidelines established by the head of the relevant element of the Intelligence Community and approved by the Attorney General in accordance with section 2.3 of that order. Whether a particular query could be conducted would depend on application of any such rules to the circumstances at hand, and I have not had the opportunity to review those rules in many years.

Senate Select Intelligence Committee
Responses to Questions for the Record for Mr. John Demers,
Nominee for Assistant Attorney General for National Security, Department of Justice
Hearing on October 31, 2017

QUESTIONS FOR THE RECORD FROM SENATOR TOM COTTON

1. **Do you believe the growing presence of Chinese state-owned telecommunications carriers and equipment providers, such a China Mobile, China Telecom, China Unicom, Huawei, and ZTE, in the United States is a national security threat that we will have to deal with?**

   RESPONSE: I believe that the U.S. government must remain vigilant against the national security threat posed by the presence of foreign state-owned or controlled telecommunications carriers and equipment providers in the United States, including from China. I know that the Intelligence Community recently assessed publicly that China will continue to actively target the U.S. government, its allies, and U.S. companies for cyber espionage, and that our communication networks are at risk as our adversaries become more adept at compromising those networks.

2. **Will you commit to reading the latest intelligence on the threat these entities pose?**

   RESPONSE: Yes.

3. **Do you believe U.S. telecommunications providers, such as AT&T, should be wary about partnering in any way with Chinese state-owned telecommunications carriers and equipment providers, such as China Mobile, China Telecom, China Unicom, Huawei, and ZTE?**

   RESPONSE: The U.S. telecommunications sector is part of our nation's critical infrastructure, underlying the operations of all businesses, public safety organizations, and government. As such, I believe U.S. telecommunications providers must have a heightened awareness of the vulnerabilities in the telecommunications supply chain and take into account the security risks associated with doing business with third-party vendors, suppliers, and other partners, particularly those subject to influence by foreign governments. Ultimately, the U.S. government has the responsibility to ensure the security and resilience of the U.S. telecommunications sector, and to use every appropriate authority to address national security risks.

4. **Do you believe that China telecommunications and equipment providers should be allowed to have their equipment incorporated into critical infrastructure, such as first responder networks? Should U.S. government agencies be allowed to purchase phones if they include components produced by Huawei?**

   RESPONSE: I believe the U.S. government has a responsibility to ensure the security and resilience of the U.S. telecommunications sector, which is an essential

part of our critical infrastructure. If confirmed, I would work with interagency partners, including the Intelligence Community, the Department of Homeland Security, and sector specific agencies, as well as critical infrastructure owners and operators to address national security threats to the sector – including threats from telecommunications and equipment providers subject to influence by foreign governments.

5. **If confirmed, will you commit to reviewing and updating any National Security Threat Assessment associated with China Mobile Communications Corporation, Huawei, ZTE, China Telecom, China Unicom, or any other Chinese telecommunications company?**

   RESPONSE: I have not been with the Department of Justice for almost nine years, so I am not aware of what role the National Security Division has played in drafting National Security Threat Assessments associated with the Chinese telecommunications companies you reference. If confirmed, I commit to working with relevant interagency partners to take appropriate steps to address any national security threats posed by foreign-owned telecommunications carriers and equipment providers' operations in the United States.

6. **If confirmed, what other steps will you take in this area? Are there ways the DOJ NSD can better partner with the FCC and NTIA in this area?**

   RESPONSE: I have been away from the Department for almost nine years, and I am not aware of what role the National Security Division currently plays with respect to addressing national security risks affecting the U.S. telecommunications sector. I know that the Division participates in "Team Telecom," an ad-hoc interagency group that assists the Federal Communications Commission (FCC) in reviewing certain license applications and determining whether granting a license to foreign-owned or -controlled entities poses national security risks. If confirmed, I commit to working with relevant interagency partners to take appropriate steps to address any national security risks posed by foreign-owned telecommunications carriers and equipment providers' operations in the United States.

Senate Select Intelligence Committee
Responses to Questions for the Record for Mr. John Demers,
Nominee for Assistant Attorney General for National Security, Department of Justice
Hearing on October 31, 2017

QUESTIONS FOR THE RECORD FROM SENATOR KAMALA D. HARRIS

1. There has been a troubling uptick in domestic terror attacks targeting ethnic and religious minorities. Prior to the August 12, 2017 "Unite the Right" violence in Charlottesville, on May 20, 2017, FBI and DHS issued a Joint Intelligence Bulletin entitled "White Supremacist Extremism Poses Persistent Threat of Lethal Violence." The report notes that White Supremacist Extremists were responsible for 49 homicides in 26 attacks from 2000 to 2016, "more than any other domestic extremist movement." Additionally, a recent Government Accountability Office report stated that of the 85 violent extremist incidents in the U.S. that resulted in death since September 12, 2001, far-right extremist groups were responsible for 73 percent.

    a. **Would the NSD, under your leadership, commit to dedicating more resources to addressing these incidents of white supremacy and domestic terrorism?**

    b. **If confirmed to head the NSD, what other steps will you take to combat domestic terrorism?**

    RESPONSE: The violence in Charlottesville was reprehensible, and, like all terrorism, domestic terrorism must be prevented and prosecuted. As a private citizen who has been out of the Justice Department for nearly a decade, I am not in a position to assess whether NSD is devoting sufficient resources to the threat of domestic terrorism. I understand from the FBI Director's recent testimony that the FBI devotes significant resources to domestic terrorism investigations, which reflects the gravity of this threat to our national security, and I am committed to working with the FBI and using the full range of our authorities to protect the public against this serious threat. I would use every lawful tool, consistent with the First Amendment, to deter and disrupt the domestic terrorism threat, including terrorist activities by white supremacists, and bring those responsible to justice.

2. Recently, the FBI's Counterterrorism Division released a report entitled, "Black Identity Extremists Likely Motivated to Target Law Enforcement." The report details that in the aftermath of Black Lives Matter protests, the FBI created a new category of extremist for individuals who seek to "establish a separate black homeland or autonomous black institutions through unlawful acts of force or violence."
    a. **The NSD and FBI often work together on national security issues. Please explain the NSD's role in determining whether an individual is categorized as a "Black Identity Extremist"?**

b. **Please explain whether the NSD provides any advice or guidance to the FBI in terms of how to train its officers to deal with individuals designated as a "Black Identity Extremist." If so, what is this guidance? Should this guidance include implicit bias training? Should it include training to prevent racial profiling?**

c. **How will you ensure that this new designation will not be abused to target Americans that are merely exercising their right to free speech and assembly?**

RESPONSE: I am not familiar with this report, and because I am not currently working at the Department of Justice, I am unaware of what role NSD is playing with respect to this issue, including with respect to any training. It is essential that our national security laws and policies both safeguard the American people from a wide range of threats and maintain the individual liberties and freedoms that define American life. I note that the Attorney General's Guidelines for Domestic FBI Operations prohibit investigations of and information gathering on United States persons solely for the purpose of monitoring activities protected by the First Amendment. This is similar the language in FISA with respect to foreign intelligence surveillance. Thus, various laws recognize the sensitivity of the First Amendment issues that may be implicated by terrorism investigations. Together with the career attorneys in the Division, I would ensure that NSD's national security activities are conducted in accord with the law and the facts, and consistent with the constitutional protections for free speech and assembly.