

1 OVERSIGHT AND REAUTHORIZATION OF THE FISA AMENDMENTS ACT:
2 THE BALANCE BETWEEN NATIONAL SECURITY, PRIVACY,
3 AND CIVIL LIBERTIES

4 - - -

5 TUESDAY, MAY 10, 2016

6 United States Senate,
7 Committee on the Judiciary,
8 Washington, D.C.

9 The Committee met, pursuant to notice, at 9:31 a.m., in
10 room SD-226, Dirksen Senate Office Building, Hon. Chuck
11 Grassley, Chairman of the Committee, presiding.

12 Present: Senators Grassley, Cornyn, Tillis, Leahy,
13 Feinstein, Whitehouse, Klobuchar, Franken, Coons, and
14 Blumenthal.

15 OPENING STATEMENT OF HON. CHUCK GRASSLEY, A U.S.
16 SENATOR FROM THE STATE OF IOWA

17 Chairman Grassley. I am going to do things a little
18 bit backward today. I am going to introduce the witnesses
19 first, and then I am going to make my opening statement.
20 And I think Senator Leahy is on his way, and I would like to
21 have him make his opening statement before we receive the
22 testimony from the witnesses.

23 Our first witness is Kenneth Wainstein. He is a
24 partner at Cadwalader, Wickersham & Taft, where he serves as
25 the Chair of the firm's White Collar Defense and

1 Investigative Group. Before that, he worked for 19 years
2 at the Department of Justice, including serving as U.S.
3 Attorney for D.C. and the first Assistant Attorney General
4 for National Security. He concluded his Government service
5 in 2008, serving as Homeland Security Adviser to George W.
6 Bush. In that capacity, he coordinated the Nation's
7 counterterrorism, homeland security, infrastructure
8 protection, and disaster response and recovery efforts. He
9 has an undergraduate degree from the University of Virginia
10 and his law degree from Berkeley.

11 The second witness, Matthew Olsen, is the president of
12 consulting at IronNet Cybersecurity. From 2011 to 2014, he
13 served as Director of the National Counterterrorism Center
14 under President Obama. Prior to that, Mr. Olsen served as
15 General Counsel for the National Security Agency, Executive
16 Director of the Guantanamo Task Force, and spent more than
17 18 years at the Department of Justice, including serving as
18 a Deputy Assistant Attorney General overseeing the National
19 Security Division. Mr. Olsen is currently a lecturer at
20 Harvard Law School on national security law and practice.
21 He has an undergraduate degree from University of Virginia
22 and law degree from Harvard.

23 Our next witness is Elizabeth Goitein. She co-directs
24 the Brennan Center for Justice's Liberty & National Security
25 Program. Before that, she served as counsel to Senator

1 Feingold on this Committee and as a trial attorney in the
2 Federal Programs Branch, Civil Division, Department of
3 Justice. She has a law degree from Yale Law School.

4 The next witness is David Medine, Chairman of the
5 Privacy and Civil Liberties Oversight Board. Before that,
6 he was an Attorney Fellow for the Securities and Exchange
7 Commission and Special Counsel at the Consumer Financial
8 Protection Bureau. From 2002 to 2012, he practiced law at a
9 firm here in Washington, and from 1992 to the year 2000
10 served as Associate Director for Financial Practices at the
11 FTC. He has his undergraduate degree from Hampshire College
12 and law degree from the University of Chicago.

13 Our final witness is Rachel Brand. Ms. Brand has
14 served as a member of the Privacy and Civil Liberties
15 Oversight Board since 2012, has served as Vice President and
16 Chief Counsel for Regulatory Litigation at the U.S. Chamber
17 Litigation Center, and practices law at two firms here in
18 Washington. She has also served as Assistant Attorney
19 General for Legal Policy at the Department of Justice and
20 Associate Counsel in the Office of White House Counsel. Ms.
21 Brand has her undergraduate degree from the University of
22 Minnesota, Morris, and her law degree from Harvard. And,
23 most importantly, she has been an intern in my office, and
24 she is from Pella, Iowa. Yes, you ought to clap for that.

25 [Laughter.]

1 Chairman Grassley. I am going to make a statement now,
2 and hopefully Senator Leahy will be here, and then we will
3 have the witnesses. I just introduced them to use up time.

4 Almost exactly 6 months ago, our Nation's oldest ally,
5 France, suffered the deadliest attack on its soil since
6 World War II. In a series of coordinated suicide bombings,
7 mass shootings, and hostage takings across Paris, ISIS
8 killed 130 people and injured 368 more. The President of
9 France referred to that as an act of war.

10 A month or so later, in December, the United States
11 sustained the most deadly terrorist attack on our soil since
12 September 11, 2001. In San Bernardino, as you know, a
13 couple inspired by ISIS opened fire on an office holiday
14 party, killing 14 and injuring 22 more.

15 A few months after that, ISIS struck again, in
16 Brussels, the home of NATO's headquarters. On March 22nd,
17 it launched a series of coordinated bombings at an airport
18 and train station that killed 32 and injured over 300.

19 These attacks underscore that one of the core
20 responsibilities of our Government is to ensure that those
21 who protect us every day, including the intelligence
22 community, have the tools to keep us safe. And these tools
23 must adapt to both the changing technological landscape and
24 the evolving security threats that we face.

25 But at the same time, the rights and liberties

1 enshrined in our Constitution are a constant. And it is the
2 duty of this Committee in particular to be vigilant in
3 ensuring that they endure, no matter what.

4 Section 702 of the FISA Amendments Act, which provides
5 the Government the authority to collect the electronic
6 communications of foreigners outside the United States with
7 the compelled assistance of American companies, sits at the
8 intersection of these responsibilities.

9 In 2008, after much debate and discussion, this law was
10 passed by Congress and signed by President Bush. And in
11 2012, it was reauthorized by Congress without any changes
12 and with President Obama's strong support. From all
13 accounts, it has proven to be highly valuable in helping to
14 protect the United States and our allies.

15 Moreover, the Privacy and Civil Liberties Oversight
16 Board, the Foreign Intelligence Surveillance Court, and many
17 other Federal courts have found Section 702 constitutional
18 and consistent with the Fourth Amendment.

19 But questions and concerns persist for some about its
20 effect on our civil liberties. Most of these concerns
21 relate to the treatment of communications collected when it
22 turns out that a targeted foreigner is in contact with
23 somebody inside the United States. But, of course, these
24 are also situations where the program can be highly
25 valuable, by letting our Government know if a foreign

1 terrorist plot might reach our shores.

2 So this Committee's oversight of this law should
3 continue to be robust. And although the FISA Amendments Act
4 does not require Congress to reauthorize it until the end of
5 2017, I would like to begin the conversation about it well
6 in advance of that reauthorization.

7 That is why I requested that the Committee receive a
8 classified briefing from the Obama administration on Section
9 702 back in March of this year. It is why I am so glad to
10 have such a distinguished panel here with us today to talk
11 about those issues. And it is why I am sure we will
12 continue this public dialogue with the administration and
13 others in the future.

14 As I mentioned, Section 702 allows for the targeting of
15 foreigners located overseas for surveillance. The statute
16 specifically prohibits the targeting of anyone in the United
17 States, or any U.S. person, wherever that person is located
18 around the world. And it also prohibits what is called
19 "reverse targeting"--that is, targeting someone outside the
20 country for the purpose of targeting a specific person who
21 is located inside it.

22 Under the statute, the FISA Court must approve
23 targeting and minimization procedures to ensure that only
24 appropriate individuals are subject to surveillance and that
25 limit the handling and use of any communications so

1 collected. And implementation of the statute is overseen by
2 all three branches of Government, including the appropriate
3 Inspectors General.

4 Now, it is true that human error has led to mistakes in
5 implementing the law over the years. But it is also
6 significant that no internal or external review of the
7 Section 702 program has ever found any instance of an
8 intentional violation of the law.

9 Moreover, Section 702 has been highly important to our
10 national security. The Privacy and Civil Liberties
11 Oversight Board found unequivocally that it "has helped the
12 United States learn more about the membership, leadership
13 structure, priorities, tactics, and plans of international
14 terrorist organizations. It has enabled the discovery of
15 previously unknown terrorist operatives as well as the
16 locations and movements of suspects already known to the
17 Government. It has led to the discovery of previously
18 unknown terrorist plots directed against the United States
19 and foreign countries, enabling the disruption of those
20 plots."

21 The Board came to these conclusions about the value of
22 the Section 702 program after conducting a lengthy, in-depth
23 review of it. Just as importantly, however, the Board found
24 that the program was constitutional and authorized by the
25 statute. In addition, the Board proposed a number of

1 recommendations to help improve the privacy and civil
2 liberties protections of the Section 702 program.

3 According to the Board's most recent assessment report
4 just in February, all of its recommendations have been
5 implemented in full or in part, or the relevant Government
6 agency has taken significant steps toward adoption. That is
7 encouraging news. Among other things, I look forward to
8 hearing about the status of these recommendations today as
9 we discuss reauthorizing this important national security
10 authority.

11 Now, what I think we will do is we will start with the
12 first witness, Mr. Wainstein, and then when Senator Leahy
13 comes, we will stop and let him give his opening statement.
14 Would you proceed, please, sir?

1 STATEMENT OF THE HONORABLE KENNETH L. WAINSTEIN,
2 PARTNER, CADWALADER, WICKERSHAM & TAFT LLP,
3 WASHINGTON, D.C.

4 Mr. Wainstein. Thank you, Chairman Grassley, members
5 of the Committee. It is an honor to be here with you today
6 to support the reauthorization of the FISA Amendments Act
7 and to discuss the issues that it raises with my
8 distinguished co-panelists.

9 Since the attacks of September 11, 2001, we have been
10 engaged in a methodical effort to enhance our intelligence
11 capabilities and, in particular, to build a legal and
12 operational framework that affords us the ability to
13 intercept our adversaries' communications. The centerpiece
14 of that effort has been Congress' decision to modernize our
15 national security surveillance efforts by passing the FISA
16 Amendments Act, the FAA, in 2008 and reauthorizing it in
17 2012.

18 It is important at the outset to remind ourselves why
19 it was necessary to modernize the Foreign Intelligence
20 Surveillance Act in the first place. As you know, the FISA
21 was passed in 1978 after the Church Committee hearings and
22 the abuses they disclosed persuaded Congress that domestic
23 national security surveillance efforts should be subject to
24 a process of judicial review and approval.

25 To effectuate that objective, Congress passed FISA,

1 which established the Foreign Intelligence Surveillance
2 Court--or the FISA Court--and defined those types of
3 surveillance that required approval from that Court. In
4 defining which surveillances fell in that category, Congress
5 differentiated by the technology of the communication in a
6 way that effectuated its intent to require Court approval
7 for the interception of domestic communications where the
8 Fourth Amendment applied, but to carve out from the Court
9 approval requirement those communications that were foreign-
10 based where the Fourth Amendment does not apply.

11 However, with the change in communications technology
12 in the intervening years, that carve-out started to break
13 down, with the result that the Government found itself
14 having to expend significant manpower generating individual
15 FISA Court applications for surveillances against persons
16 who were outside the United States--the very category of
17 surveillances that Congress specifically intended to exclude
18 when it imposed the FISA Court approval requirement in 1978.

19 That situation became untenable with the dramatic
20 increase in counterterrorism surveillance efforts after
21 9/11. To its enduring credit, Congress stepped up in the
22 spring of 2007, undertook a thorough analysis and debate
23 about how best to revise FISA, and ultimately passed the
24 FISA Amendments Act in July 2008 and its reauthorization in
25 2011. And on both occasions, members from both parties

1 worked in a bipartisan fashion to craft a law that was a
2 significant step forward for both national security and
3 civil liberties.

4 The statute amended FISA in three important ways:

5 First, and most significantly, it authorized the FISA
6 Court to approve surveillance of categories of terrorist
7 suspects and other foreign intelligence targets who are
8 overseas without requiring the Government to provide an
9 individualized application as to each particular target. In
10 Section 702, the FAA prescribed a new, streamlined process
11 by which categories of overseas targets can be approved for
12 surveillance pursuant to strict procedural requirements and
13 subject both to review and approval by the FISA Court and to
14 substantial oversight regimes by a variety of Government
15 entities, to include the Attorney General, the Director of
16 National Intelligence, the heads and Inspectors General of
17 the relevant agencies, the FISA Court, and the Intelligence
18 and Judiciary Committees of Congress.

19 In addition to providing this authority and prescribing
20 substantial oversight, the FAA also added to the protections
21 for U.S. persons in a very significant way by imposing for
22 the very first time the requirement that the Government
23 obtain an individualized order from the FISA Court whenever
24 it undertakes surveillance of a U.S. person while that
25 person is outside the U.S.

1 In sum, the FISA Amendments Act was a very well
2 calibrated piece of legislation. It provided the Government
3 with the authority it needed, but did so with a careful eye
4 on the importance of oversight and on the privacy rights of
5 U.S. persons.

6 Since its implementation, FAA-authorized surveillance
7 has been absolutely critical to detecting and understanding
8 the threats that we face. That was the case when I was
9 reviewing FAA-derived reporting as Homeland Security Adviser
10 in 2008, and it is still the case today, as you know from
11 your briefing the other day.

12 Importantly, besides being implemented effectively, it
13 has also been implemented responsibly, as evidenced by the
14 PCLOB's findings that there have been no known instances of
15 intentional misuse of that authority.

16 So in supporting reauthorization, I ask Congress to
17 focus on the three considerations laid out in my remarks:
18 one, the vital importance of the FAA surveillance authority
19 to our counterterrorism efforts; two, the extreme care with
20 which Members of Congress of both parties crafted and
21 limited this authority when they passed the FAA in 2008 and
22 reauthorized it 4 years later; and the findings that this
23 authority has been implemented to great effect and in
24 compliance with the law and the Constitution.

25 In addition to these considerations, we want to focus

1 on one other important consideration, which is the severity
2 of the terrorist threat that we still face today. Given
3 that continuing threat, as evidenced by the recent attacks,
4 now is not the time to weaken our defenses or scale back on
5 a critical intelligence authority like the FISA Amendments
6 Act. To the contrary, now is the time to ensure that our
7 Intelligence Community operators have the authorities they
8 need to protect our country, and it is time to reauthorize
9 the statute that has done so much to protect our people and
10 our liberties for the last 8 years.

11 Thank you for the opportunity to speak about this
12 important issue, and I look forward to your questions.

13 [The prepared statement of Mr. Wainstein follows:]

1 Chairman Grassley. Thank you, Mr. Wainstein.

2 Before Mr. Olsen goes ahead, I would ask Senator Leahy
3 to give his opening remarks at this point.

4 OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S.

5 SENATOR FROM THE STATE OF VERMONT

6 Senator Leahy. Well, thank you, Mr. Chairman, and as I
7 mentioned earlier, we have conflicting schedules this
8 morning. But I think this is a very important hearing.

9 I think a year ago this week, the House of
10 Representatives overwhelmingly passed the USA FREEDOM Act.
11 Several weeks later the Senate followed suit. That marked
12 the first major overhaul of the Government's surveillance
13 authorities in decades.

14 Now, today we are examining the FISA Amendments Act,
15 often referred to, as you have noted, as Section 702. This
16 law expires at the end of 2017, so I am glad we are getting
17 an early start on this. I hope we can avoid the needless
18 expiration of authorities we saw last year when the
19 leadership would not bring up the USA FREEDOM Act until
20 after the expiration. And I am also glad--I applaud you on
21 this, Mr. Chairman--that we are holding this hearing in the
22 open so that the American people can be a part of this
23 conversation.

24 When Congress last reauthorized the FISA Amendments Act
25 in 2012, this type of discussion was not possible. Almost

1 everything about its implementation remained classified.

2 Since then, the Obama administration has declassified
3 much about the Government's use of the law. So the
4 transparency reforms put in place through the USA FREEDOM
5 Act are prompting our efforts.

6 But we have a lot of work to do. We are still missing
7 a lot of facts about Section 702 implementation. And
8 additional reforms are needed to protect Americans' privacy.
9 We also have to restore global trust in the U.S. technology
10 industry--not a minor thing.

11 Section 702 is an important tool for our national
12 security agencies. We all acknowledge that. But it is also
13 extremely broad. Although Section 702 is aimed at
14 surveillance of foreigners outside the United States, it
15 sweeps up a sizeable amount of information about innocent
16 Americans who are communicating with foreigners. So the
17 authority requires strong oversight, transparency, and
18 safeguards to protect the American people. In 2008 and
19 again in 2012, I opposed the FISA Amendments Act because it
20 lacked these safeguards.

21 Despite these concerns about Americans' communications
22 being swept up, we still do not know how much of our data is
23 collected under this authority. I understand the
24 intelligence community is now developing a methodology to
25 estimate that figure, and that is long overdue, but I

1 applaud that it is happening. It is all the more
2 significant because both intelligence and law enforcement
3 agencies search this data for information about Americans--
4 without judicial approval. And these back-door searches I
5 think raise some serious constitutional questions. I ask
6 consent to enter into the record written testimony from
7 several organizations raising additional concerns, including
8 Third Wave and the Electronic Frontier Foundation.

9 Chairman Grassley. Without objection, they will be
10 included.

11 [The information follows:]

12 / COMMITTEE INSERT

1 Senator Leahy. Now, let me just conclude with this: I
2 know we are going to hear about the importance of this
3 authority to our national security, and I understand that.
4 It is a conversation we should have. But we also must
5 ensure the surveillance programs operated under Section 702
6 respect the other part of American security--our liberties
7 and our constitutional values, because unless they align
8 with that, then it is a false sense of security.

9 I look forward to hearing from our witnesses. Thank
10 you.

11 Chairman Grassley. Thank you.

12 Now, Mr. Olsen, would you continue?

1 STATEMENT OF THE HONORABLE MATTHEW G. OLSEN,
2 PRESIDENT, CONSULTING, IRONNET CYBERSECURITY,
3 FULTON, MARYLAND, AND FORMER DIRECTOR, NATIONAL
4 COUNTERTERRORISM CENTER

5 Mr. Olsen. Yes, thank you, Chairman Grassley, Ranking
6 Member Leahy, and distinguished members of the Committee. I
7 am honored to be here this morning to talk about this
8 important issue.

9 As the former Director of the National Counterterrorism
10 Center, I can attest to the value that FAA has provided t
11 our national security. It significantly has contributed to
12 our ability to prevent terrorist attacks inside the United
13 States and around the world.

14 Also as the former General Counsel of the National
15 Security Agency and as a former official at the Department
16 of Justice's National Security Division, I was responsible
17 in those jobs for ensuring that the law was implemented in a
18 way that complied with the law, the Constitution, and
19 protected the privacy and civil liberties of Americans.

20 In my brief remarks this morning, I will focus on the
21 operational aspects of Section 702 and the value that this
22 authority has provided to our counterterrorism efforts.

23 I think to start, to appreciate the importance of
24 Section 702 it is helpful to described briefly the threat
25 that the United States faces from terrorism. Over the past

1 several years, the range of terrorist threats we face from
2 al Qaeda-linked groups has expanded and become more diverse.
3 By any measure, the so-called Islamic State, or ISIS,
4 presents the most urgent threat to our security today. It
5 has seized territory, it is governing territory, and at the
6 same time it has secured the allegiance of terrorist groups
7 across North Africa and the Middle East. Its sanctuary in
8 Syria and Iraq has provided it the ability to recruit,
9 train, and then execute external attacks, as we have seen
10 now in Paris and in Brussels. It also has the ability to
11 incite other assailants around the world, as we have seen in
12 San Bernardino.

13 Looking more broadly, ISIS is not the only threat we
14 face in Syria. Veteran al Qaeda fighters have traveled from
15 Pakistan to take advantage of the permissive environment
16 there. They are seeking to carry out attacks against the
17 West. Al-Shabaab maintains a safe haven in Somalia and
18 threatens our interests in the region. AQIM and Boko Haram--
19 now an ally of ISIS--continue to maintain their base of
20 operations in North and West Africa.

21 And al Qaeda core continues to support attacking the
22 West. It is vying with ISIS to be the leader of a global
23 jihad. The core leadership of al Qaeda wields substantial
24 influence over affiliated groups, in particular, al Qaeda in
25 the Arabian Peninsula. Indeed, on three occasions over the

1 past several years, AQAP has sought to bring down an
2 airliner headed for the United States. There is every
3 reason to believe it still has the intent and substantial
4 capability to carry out such an attack.

5 So against this backdrop of a dynamic and lethal
6 terrorist threat, the ability of the United States to
7 conduct surveillance under Section 702 is vital to our
8 security. As the Director of NCTC, I relied on daily
9 intelligence briefings from information collected by 702.
10 This intelligence was instrumental to our efforts to discern
11 the intentions and capabilities of our terrorist
12 adversaries, contributing both to the strategic judgments
13 and tactical insights.

14 Two specific cases, now declassified, highlight the
15 value of Section 702.

16 In September 2009, NSA analysts use 702 to target an
17 email address used by an al Qaeda courier in Pakistan.
18 Based on this surveillance, NSA discovered a message sent to
19 an individual in the United States, in Colorado,
20 subsequently identified as Najibullah Zazi. He was urgently
21 seeking advice on how to make explosives. Further
22 investigation revealed that Zazi and a group of operatives
23 had imminent plans to detonate explosives in the New York
24 subway. The FBI and local law enforcement arrested Zazi and
25 his confederates and stopped that attack before it could

1 occur.

2 In another case, NSA conducted surveillance under
3 Section 702 of an email address used by a suspected
4 extremist in Yemen. This surveillance led to the discovery
5 of a connection between that person and an unknown person in
6 Kansas City, Missouri, later identified as Ouazzani. The
7 follow-up investigation revealed that Ouazzani was connected
8 to other al Qaeda associates in the United States who were
9 part of an earlier plot to bomb the New York Stock Exchange.
10 These individuals were prosecuted and pled guilty.

11 In the context of these cases, Zazi and Ouazzani, it is
12 worth emphasizing the role of "incidental collection" under
13 Section 702. In these cases the Government collected the
14 communications of operatives inside the United States
15 directly as a consequence of their contacts with Section 702
16 targets located overseas. This was critical to the
17 disruption of these plots and to the arrest of al Qaeda
18 operatives here. So-called incidental collection led to the
19 initial identification of Zazi and Ouazzani and enabled the
20 Government to use other investigative tools, including
21 traditional FISA, to advance their investigations.

22 Beyond the United States, Section 702 has proven to be
23 an invaluable tool in supporting the counterterrorism
24 efforts of our allies around the world.

25 Finally, in describing the value of Section 702, it is

1 important to explain why this is uniquely important. As the
2 Deputy Assistant Attorney General from 2006 to 2009
3 overseeing DOJ's foreign intelligence surveillance programs,
4 I experienced firsthand the consequences of the pre-FAA
5 approach. In some cases, it simply was not possible under
6 that prior approach to demonstrate probable cause that a
7 proposed target overseas was an "agent of a foreign power."

8 In short, Section 702 authorizes the Government,
9 consistent with the Constitution, to obtain critical
10 intelligence about terrorists and other targets that it
11 simply cannot obtain by other means.

12 In conclusion, I would say that the authority Congress
13 established under Section 702 has played an indispensable
14 role in protecting the Nation from terrorist threats. I
15 look forward to your questions.

16 [The prepared statement of Mr. Olsen follows:]

1 Chairman Grassley. Thank you.

2 Now, Ms. Goitein.

1 STATEMENT OF ELIZABETH GOITEIN, CO-DIRECTOR,
2 LIBERTY & NATIONAL SECURITY PROGRAM, BRENNAN
3 CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL
4 OF LAW, WASHINGTON, D.C.

5 Ms. Goitein. Thank you. Chairman Grassley, Ranking
6 Member Leahy, and members of the Committee, thank you for
7 this opportunity to testify on behalf of the Brennan Center
8 for Justice.

9 Our Nation faces real threats from international
10 terrorism. Your challenge and your responsibility is to
11 ensure that these threats are addressed, not only
12 effectively, but in a way that is consistent with the
13 Constitution, the privacy interests of law-abiding
14 individuals, and our Nation's economic interests. Section
15 702 in its current form does not accomplish those aims.

16 Technological advances have revolutionized
17 communications. People are communicating at a scale that
18 was unimaginable just a few years ago. International phone
19 calls, which were once difficult and expensive, as I
20 remember, are now as simple as tapping a screen, and the
21 Internet offers countless additional means of international
22 communication. Globalization makes these exchanges as
23 necessary as they are easy. As a result, the amount of
24 information about Americans that the NSA intercepts, even
25 when targeting foreigners overseas, has exploded.

1 But instead of shoring up safeguards for ordinary
2 Americans and foreigners who communicate internationally,
3 Section 702 did the opposite. It eliminated the requirement
4 of an individual court order to collect communications
5 between foreign targets and Americans. It also eliminated
6 the requirement that the target be affiliated with a foreign
7 power or terrorist group.

8 The Government today can target any foreigner overseas
9 regardless of whether he poses any threat to the United
10 States and obtain his communications with Americans. While
11 the Government must certify that acquiring foreign
12 intelligence is one of its purposes, the law defines
13 "foreign intelligence" broadly enough to include
14 conversations about current events. Moreover, the
15 Government has interpreted the law to allow collection of
16 communications, not just to and from the target but about
17 the target.

18 This legal sea change underlies the NSA's "upstream
19 collection" program whereby a huge proportion of
20 communications flowing into and out of the United States are
21 scanned for selectors associated with designated foreigners
22 and picked up. Using upstream collection and PRISM, which
23 obtains stored emails from U.S. companies, the NSA collects
24 more than 250 million Internet communications a year. That
25 undoubtedly includes millions, if not tens of millions, of

1 Americans' emails. And as we know, wholly domestic
2 communications are included as well. To call this kind of
3 mass collection "targeted" elevates form over substance.

4 There are deep constitutional concerns with this
5 surveillance. The Fourth Amendment may not apply to
6 foreigners overseas, but when a law is designed to collect
7 communications between foreigners and Americans, the Fourth
8 Amendment is very much in play. And when the FBI searches
9 through those communications for evidence to use against
10 Americans in criminal cases and then fails to notify the
11 defendants how it obtained the evidence, it drives a hole
12 the size of Fort Meade through the Fourth Amendment.

13 Constitutional concerns aside, the mass collection of
14 communications comes with significant risks and harms. The
15 OPM fiasco reminded us how vulnerable Government databases
16 are to foreign governments and other hackers. And any
17 massive database that contains sensitive information about
18 Americans carries with it the risk of abuse or negligent
19 mishandling by this or some future administration.

20 Overbroad surveillance also threatens our economic
21 interests by impairing the legal and practical ability of
22 U.S. technology companies to do business with customers
23 overseas.

24 We are told that these risks are justified because
25 Section 702 has helped to stop terrorist plots, but the

1 question is not just whether Section 702 is useful. We must
2 also ask whether effective surveillance can be conducted in
3 a manner that is less intrusive with fewer costs to our
4 liberties.

5 One final point. Within constitutional bounds set by
6 the courts, Americans should be able to decide for
7 themselves how much surveillance is too much. But to do
8 that we need information. Five years after Senator Wyden
9 first requested an estimate of the number of American
10 communications collected under Section 702, we are still
11 waiting. Congress and the public need this basic
12 information for the democratic process to work.

13 Thank you, and I look forward to taking your questions.

14 [The prepared statement of Ms. Goitein follows:]

- 1 Chairman Grassley. Thank you very much.
- 2 Mr. Medine.

1 STATEMENT OF THE HONORABLE DAVID MEDINE, CHAIRMAN,
2 PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD,
3 WASHINGTON, D.C.

4 Mr. Medine. Chairman Grassley, Ranking Member Leahy,
5 members of the Committee, thanks very much for the
6 opportunity to testify today on the reauthorization of
7 Section 702 of the FISA Amendments Act.

8 In 2014, the Privacy and Civil Liberties Oversight
9 Board, which I chair, issued an extensive report on Section
10 702 and how it operates, in part to foster just the type of
11 democratic debate that we are having today. In short, the
12 Section 702 surveillance program collects the contents of
13 communications of non-U.S. persons outside the United States
14 where there is a foreign intelligence value. As has been
15 mentioned earlier, it has proven to be a valuable
16 intelligence tool for the U.S. Government, thwarting
17 terrorist plots and providing valuable information to U.S.
18 Government decisionmakers.

19 Section 702 has two components: PRISM and Upstream.
20 In PRISM, the Government collects the contents of targets'
21 emails and other communications from electronic
22 communications providers. While the targets are non-U.S.
23 persons, from time to time those non-U.S. persons
24 communicate with Americans, and as a result, the Government
25 is collecting large quantities of Americans' communications.

1 These are incidental communications because the U.S. persons
2 are not the targets, but they are no inadvertent because it
3 is known in advance the Americans' communications will be
4 collected.

5 In contrast, in the Upstream program, the Government
6 gets access to the telecommunications "backbone" over which
7 some telephone and Internet communications transit and can
8 collect the contents of emails and phone calls. By using
9 "about collection," the Government does not look just in the
10 header of "to" and "from" of an email, but it also scans the
11 contents of the email for a targeted selector.

12 As a result, if Liza and I were communicating by email
13 and I sent her a message with an email address from my uncle
14 in Turkey so she has a place to stay when traveling to
15 Turkey, if it turns out that my uncle's email address is one
16 of the 94,000 selectors currently on target in the Section
17 702 program, my email to Liza could be picked up and copied
18 into an NSA database, even though neither one of us is
19 suspected of wrongdoing and even my uncle might not be
20 suspected of wrongdoing and may simply have valuable foreign
21 intelligence information.

22 If this program is to continue, it should have privacy
23 and civil liberties, particularly where U.S. persons are
24 implicated. Accordingly, I recommend three legislative
25 changes:

1 First, many of the communications collected under 702
2 have nothing to do with terrorism or crime. They can
3 include family photographs, love letters, personal financial
4 matters, discussions of physical and mental health, and
5 political and religious exchanges. U.S. persons' queries of
6 that database are, therefore, capable of revealing a
7 significant slice of an American's personal life. This is
8 particularly the case for Americans who correspond
9 frequently with foreigners, including relatives, friends,
10 and business associates. Since no warrant was ever issued
11 for these communications, which are covered by the Fourth
12 Amendment, there should be some form of protection. Before
13 querying these databases for a U.S. person identified,
14 intelligence agencies and the FBI should be required to
15 submit their U.S. person identifier queries to the FISA
16 Court for approval other than in exigent circumstances.
17 Most important here is that there be an impartial life-
18 tenured Federal judge have the final say over whether
19 Americans' personal communications are collected and
20 reviewed.

21 Second, upstream and "about" communications raise two
22 potential concerns: one is the colleague of purely domestic
23 communications, American to American; and the other is
24 overcollection of communications. Building on the
25 recommendations put forward in PCLOB's 702 report, as

1 technology evolves, the Government should be required to
2 evaluate the effectiveness of screening of domestic
3 communications and also should determine ways of separating
4 out various types of "about" communications so we can have
5 policy decisions as to whether all of them should be
6 collected.

7 Third, a large number of U.S. persons' incidental
8 communications are collected under 702, as I have mentioned.
9 But how many? In order to have an informed democratic
10 debate about the scope of this program, it is important that
11 citizens and Members of Congress know how many Americans'
12 communications are being implicated in this program.

13 I have no reason to doubt that the Government has
14 encountered difficulties in quantifying the number of U.S.
15 persons' records it incidentally collects. Nevertheless, I
16 urge this Committee to require all agencies collecting
17 information under Section 702 to develop a manageable way to
18 gather statistics and provide them to Congress on a regular
19 basis.

20 I hope that Congress will use the reauthorization
21 process as an opportunity to enhance privacy and civil
22 liberty protections in Section 702 while maintaining a
23 program that has provided enormously valuable information to
24 protect our country from terrorism.

25 I appreciate the opportunity to present my views to the

1 Committee. Thank you.

2 [The prepared statement of Mr. Medine follows:]

1 Chairman Grassley. Thank you.

2 Now, Ms. Brand.

1 STATEMENT OF THE HONORABLE RACHEL L. BRAND, BOARD
2 MEMBER, PRIVACY AND CIVIL LIBERTIES OVERSIGHT
3 BOARD, WASHINGTON, D.C.

4 Ms. Brand. Mr. Chairman, Ranking Member Leahy, and
5 members of the Committee, thank you for the opportunity to
6 testify today about Section 702 of FISA. Like Mr. Medine, I
7 serve as a member of the Privacy and Civil Liberties
8 Oversight Board. Although you, Mr. Chairman, and other
9 witnesses have already discussed some aspects of the 702
10 program, it has been so widely misunderstood that I think a
11 few key points are worth stressing.

12 The first is the limits under which the 702 program
13 operates. Section 702, as the PCLOB unanimously found, is a
14 targeted collection program. It does not authorize bulk
15 surveillance. The Government may target only non-U.S.
16 persons located outside the United States, which means that
17 it can never target any U.S. person located anywhere, and it
18 can never target anyone located inside the United States.
19 And the Government cannot target just any foreign person
20 located outside the United States. It can target only
21 persons likely to communicate information about foreign
22 intelligence topics approved by the FISA Court. And, in
23 fact, the NSA targets only a tiny fraction of a percentage
24 point of Internet users in the world.

25 Although U.S. persons cannot be targeted, some U.S.

1 person communications will be incidentally collected. If a
2 target communicates with a U.S. person, for example, that
3 communication will be collected. This does not mean that
4 all of that U.S. person's communications will be collected,
5 but only his communications with the target. Of course, as
6 Chairman Grassley noted, if those communications revealed a
7 terrorist threat inside the United States, they would be
8 among the most important communications collected under the
9 program. But because this has privacy implications for some
10 U.S. persons, the statute requires the Government to operate
11 the program under strict rules that minimize its privacy
12 impact.

13 The second major point is that Section 702 is
14 unquestionably a highly effective source of foreign
15 intelligence. Mr. Olsen and Mr. Wainstein have already
16 discussed this. The PCLOB also unanimously found that 702
17 collection has helped to disrupt terrorist plots, identify
18 previously unknown individuals involved in terrorism, and
19 understand terrorists' operations priorities, strategies,
20 and tactics. The Board concluded the program was authorized
21 by Congress and is reasons under the Fourth Amendment. The
22 Board did recommend refinements to the program but did not
23 find them to be legally required. The Board did not
24 recommend any legislative changes to Section 702.

25 It is worth noting that the Board's five members were

1 unanimous in the report's central conclusions. We are also
2 unanimous in virtually all of our recommendations for how to
3 improve the privacy protections and the program's rules.
4 The administration has implemented many of those
5 recommendations and is working on the rest.

6 One issue that divided the Board concerns U.S. person
7 queries. Particular concern has been raised about U.S.
8 person queries by the FBI, so I would like to address that
9 for a moment. At the FBI a typical early step in a criminal
10 investigation is to query the FBI's databases to see what
11 the FBI already knows. These queries do not distinguish
12 between U.S. persons and others because nationality is
13 normally irrelevant to a criminal investigation.

14 One of the FBI's databases contains a subset of the
15 information collected under Section 702, though none of the
16 data collected upstream, so none of the "about"
17 communications that Mr. Medine referenced. An FBI query MA
18 include this database along with other databases, even if
19 the crime being investigated does not relate to national
20 security. However, it is extremely unlikely that an FBI
21 query in a non-national security investigation will hit on
22 702 data.

23 Some have suggested requiring the FBI to get court
24 approval before conducting a query of 702 information in an
25 investigation of a non-national security crime. The Board

1 did not recommend this approach, and I think it would be a
2 mistake. In the interest of time, I will mention just one
3 of several reasons why.

4 Requiring judicial approval for FBI queries would be a
5 step toward re-erecting the information-sharing wall that
6 the Government has worked so hard to tear down since 9/11.
7 An investigator looking into a non-national security crime
8 likely would not expect to find a connection with 702
9 information. But if such a connection existed, it would be
10 extremely important to know. The FBI's procedures should
11 not limit queries in a way that would prevent the Government
12 from discovering these potential connections.

13 Limits should be placed not on queries of information
14 but on the use of that information. The law should, and
15 does, limit what can be done with 702 information if it is
16 responsive to a query. This includes, for example, limits
17 on who can view responsive information, high-level approval
18 requirements before that information can be used in any
19 criminal proceeding, and notice to a defendant if his
20 communications are used against him. I believe these
21 protections strike the right balance between getting the
22 benefit of important intelligence collected under 702 and
23 protecting the interests of those whose communications are
24 collected.

25 Thank you. I look forward to your questions.

1 [The prepared statement of Ms. Brand follows:]

1 Chairman Grassley. Thank you.

2 I am going to ask Mr. Wainstein and Mr. Olsen, based on
3 your experience serving in Government, what else can you
4 tell us in this unclassified setting about the value of 702
5 surveillance and how it has been used? And how would it
6 affect our intelligence capability if Congress failed to
7 reauthorize?

8 Mr. Wainstein. Thank you, Chairman Grassley. I will
9 be brief and then turn it over to Mr. Olsen, who has more
10 current information since he recently left Government.

11 I was the Homeland Security Adviser in 2008 when the
12 FISA Amendments Act was passed. At that point, as you
13 recall, the intelligence community was already collecting
14 surveillance intelligence through the PROTECT America Act,
15 which is sort of the stop-gap legislation that preceded the
16 FISA Amendments Act. And you could see even at that point
17 the richness of the information that was coming into the
18 reporting that got all the way up to the White House. You
19 could tell it was really a major step forward. And as I
20 mentioned in my remarks earlier, that is critical. It is a
21 critical remedy for the problem that arose with the changing
22 technology over the time between 1978 and when the FISA
23 Amendments Act was passed in 2008. If we were to go back to
24 that point, we would be back in the same situation where we
25 have way too many surveillances that are critical to carry

1 out and not enough manpower to do individualized orders for
2 each of them.

3 Chairman Grassley. Mr. Olsen?

4 Mr. Olsen. I essentially agree with Mr. Wainstein. I
5 was in the Justice Department before the FISA Amendments Act
6 was passed. We were at that time having a very hard time
7 keeping up with the number of terrorist targets that we were
8 trying to track who were not U.S. persons, who were located
9 overseas. We were seeking individualized warrants. The
10 system was overwhelmed with the effort to try to get
11 individualized probable cause warrants for individuals who
12 were not entitled to that level of Fourth Amendment
13 protection.

14 The FISA Amendments Act changed that in a way
15 consistent with the Constitution. To go back to that,
16 especially in the current threat environment, would, I am
17 confident, overwhelm executive branch and judicial
18 resources.

19 I also will say, in terms of the value today, my last
20 post at the National Counterterrorism Center, as I
21 mentioned, I saw the value almost on a daily basis of FAA
22 reporting. It was typical for analysts in the reports to
23 say this came from FAA or 702 collection. And the PCLOB
24 cited 30 cases in their report based on their classified
25 review--or their ability to see classified information, 30

1 specific cases in which Section 702 was the initial catalyst
2 that identified previously unknown terrorist operatives or
3 plots. So that is 30 cases that the PCLOB was able to cite
4 that were otherwise unknown.

5 Chairman Grassley. Ms. Brand, about some people's
6 suggestion that we get judicial approval or even a warrant
7 before querying the database of 702 with a U.S. person's
8 phone number or email, in your testimony a moment ago you
9 mentioned one reason you thought this was not a good idea.
10 Are there other reasons that you can describe for us that,
11 in your view, make such requirements problematic?

12 Ms. Brand. Thank you, Mr. Chairman. Yes, I will
13 mention two. One is that I am not sure it would further
14 protect privacy to do that. And, number two, I am not sure
15 it would be workable.

16 With respect to privacy, a query is a relatively
17 unintrusive tool. It is less intrusive for the Government
18 to look at the information it already has than to go out and
19 collect more information about a person. But if we require
20 judicial approval before a query can be conducted, the
21 Government will have to assemble a package for the FISA
22 Court, which presumably will require the Government to go
23 out and get more information, which means you would require
24 a more intrusive means to justify the use of a less
25 intrusive means. And that seems backwards to me.

1 In terms of workability, as I said before, the FBI does
2 not distinguish between U.S. person queries and other
3 queries because it is normally irrelevant. If an agent or
4 an analyst is doing a bank fraud investigation and they want
5 to see what the FBI knows about somebody, they are not going
6 to indicate whether it is a U.S. person or not because there
7 is no reason to ask that question. So it is not clear to me
8 how you could find a workable system of requiring judicial
9 approval for U.S. person queries without requiring judicial
10 approval for all queries. And because the FISA Court
11 process is so cumbersome and time-consuming, that would
12 likely result in no queries, which would then prevent the
13 discovery of any connections between 702 information and
14 other investigations, which I think would be a mistake.

15 Chairman Grassley. Okay. A follow-up for Mr.
16 Wainstein and Mr. Olsen. Based on your experience in law
17 enforcement and the intelligence community, what would the
18 operational effect be of subjecting these queries to
19 judicial approval?

20 Mr. Olsen. I agree with Ms. Brand. It is hard to
21 predict. But it is certainly the case, having worked in the
22 National Security Division at Justice, that that would slow
23 down the process of simply searching through information
24 that was lawfully collected. The attorneys in the National
25 Security Division, working with whether it is the FBI or

1 NSA, would have to compile applications to the Court. Now,
2 in cases the Court can move quickly. It has proven it can
3 move quickly. But there is no doubt that it would become a
4 more cumbersome and slow process in instances where I am
5 confident that agility and speed is critical. So I think
6 without really any gain from a privacy perspective and
7 against a record that does not have any indication of abuse
8 in terms of the current approach of allowing these agencies
9 to conduct these searches without judicial approval.

10 Chairman Grassley. I am going to--go ahead.

11 Mr. Wainstein. Thank you, Mr. Chairman. Just to add
12 to that, just keep in mind that that kind of requirement is
13 not in place for, let us say, information collected--
14 incidentally collected communications under Title III, which
15 is the criminal wiretap statute. And so it is a bit ironic
16 that you would impose that requirement in the national
17 security context where often you are trying to prevent
18 something from happening, like a terrorist attack, where
19 speed is of the essence, and not require it in the criminal
20 context, where speed is of less importance.

21 Chairman Grassley. Okay. Senator Leahy? And then the
22 Senator from Texas. I am going to step out just for a
23 minute, but you two go ahead.

24 Senator Leahy. Thank you. I think everybody agrees we
25 want to keep the country safe. I do appreciate numbers

1 being tossed around here. I always worry, though, what is
2 behind the numbers. We heard on a different issue from the
3 NSA about 52 attacks that their wiretaps stopped, and the
4 numbers are always given, until they testified in public and
5 the 52 became a dozen, which became 5, which became part of
6 one after the fact and following up on an FBI investigation.

7 I am not suggesting these are exactly the same here,
8 but I always worry about numbers. We were assured, however,
9 at that time that Americans' privacy was protected because
10 of the tough security measures NSA had. They were not good
11 enough to stop a 28-year-old from stealing all the
12 information and bringing it to China and Russia, but,
13 otherwise, they were very protective of American rights.

14 Part of this worries me. I want us to be secure. But
15 I also want--I mean, we could be very secure if we put a
16 tail on every single American and searched every single
17 American's company and phone. None of us are suggesting
18 that. But I worry if we do parts of that.

19 So let me ask you, Ms. Goitein, why do you agree with
20 the Review Group that Congress should require a court order
21 based on probable cause?

22 Ms. Goitein. I think to understand what is so
23 disturbing about back-door searches, you have to look at
24 what comes before them. In order to fit its way into the
25 foreign intelligence exception, as it is called, to the

1 Fourth Amendment and in order to avoid getting a warrant or
2 getting an individual FISA order, the Government has to
3 certify to the FISA Court not only that it is targeting a
4 foreigner not an American, not only that it has a foreign
5 intelligence purpose, but also that it is not doing any
6 reverse targeting, which means it has no intent to target
7 any particular known Americans.

8 Then having made that certification, as soon as the
9 data is obtained, all three agencies can sort through the
10 data, looking for the communications of the very particular
11 known Americans in which the Government just disclaimed any
12 interest. And the FBI does not even need a foreign
13 intelligence purpose to do it. The FBI can search for
14 evidence in criminal cases that have no national security or
15 foreign intelligence component whatsoever.

16 So this is a bait-and-switch that undermines the spirit
17 if not the letter of the reverse targeting prohibition.
18 And, more important, it undermines the purpose of that
19 prohibition, which is to ensure that Section 702 does not
20 become an end run around the Fourth Amendment's requirement
21 and around the FISA Court's--the FISA's individual order
22 requirement when an American is a target.

23 And I would note one more thing, which is that the
24 President's Review Group on Intelligence and Communications
25 Technologies, which included a former Deputy Director and

1 Acting Director of the CIA, a former Chief Counterterrorism
2 Adviser to President George W. Bush, recommended a warrant
3 to search Americans' communications. They were not trying
4 to rebuild the wall. They were trying to protect Americans
5 from warrantless surveillance, and that is what closing the
6 back door is about.

7 Senator Leahy. Well, some have argued that we should
8 not worry because Section 702 programs or these minimization
9 procedures limit the use of retention of this information.
10 So I would ask both you and Professor Medine, do you believe
11 the current minimization procedures ensure that data about
12 innocent Americans is deleted? Is that enough?

13 Mr. Medine. Senator Leahy, they do not. The
14 minimization procedures call for the deletion of innocent
15 Americans' information upon discovery to determine whether
16 it has any foreign intelligence value. But what the Board's
17 report found is that, in fact, information is never deleted.
18 It sits in the databases for 5 years or sometimes longer.
19 And so the minimization does not really address the privacy
20 concerns of incidentally collected communications, again,
21 where there has been no warrant at all in the process. And
22 when the Government shifts its attention from the non-U.S.
23 person to the Americans' communications, there should be
24 court approval in that exchange.

25 As mentioned earlier, in Title III there has been a

1 warrant before the information was collected. In the United
2 States, we simply cannot read people's emails and listen to
3 their phone calls without court approval. And the same
4 should be true when the Government shifts its attention to
5 Americans under this program.

6 Senator Leahy. Do you agree with that, Ms. Goitein?

7 Ms. Goitein. I do agree with that. I think that there
8 is this idea that if the Government has collected the
9 information lawfully, it should be able to use it for any
10 legitimate Government purpose. And whatever truth that may
11 have in other contexts, it is clearly not the case with
12 Section 702 because Congress has required minimization.
13 Minimization is the opposite of you can use it for any
14 purpose you want. And, constitutionally, it is not the case
15 either because the reasonableness inquiry includes an
16 assessment of whether the safeguards on Americans' data are
17 sufficient.

18 Senator Leahy. Thank you.

19 Senator Cornyn?

20 Senator Cornyn. Well, thank you all for being here. I
21 am actually encouraged that everybody on the panel,
22 including the people sitting up here, agree that targeting
23 foreign intelligence sources using 702 has been not only
24 demonstrated as constitutional but also as effective. And
25 so the question to me is: Do we want to somehow limit

1 ourselves in terms of access to foreign intelligence in a
2 way that could make us less safe? And that is an important
3 conversation to have, but I am pretty clear on where I come
4 down.

5 So the concern is, of course, with what is happening in
6 Syria and with the growth of the Islamic state or DAESH or
7 whatever you want to call it, with the meltdown in Libya
8 where you are seeing a pathway of foreign fighters now
9 making their way into Europe, where, of course, they do not
10 need a passport to travel among various member states of the
11 European Union, and many of those countries have visa waiver
12 programs with the United States, whether people can gain
13 access to the United States, or whether they can just, as in
14 the case of San Bernardino, radicalize people in place,
15 although obviously the two individuals involved there had
16 traveled to the Middle East as well.

17 So I think it is really important that we understand
18 what the process is, obviously, a lot of oversight by the
19 FISA Court, which many of my colleagues say is very
20 important to them; by the Director of National Intelligence,
21 the ODNI; the Department of Justice. There is a lot of
22 oversight here and a lot of effort to try to minimize the
23 impact on American citizens, although the fact of the matter
24 is, as I understand it under 702, that the only American
25 citizens who will be impacted by this process without a

1 court order will be those who are communicating with a known
2 terrorist target overseas. Now, that is not exactly an
3 innocuous purpose, it seems to me.

4 So, Mr. Olsen, I wonder, just briefly, if you could
5 talk a little bit more about what efforts have been built
6 into this program to minimize the breadth of the sweep of
7 this program in a way that might otherwise pick up American
8 citizen communications, in a way that really, frankly, the
9 intelligence community could care less about.

10 Mr. Olsen. Thank you, Senator. And as you mentioned,
11 one of the hallmarks of the legislation is that all three
12 branches of Government play a central role in ensuring that
13 the law is implemented in a way that protects privacy and
14 civil liberties. Certainly, the executive branch agencies
15 that implement the law are on the front lines of oversight
16 and compliance. The FISA Court plays a robust role. Having
17 been a Federal prosecutor for years, I can tell you that the
18 Court is not a rubber stamp. It is aggressive and assertive
19 in its oversight of the cases it handles. And, of course,
20 this Committee and the Intelligence Committees play a
21 significant role. So all three branches of Government are
22 involved in overseeing this authority.

23 With respect in particular to U.S. person information
24 and the minimization procedures, as the PCLOB found, those
25 procedures were consistent with the Fourth Amendment and

1 they were consistent with the statute. In fact, that is the
2 exact opinion that Judge Hogan recently reached last fall in
3 a case that was declassified recently, an 80-page opinion by
4 Judge Hogan finding that the Government's recent
5 certification was constitutional and complied with the law;
6 and, in particular, that the use of FBI queries of 702--the
7 issue that we have been discussing--was also consistent with
8 the law and with the Constitution.

9 Senator Cornyn. Under the Fourth Amendment, the issue
10 is whether the search is reasonable, right?

11 Mr. Olsen. Yes, generally.

12 Senator Cornyn. It is not an outright--I think some
13 people are suggesting there is some outright prohibition
14 here. But under the protective mechanisms, as you say,
15 built into the statute, the courts have upheld access to the
16 communication by an American citizen with somebody who we
17 know is a target for foreign intelligence purposes.

18 I know Mr. Medine did not mean this seriously, but he
19 mentioned sweeping up love letters. My staff tells me that
20 there was a significant case recently, the Zazi case, where
21 terms like "wedding cake" and "marriage" were used as code
22 words that the terrorists used to plot attacks against the
23 United States. I do not know. Mr. Olsen, is that something
24 you can talk to us about?

25 Mr. Olsen. Well, certainly the Zazi case was one of

1 the key cases that the Government has referred to over the
2 last several years as an example of the value of the
3 program.

4 Senator Cornyn. In other words, in our zeal to protect
5 love letters, we do not want to protect terrorists who use
6 code words that might otherwise escape scrutiny by the
7 intelligence community. Is that not one of the--

8 Mr. Olsen. That is absolutely right, and I can give a
9 very brief example, hypothetical.

10 Senator Cornyn. Please.

11 Mr. Olsen. Two foreign terrorist targets in Syria
12 communicating with each other, targets of 702, this is
13 hypothetical. Say they share a passport photo of an
14 American. That would be viewed by--you know, potentially
15 viewed by the NSA in the collection under 702. That
16 passport photo could be innocent. Right? It could be just
17 two people sharing a photo of somebody they know. But it
18 certainly would be of significant interest to the FBI and
19 the NSA to not only collect that information incidentally
20 about that U.S. person, but then to be able to search 702
21 quickly to say, "Okay, who is this person? Do we have other
22 information in our 702 databases and other databases?"

23 I think that is exactly, from my perspective coming
24 from the National Counterterrorism Center, what we would
25 want to be able to do quickly.

1 Senator Cornyn. Thank you.

2 Mr. Olsen. And without probable cause, if I may add.
3 There may not be probable cause to do that. But certainly
4 that would be within the statute, as Judge Hogan has found.

5 Senator Cornyn. We talked about the wall between law
6 enforcement and intelligence, and obviously probable cause
7 is critical under the Fourth Amendment. You are talking
8 about a prosecution under the Fourth Amendment where an
9 American citizen's rights under the Bill of Rights has to be
10 protected by a court order requiring the showing of probable
11 cause. Terrorists do not have any protection of the Fourth
12 Amendment, nor is probable cause required to get that
13 information. That is, I think, the point we need to
14 continue to hammer home because I think people are a little
15 bit confused about that.

16 Thank you, Mr. Chairman.

17 Chairman Grassley. Senator Feinstein.

18 Senator Feinstein. Thanks very much, Mr. Chairman, and
19 thank you for holding this hearing because it does give us a
20 little bit of an advance on the hearings that will be held
21 certainly next year. And so I very much--and I want to
22 commend those who serve on the PCLOB board. Thank you for
23 your service. And, Matt Olsen, it is good to see you again,
24 and thank you so much for your service. It is very much
25 appreciated.

1 As a long-term member of the Intelligence Committee,
2 about 15 years now, we see the value of this program
3 frequently. The problem is that the Government has been
4 reluctant to declassify sufficient numbers of cases so the
5 public gets an understanding of the value of the program.
6 And the Zazi case has been used in the 215 situation; it is
7 used intensively in the 702 situation. So for anyone that
8 is listening, it is really important to declassify more of
9 these, to show the value of this program.

10 Those of us that meet two afternoons a week and go over
11 intelligence and hold hearings and read the intelligence see
12 the value of the program. But I think the general public
13 does not. I see it as practical, as prudent, and as
14 maintaining constitutional guarantees.

15 I have just been reading the Director of National
16 Intelligence's unclassified report on the ability to query
17 Section 702 using U.S. person identifiers as an essential
18 national security tool. And I would just like to read a
19 couple of things and then ask that you all comment on them.
20 And he is talking about using a U.S. person identifier and
21 saying that it would impede and in some cases preclude the
22 intelligence community's ability to protect the Nation
23 against international terrorism and other threats. And then
24 he discusses that such a requirement is not required by the
25 Fourth Amendment, that it would be impractical, and that it

1 is rare that the intelligence community begins an
2 investigation having already developed probable cause. And
3 I think that has been said by one of our witnesses.

4 I would like to ask Mr. Medine and others to comment on
5 the text of your recommendation. There are 22 of them. You
6 say many have already been accepted by the Government, but
7 the one I am curious about is on page 16, Recommendation 2,
8 updating the FBI's minimization procedures to accurately
9 reflect the Bureau's querying of 702 data for non-foreign
10 intelligence matters and place additional limits on the
11 FBI's use of Section 702 data in such matters.

12 Would you comment on that, please?

13 Mr. Medine. Thank you, Senator Feinstein. One of the
14 things that our Board discovered in our 702 investigation
15 was, as Board Member Brand indicated, that the FBI routinely
16 looks into 702 databases, and not just in investigations but
17 even in assessments. When the FBI has absolutely no
18 suspicion of wrongdoing but they are just entitled to poke
19 around and see if something is going on, they nonetheless
20 access--query the 702 database. But the FBI's minimization
21 procedures were not transparent about that process--

22 Senator Feinstein. Stop for a minute. Are you saying
23 that the PCLOB believes that there should be a FISA board
24 approval prior to querying?

25 Mr. Medine. The PCLOB majority did not support FISA

1 approval, but Judge Patricia Wald and I--Judge Patricia Wald
2 is a member of the Board--dissented from the Board's report
3 and did call--

4 Senator Feinstein. Well, would you please put--because
5 I think this is going to come up. Would you please put
6 before this body both sides of the question?

7 Mr. Medine. Sure. On the side of having a query, as I
8 mentioned earlier, under the Fourth Amendment the Government
9 is now accessing Americans' personal communications--and I
10 did want to clarify one point earlier. This program does
11 not just target terrorists. I think it might be a very
12 different situation if the only focus was terrorists. This
13 program targets anyone with foreign intelligence value. It
14 could be a completely innocent businessman or anyone else
15 out of the country who has that information. And so we have
16 an American talking to someone who is potentially innocent
17 of any wrongdoing and yet capturing that American's
18 communications. It could be a love letter; it could be a
19 business transaction. But all those are being captured.
20 And the question is: When we shift our attention to those
21 communications, should we have court approval?

22 Senator Feinstein. All right. I want to hear the
23 other side of the question. Ms. Brand, would you please--

24 Ms. Brand. Thank you, Senator Feinstein. It is
25 important to keep in mind--when you are talking about the

1 FBI and queries of 702 data, you have to keep in mind the
2 scope of the issue. The FBI does not get any upstream data,
3 so there are two aspects of 702, as you know. There is
4 PRISM and there is Upstream. Upstream is more concerning
5 from a privacy standpoint because there could be "about"
6 collection and so forth. The FBI does not get any of that
7 data. They get a subset of 702 data.

8 Now, when concerns are raised about queries of 702
9 data, the concern is not raised about querying 702 data in a
10 national security investigation--because everyone seems to
11 agree that in a national security investigation you ought to
12 be able to query 702 data--but querying that data in other
13 investigations.

14 When we were doing our 702 report, in discussing this
15 issue with the FBI, they were not able to give us any
16 example of that ever having happened. So it is at the very
17 least extremely unlikely, and, in fact, when Judge Hogan
18 wrote his opinion recently, he referred to this possibility
19 as remote if not entirely theoretical. So it is extremely
20 unlikely that 702 information is ever going to come back in
21 a regular criminal investigation. But as I said in my
22 opening statement, if there is a connection there, you want
23 it to be discoverable. So that was the other side of the
24 story.

25 Senator Feinstein. Thank you.

1 Thank you, Mr. Chairman.

2 Chairman Grassley. Yes. Now, Senator Tillis.

3 Senator Tillis. Thank you, Mr. Chair. And I was glad
4 to hear Senator Feinstein talk about the value of this
5 program. She has insights that many of us who are not on
6 intelligence would not have, so I think it is very important
7 for the American people to understand why this is a very
8 useful tool and important tool.

9 Back to the point about declassification, I would guess
10 that some of the apprehension around declassifying some of
11 the other cases could relate to other bad actors reverse
12 engineering how they can avoid detection if they know what
13 patterns were used to identify and thwart the other event so
14 I can kind of see that it is not just merely because they
15 want to keep it private. There are probably legitimate
16 future risks that could result in understanding how this
17 data was triangulated and used to thwart an existing attack.
18 Is that correct, Mr. Olsen?

19 Mr. Olsen. I think that is generally exactly right.
20 The ability to understand how the Government collects this
21 type of information is something the Government certainly
22 does not want in the public record.

23 Senator Tillis. And, Ms. Brand, I wanted to go back to
24 the last question Senator Feinstein asked because in your
25 opening comments you talked about the irony of requiring a

1 court order before you get access to the 702 data, actually
2 requiring more information to be captured before you could
3 move forward with a query. Can you talk a little bit about
4 that? I think it also speaks to the elongation of the
5 process of the investigation, because while the FISA Courts
6 may be able to move reasonably quickly after the information
7 is gathered, there is time associated with gathering that
8 information. Can you talk a little bit about that?

9 Ms. Brand. Sure, and then I will hand it off to Mr.
10 Olsen and Mr. Wainstein, who have more practical experience
11 with the investigative process than I do. But, in general,
12 investigations progress from using less intrusive means to
13 using more intrusive means. At the beginning of the
14 investigation, you may just have a tip, and you want to
15 figure out whether to pursue that tip or not do anything.
16 And so you will start by doing a query of databases to see
17 what you already know and see if it is worth pursuing.

18 Then as the investigation proceeds, you may develop
19 enough information to satisfy a probable cause requirement
20 for a search warrant or a wiretap or so forth. But at the
21 very initial stages of the investigation, you typically do
22 not have much information, and that is why you do a query.

23 To then require the Government to compile more
24 information in order to start with the less intrusive means,
25 that just does not make sense to me. But Mr. Wainstein and

1 Mr. Olsen may have more insights into that.

2 Senator Tillis. Mr. Wainstein?

3 Mr. Wainstein. Thank you, Senator. I just want to
4 address the speed issue, and I think that is something that
5 people need to focus on. Mr. Olsen and I have been through
6 a number of different threat investigations where there is
7 an indication of a threat, maybe somebody here in the U.S.,
8 and at that point you want the intelligence community
9 operators to get access immediately to every area that there
10 might be relevant information. And while the FISA Court
11 does act quickly, the process of having to put together that
12 information not only being more intrusive in relation to
13 U.S. person privacy, it just takes time. And that time
14 could be absolutely critical in a hot threat investigation.
15 We have seen that over and over, over the years.

16 Senator Tillis. Ms. Goitein?

17 Ms. Goitein. Would you mind if I speak to the privacy
18 issue a little bit as a representative of the civil
19 liberties community here?

20 Senator Tillis. Please.

21 Ms. Goitein. I would hope that this Committee would
22 take note of the fact that the privacy community is
23 unanimously behind the requirement of a warrant because it
24 is our considered opinion that this is far more protective
25 of privacy to require a warrant than to allow queries of

1 that data.

2 Senator Tillis. Ms. Goitein, are you aware of any
3 examples to this point here it would be likely that the
4 warrant would be denied? I am trying to find the--and here
5 is the reason why I am concerned with this. We are in an
6 environment where the number and the severity of threats,
7 according to leading people in the intelligence community,
8 are at an all-time high. And so time is not only--it is not
9 only the investment in time, but it is also the investment
10 in resources. We need to be able to identify and cast as
11 wide a net as possible.

12 So I am trying to figure out--I understand your
13 concern, and I am sympathetic to it. The question is: Have
14 we seen this necessarily produce a systemic risk that has
15 actually resulted in legitimate violations of someone's
16 Fourth Amendment rights?

17 Ms. Goitein. I think the search itself is the
18 violation of the Fourth Amendment right. I know Mr. Olsen
19 said there was no evidence of abuse of back-door searches.
20 Back-door searches are the abuse. It is a warrantless
21 search of Americans' communications that were gathered based
22 on a representation that the Government was not targeting
23 Americans.

24 Senator Tillis. And this is a search of data that the
25 Government is already in possession of?

1 Ms. Goitein. It is a search of data that the
2 Government is required by law and by the Fourth Amendment to
3 minimize the use and access to U.S. person information.

4 Senator Tillis. And, Mr. Medine, I had a question for
5 you in my remaining time. In your opening comments, did I
6 understand you to say that the PCLOB did not necessarily
7 recommend any legislative action but there were additional
8 changes that should be--I was trying to reconcile that. Is
9 that correct? Would that suggest then that the acts as they
10 currently stand are sufficient, the implementation needs to
11 be modified or adjusted?

12 Mr. Medine. Senator, it is correct that the Board only
13 recommended administrative changes, and as I mentioned
14 earlier, the Government has been very responsive to those
15 and has implemented or is in the process of implementing
16 those. One of the other Board members, Judge Wald, and I
17 did dissent and did recommend the requirement of a court
18 approval.

19 If I could also add on the classification front, one of
20 the things the Board experienced in preparing its report is
21 that we found some facts about the 702 program that we
22 thought could be made public without harming national
23 security. And we had a very positive dialogue with the
24 intelligence community, as a result of which there are 100
25 facts in our report that had been previously classified that

1 the intelligence community felt could be declassified and
2 allow for a greater public debate about this program.

3 Senator Tillis. Thank you.

4 Thank you, Mr. Chair.

5 Chairman Grassley. Yes.

6 Senator Feinstein. Mr. Chairman, may I just know which
7 report that is? Is that the Recommendations Assessment
8 Report you are speaking of?

9 Mr. Medine. Senator, it is the 702 report. It is our
10 almost-200-page report on the 702 program. And, again, we
11 were able to have greater transparency about the program.

12 Senator Feinstein. I think it would be valuable if we
13 could add these documents to the record, Mr. Chairman.

14 Chairman Grassley. Yes, without objection, they will
15 be added.

16 [The information follows:]

17 / COMMITTEE INSERT

1 Chairman Grassley. I think Senator Franken is next.

2 Senator Franken. I am ranking, so I am going to stay
3 here for the remainder of the hearing. So I would yield to
4 Senator Whitehouse.

5 Chairman Grassley. Senator Whitehouse.

6 Senator Whitehouse. Thank you, Chairman.

7 First, let me welcome Ken Wainstein back to the
8 Committee. He and I were on adverse sides of a considerable
9 number of issues during the Bush administration, but he was
10 always an entirely honest and honorable broker on his side,
11 and I think we worked well together. And it is nice to see
12 you back before the Committee.

13 You mentioned the comparison between incidental
14 collection under Fourth Amendment searches and under the 702
15 program. And, of course, if you go back to the earliest
16 days of the warrant requirement, when somebody had a search
17 warrant and was able to go into somebody's desk and search
18 their papers with that warrant, their papers were not just
19 their papers; their papers were notes that they had made
20 about their letters out and also their letters in. And so
21 there was incidental collection of people who were not the
22 subject of the search warrant from the earliest days of the
23 Republic.

24 When we got into wiretapping, it became a little bit
25 more complicated, but once again, you cannot listen in to

1 the conversations of a mobster without listening in to the
2 other side of that conversation. And so wiretaps over and
3 over and over again engaged in incidental communication. So
4 there is really nothing new--incidental collection. So
5 there is really nothing new about incidental collection of
6 people who are not the subject of the investigation in
7 question.

8 It strikes me that what is new is the creation of a
9 database to preserve the incidental collection and the
10 question of minimization. Now, minimization I do not think
11 really applied back in the search warrant days other than
12 that there was obliged to be a return ultimately of the
13 product. I guess that was the minimization of its era.

14 In the wiretap era, FBI agent listening in on a
15 mobster's conversation, once it turned out it was their mom
16 or that they were placing an order at the butcher's, you
17 were required to switch off and not listen, and then check
18 back in to see if the conversation had changed to something
19 inculpatory, but you would be switching on and off.

20 Could you just elaborate a little bit more on how
21 modern Fourth Amendment search techniques and storage of
22 that data takes place in the domestic context under the
23 Fourth Amendment search requirements and compare the
24 minimization and the database collection to what we see with
25 the 702 program?

1 Mr. Wainstein. Thank you, Senator. Thank you for
2 those kind remarks, and I share those sentiments completely.
3 It was a pleasure to work with you over the years.

4 Your question is, as usual, a very good one. Let me
5 break it down into two different questions.

6 First, in terms of the database, you are right that
7 under 702 there is the need, especially in the national
8 security context, to pool data that might be relevant for
9 the very reason that we discussed earlier, that when you
10 have a threat, you have an indicator of a threat, you want
11 to be able to access all that information at once, not go to
12 different databases or every different agent who collected
13 from one particular target. So, yes, it is pooled, in the
14 way that often Title III take is not pooled, where you have
15 a Title III wiretap in one criminal case in this district
16 collected by the FBI in one place and maybe not pooled with
17 Title III conversations elsewhere. But as a doctrinal, as a
18 legal matter, they are indistinguishable in the following
19 way:

20 In terms of Title III, you are right, there is
21 minimization. It is minimization, though, that if I am the
22 target, the Government is duly authorized to collect on me,
23 and I am talking to the pizza delivery guy, the agent is
24 supposed to turn it off and then turn back in some interval
25 of time later to see whether I am then talking to, you know,

1 my terrorist confederate or my drug-dealing confederate.

2 But the reality is if they are listening and I am
3 talking to somebody else and that information is
4 incidentally collected on this other person, it is
5 collected, and that person's--regardless of whether that
6 person is involved in the criminal activity or not, and that
7 person's privacy has not been reviewed by a judge, the judge
8 that issued the warrant that authorized the collection
9 against me. And that is the same thing that is happening in
10 702, and the other person, the counterparty in the
11 conversation, has just the same limited rights to resist the
12 Government's ability to listen to that conversation as the
13 counterparty, the pizza guy, the guy in my situation.

14 Senator Whitehouse. I guess, to use your word, the
15 doctrinal question we face is once that has been
16 legitimately collected and then the Government puts it into
17 a database and enables itself to go and search it at will in
18 a large pooled database, should that be seen as a secondary
19 event that suggests the requirement for some gatekeeper
20 before they have full access?

21 My time has expired, so I cannot continue the
22 conversation any further, but thank you, Chairman, for the
23 hearing.

24 Chairman Grassley. Senator Klobuchar.

25 Senator Klobuchar. Thank you very much, Mr. Chairman,

1 and thank you to Senator Franken for his good work in this
2 area and for allowing me to go before him. That was nice.

3 Thank you for all you have done, and like Senator
4 Whitehouse, I have had experience with this before. For 8
5 years I managed a prosecutor's office with about 400 people
6 and have been personally in the room for some of these
7 wiretaps. They were not Federal wiretaps. They were local
8 ones. But as many of you noted in your testimony, it is
9 critical that our laws reflect this balance between national
10 security interests and privacy and civil liberties. That is
11 one of the reasons I cosponsored and voted for the
12 bipartisan USA FREEDOM Act. And what I wanted to ask you
13 about was that bill itself as we look at the reauthorization
14 ahead and what we should be doing when we consider any
15 changes to the law.

16 As Section 702 is currently constituted, do you believe
17 that it strikes the appropriate balance between the
18 protection of national security and civil liberties? And
19 what changes would you like to see? We can go down the line
20 here. Mr. Wainstein?

21 Mr. Wainstein. Thank you, Senator. Yes, I do think it
22 strikes the right balance, and I believe it does that by
23 providing for ample oversight, which is meaningful
24 oversight, by all three branches. And then also I think you
25 see that balance being played out in terms of the internal

1 procedures that are implemented by the intelligence
2 community, which are reviewed by the FISA Court and then
3 also by the Intelligence and Judiciary Committees, and have
4 resulted in the finding by the Privacy and Civil Liberties
5 Oversight Board with a finding that there have been no
6 instances of intentional misuse of authority, which I think
7 is very meaningful.

8 Senator Klobuchar. All right. Thank you.

9 Mr. Olsen?

10 Mr. Olsen. I also, Senator, believe it should be
11 reauthorized. I was, along with Mr. Wainstein, part of the
12 effort in the executive branch in 2008, behind the passage
13 of the law and can attest to the way in which it was
14 calibrated at the time to make compromises on both sides, I
15 think, to achieve an appropriate balance. But it has also
16 not been static. The implementation of the law has been
17 dynamic and has changed over the years, and, in particular,
18 what I think really is a landmark report by the Privacy and
19 Civil Liberties Oversight Board, which did an intensive and
20 thorough investigation, found that the law was not only
21 valuable but also constitutional and legal, made
22 recommendations which then the executive branch has
23 implemented.

24 Senator Klobuchar. One of the concerns Ms. Goitein
25 raised in her testimony was that there was too much data to

1 analyze. Do you think there is merit to that?

2 Mr. Olsen. I did read that part, and I, with respect,
3 do not think there is merit in that. I served at the
4 National Counterterrorism Center. I can tell you that more
5 data of this type, 702 data, is better than less. The
6 Government has the ability with that data to search it, and
7 we talked about that, search it, process it, and find--has a
8 better chance of finding those needles that we are looking
9 for when we are trying to stop a terrorist attack.

10 So that can be a concern in other contexts. I
11 understand that more data might just obfuscate the needle.
12 In the 702 context, I do not think that is a persuasive
13 argument.

14 Senator Klobuchar. Thank you.

15 Ms. Goitein?

16 Ms. Goitein. So I believe that Section 702 goes much
17 further than it needs to go in order to accomplish the aims
18 that I think we all want to see accomplished. And I would
19 point out that some of the cases--in fact, all of the cases
20 that have been made public relating to Section 702 successes
21 are cases in which the surveillance, the Section 702
22 surveillance, was of a known or suspected terrorist or
23 someone known or suspected to have ties to terrorism. So
24 while these are certainly evidence of Section 702 working,
25 they do not support the idea that Section 702--

1 Senator Klobuchar. And so what would you--

2 Ms. Goitein. --needs to be--

3 Senator Klobuchar. I just want--

4 Ms. Goitein. I am sorry. I realize that you are short
5 on time.

6 Senator Klobuchar. Yes.

7 Ms. Goitein. So the Brennan Center's position is that
8 the only way to secure the constitutional validity of
9 Section 702 is to have an individual order when the
10 Government collects communications between a foreign target
11 and an American, but there are many, many other steps that
12 could be taken to improve Section 702. That includes
13 closing the back-door search loophole. It includes
14 narrowing the definition of "foreign intelligence,"
15 narrowing the pool of people who can be targeted, so it is
16 not just any foreigner overseas, and ensuring that notice is
17 given anytime that Section 702 evidence is used in court or
18 evidence derived from Section 702 is used in legal
19 proceedings.

20 Senator Klobuchar. Do you want to add anything, Mr.
21 Medine and Ms. Brand?

22 Mr. Medine. Senator, I would recommend three
23 legislative changes: one is require the Government to
24 estimate the number of Americans' communications that are
25 intercepted under 702; second is tighten up the upstream

1 "about" collection process; and third is to require court
2 approval for queries of Americans' information under 702.

3 And following up on Senator Whitehouse's point, there
4 has been no warrant issued for these collections, and when
5 the attention shifts to Americans' communications that are
6 collected over a 5-year period with any of 90,000-plus other
7 people outside the United States, I think it becomes a
8 moment within the Fourth Amendment would require a court
9 approval.

10 Senator Klobuchar. Okay. Thank you.

11 Last but not least, Ms. Brand?

12 Ms. Brand. Thank you, Senator Klobuchar. I would urge
13 Congress to reauthorize Section 702, and I do not think any
14 changes to the statute are necessary. I would note that the
15 PCLOB in our very in-depth review of the program and our
16 lengthy report did not recommend any legislative changes.
17 We did recommend a number of changes to the way the program
18 operates that could be implemented by the administration or
19 the FISA Court, and almost all of them have been already
20 implemented. The Government is continuing to work on some
21 others, so I think those are the appropriate way to handle
22 it.

23 Senator Klobuchar. Okay. Thank you to all of you.
24 Thanks.

25 Chairman Grassley. Senator Blumenthal.

1 Senator Blumenthal. Thank you, Mr. Chairman.

2 Welcome to this very important and helpful panel. This
3 is a very complex topic, and you have given some very
4 insightful and intelligent responses to difficult questions.

5 Having spent a good part of my career before this job
6 in various courtrooms, I am a strong believer in the
7 importance of the adversarial process in ensuring that a
8 court has the best possible information to make decisions,
9 and as a result, I proposed some years ago that a special
10 advocate be established to argue before the FISA Court, as
11 you know, in cases presenting particularly novel legal
12 issues. And I am pleased that a version of this proposal
13 was incorporated in the USA FREEDOM Act. I know that
14 enabling the FISA Court to hear independent views was among
15 the PCLOB's recommendations, for which I thank you, and that
16 a panel of outside lawyers has been established,
17 accordingly, and that on several occasions the Court has
18 actually appointed one of them to serve as amicus.

19 So let me begin by asking Mr. Medine, but this is
20 really a question for the entire panel: Could you discuss
21 why the PCLOB initially recommended this change and how you
22 have assessed the process of implementation, and then also
23 whether a technical expert will be shortly appointed to
24 fulfill the role that was envisioned by the statute?

25 Mr. Medine. Senator Blumenthal, the origin of the

1 recommendation was the PCLOB's first public workshop. We
2 invited a former judge from the FISC Court to testify about
3 his experiences, and he said how frustrating it was as a
4 judge to only hear one side. He said in his normal civil or
5 criminal docket he hears one side make an argument, sounds
6 pretty persuasive; then the other side makes an argument,
7 that sounds pretty persuasive, too; and the judge's role is
8 to reconcile those competing views, but when he was on the
9 FISC, he only heard one side. And that led the Board to
10 ultimately recommend that there be another side,
11 particularly in cases having novel, legal, or technological
12 considerations like programmatic approvals of 215 or 702.

13 I think we have just begun to see how that program is
14 operating, so I think it is too early to test, but I think
15 it is encouraging that an advocate, an amicus was appointed
16 and that the amicus was able to make arguments. And we also
17 support having technical advice as well because a lot of
18 these programs have important technological implications.
19 Our Board has just brought on our first technology scholar
20 to advise us on these issues, and I think blending the other
21 side of law and technology is important to make the court
22 process work better.

23 Ms. Brand. May I jump in, Senator Blumenthal?

24 Senator Blumenthal. Ms. Brand, yes.

25 Ms. Brand. As a member of the PCLOB as well who signed

1 on to the recommendation for a special advocate in the FISA
2 Court, what I saw prior to the Board's 215 report was a lot
3 of public mistrust and misunderstanding of the FISA Court
4 process and a mistrust of the FISA Court because it was
5 viewed as a rubber stamp.

6 Now, of course, folks that have served in the Justice
7 Department, like Mr. Wainstein and Mr. Olsen, who have been
8 in the FISA Court process, know that that is not an accurate
9 description of the FISA Court. But the public certainly
10 viewed it that way, and so I think it is important to have
11 some--for the public to have some visibility into how the
12 Court works and for the public to have more confidence about
13 how the Court works. And so I think that the public
14 advocate serves that purpose. I think the two recent
15 occasions on which the FISA Court has appointed an amicus, I
16 think they have been useful to the Court, and I think they
17 have helped to illuminate the process for the public as
18 well.

19 Senator Blumenthal. But the help to the Court has not
20 just been in appearance, that is, enhancing the perception
21 of actual scrutiny. And the value that you describe, Mr.
22 Medine, to judges who hear one side and then the other side
23 is not just an entertainment value. It is actually--it
24 elucidates questions. It permits the contrast and conflict
25 of ideas, and out of that contention, sometimes heated,

1 emerges a better conclusion for the Court.

2 Ms. Brand. I agree with that, but I do think there was
3 a real misunderstanding in the public because there was a
4 sense that the Court did not push back, that the Court just
5 simply accepted what the Government said at face value. And
6 that was not an accurate perception, so I agree, it will
7 refine the Court's thinking, it will challenge the Court's
8 thinking, and that is a very important benefit. It will
9 also then have the benefit of assuring the public that the
10 process has integrity.

11 Senator Blumenthal. Did you have a response, Ms.
12 Goitein?

13 Ms. Goitein. Well, Senator Blumenthal, I wanted first
14 to just thank you for your leadership in ensuring that that
15 very important provision was part of the USA FREEDOM Act. I
16 think it was very important.

17 I do not see the FISA Court as a rubber stamp at all,
18 but I do think that it has in the past seen its job--and I
19 have heard this from former National Security Division
20 attorneys--as getting to "yes." And that is not the role of
21 the judiciary.

22 I think part of that was that when there was not
23 another party there, the Court was not in the role of being
24 a neutral adjudicator between two sides, and, therefore, if
25 the Court said no to the Government, the Court effectively

1 became the other side. I think that was a very
2 uncomfortable role for the Court, and I think it made the
3 Court more inclined to try to move toward yes.

4 So I am hopeful that having an amicus there will
5 ultimately help the Court to take more of a stance as a
6 neutral arbiter. I think that will take time. I think it
7 will be a cultural shift. But I think so far it is a very
8 good thing that this is in place.

9 Senator Blumenthal. My time has expired. This is a
10 very important topic. I know it is an evolving question. I
11 just want to say for most of my career, I was a Government
12 lawyer, and so I wanted the Court to get to "yes." But at
13 the same time, I welcomed, actually, a strong adversarial
14 process because it made the case better. It reduced the
15 likelihood of a successful appeal. And we are dealing in a
16 different context here where appeals are unlikely, but,
17 still, the result was better. And as all of you know, a
18 judge's worst nightmare is a defendant representing himself,
19 for all the reasons that you well know. And since my time
20 has expired, I am not going to go into them, but I welcome
21 and thank you for your very, very important work in this
22 area, every one of you. Thank you very much.

23 Chairman Grassley. Senator Coons.

24 Senator Coons. Thank you, Chairman Grassley. And I
25 would like to thank Ranking Member Franken of the

1 Subcommittee and all the witnesses for your very hard work
2 in a very difficult area that really is about balancing our
3 national values, our security, and our enduring concerns
4 about privacy. This is a debate that goes back to the
5 founding of our Republic and is, as you can tell from
6 attendance at the hearing today, still vibrant today.

7 Let me try to cover some ground that has not been
8 covered thoroughly because there are an awful lot of
9 questions that have gone back and forth between this very
10 able panel and members.

11 My understanding is the Government does not obtain a
12 warrant for querying the Section 702 database for
13 information about Americans, despite an expressed
14 understanding from some members who were present when
15 Section 702 was adopted that it was not intended to allow
16 this type of warrantless search of Americans'
17 communications.

18 Can any of you proffer an estimate of how many
19 communications with U.S. persons have been collected under
20 702? I understand it is difficult, but if anyone can give
21 us an estimate, I would welcome that. And can you answer
22 the question, Do you think we should require queries to be
23 tracked in order to obtain information about how often the
24 Section 702 database is used to search for information about
25 U.S. persons? I see ready volunteers.

1 [Laughter.]

2 Mr. Medine. Senator, there is a challenge in
3 quantifying how many Americans' communications are
4 collected. Our Board recommended some metrics, and I know
5 that recently Director Clapper has indicated he will be
6 trying to come up with some estimates. I think it would be
7 useful to require by legislation that the Director of
8 National Intelligence report annually to the Congress on the
9 number of Americans' communications that are incidentally
10 collected and the methodology used to do that, because that
11 is an important part in this reauthorization process of
12 evaluating it but also on an ongoing basis how the program
13 is operating.

14 Ms. Brand. Just to add to what David said, the PCLOB's
15 report recommended that the Government publish more
16 statistics about the impact of 702 on U.S. persons. And I
17 think there is a good story here of how the PCLOB report is
18 pushing the Government to do that. So the administration
19 recently released numbers on two of those measures,
20 including on U.S. person queries by the CIA and the NSA.
21 And it is working very hard to come up with a reliable
22 estimate to satisfy the other three recommendations.

23 The PCLOB staff is in constant communication with the
24 administration about their efforts to find those numbers,
25 and they really are working hard to get to a position of

1 giving Congress and the public more and reliable
2 information.

3 Senator Blumenthal. Thank you. I appreciate that.

4 Ms. Goitein?

5 Ms. Goitein. I do think getting an estimate of the
6 number of Americans' communications that are obtained is
7 extremely important. I have heard that the intelligence
8 community is working on it, but this is a request that has
9 been pending for years. So I would urge the Committee to
10 support these efforts to move this process along so we can
11 get this information as soon as possible.

12 With respect to the queries, we do not have numbers of
13 how many times the FBI runs U.S. person queries of the data
14 because the FBI does not track those. The FBI, however, is
15 by far--we know from the Board's report--the most active and
16 frequent U.S. person querier, and so it is important to get
17 that information.

18 I heard Ms. Brand saying that, you know, the FBI would
19 have trouble figuring out who is a U.S. person in order to
20 track these queries. The NSA does it; the CIA does it.
21 They are able to track the queries. I think the FBI should
22 be able to as well.

23 And just one quick point that I was hoping to get in
24 when Senator Whitehouse was talking about this incidental
25 collection idea, there is a very important distinction

1 between the cases that have upheld the incidental collection
2 of people who are in communications with a target and what
3 we are seeing with Section 702. In those cases under Title
4 III criminal warrants, there was not only strict
5 minimization procedures, which was mentioned, but there was
6 also a warrant in the beginning to target the original
7 suspect. And the courts have emphasized the importance of
8 that warrant at the front end, because that provides some
9 vicarious protection to people in contact with the target
10 and narrows the pool of people who can be collected on.

11 Senator Coons. Thank you for that addition. Let me
12 ask just two more questions, if I might.

13 First, if you would answer this, and Mr. Wainstein as
14 well, give Section 702 was initially adopted for foreign
15 intelligence and national security purposes, do you have any
16 concerns about whether it is appropriate for Americans'
17 communications collected under the statute to be used for
18 domestic law enforcement purposes? Do you think that is a
19 distinction that can be neatly made? Or is that a boulder
20 that you think is worth respecting?

21 And then my last question to Mr. Medine, if I might,
22 what standard does DOJ apply to determine whether it is
23 obligated to provide criminal defendants with notice? And
24 how, in your view, does the DOJ ensure compliance with its
25 Brady obligation to provide Section 702-derived exculpatory

1 information? If you would answer those in sequence, I will
2 be out of time. Thank you.

3 Ms. Goitein. I think the distinction is not so much
4 between foreign and domestic in terms of the nature of the
5 case, but in terms of who the target is. So if the target
6 is foreign, then there can be warrantless collection. But
7 if the Government is trying to build a case against an
8 American, the American is the target, then if it is a
9 foreign intelligence case, they go to the FISA Court and
10 they get an individualized order; if it is a criminal case,
11 they go to a magistrate and they get a warrant. And that
12 distinction is very easy to make, whether someone is an
13 American or not.

14 Senator Coons. Sir?

15 Mr. Wainstein. Thank you for the question. I think
16 the problem here--and Ms. Brand alluded to this earlier
17 today--is that we were involved right after 9/11 with
18 bringing down the wall, and Congress, through the PATRIOT
19 Act, did exactly that. And the wall was based fundamentally
20 on a distinction between foreign intelligence work and
21 criminal work, law enforcement work. And that was a
22 distinction that created this barrier that impaired
23 information sharing that the 9/11 Commission said led in
24 part to the attacks of 9/11. The last thing we want to do
25 is re-erect that wall at this point. We have seen the

1 benefit of having seamless coordination and information
2 sharing among our law enforcement and intelligence
3 personnel. We do not want to do anything to bring us back
4 to the old days which led to 9/11.

5 Senator Coons. Thank you.

6 Mr. Medine. Our Board, unfortunately, did not look at
7 the question you raise, so I would defer to Ms. Goitein
8 about the notification to criminal defendants of the 702
9 information.

10 Ms. Goitein. I am sorry. Was the question on
11 notification or on--okay.

12 Senator Coons. Notification of criminal defendants.

13 Ms. Goitein. Yes, okay. So that appears to be being
14 honored in the breach, is what I would say. For a while it
15 was not honored at all, and then about 3 years ago, there
16 was apparently a change in policy. But there have only been
17 eight notifications in the last 3 years, and that is against
18 a backdrop of hundreds of terrorism and national security
19 prosecutions, dozens of material support prosecutions. So
20 there is definitely concern that the FBI is avoiding the
21 requirements, perhaps by a creative definition, perhaps by
22 parallel construction, which is re-creating the evidence
23 using less controversial tools or methods, perhaps both.
24 You know, it is very easy to clear this up, for the
25 Department to simply release its policies for how it

1 interprets the notification requirement. But the Government
2 has been fighting tooth and nail against FOIA requests to
3 get those policies. So that is another area where this
4 Committee could be helpful to try to pry those loose.

5 Senator Coons. Well, thank you. I notice I am out of
6 time. Thank you very much, Mr. Chairman.

7 Chairman Grassley. Senator Franken.

8 Senator Franken. Thank you, Mr. Chairman.

9 Ms. Goitein, I understand that you worked for Senator
10 Feingold when he was on this Committee, so welcome back.

11 Ms. Goitein. Yes. Thank you.

12 Senator Franken. I would like to focus for a moment on
13 the question of transparency in our surveillance programs.
14 Last year, we passed the USA FREEDOM Act, a bicameral,
15 bipartisan bill, which brought much needed reforms to the
16 Federal Government surveillance programs, including an end
17 to the bulk data collection program that the intelligence
18 community said was not necessary and that the public said it
19 did not support.

20 I was a proud cosponsor of that bill, and I am
21 particularly proud to have developed the bill's transparency
22 provisions with my friend Senator Dean Heller of Nevada.
23 Senator Heller and I recognized that when the public lacks
24 even a rough sense of the scope of the Government's
25 surveillance program, they have no way of knowing if the

1 Government is striking the right balance, whether we are
2 safeguarding our national security without trampling on our
3 citizens' fundamental privacy rights. But the public cannot
4 know if we succeed in striking that balance if they do not
5 even have the most basic information about our major
6 surveillance programs, and that is why my focus has been on
7 transparency, and that is why Senator Heller and I crafted
8 the provisions in USA FREEDOM that now require the
9 Government to issue detailed annual reports for the
10 surveillance authorities at issue.

11 Importantly, the Government now has to provide the
12 public with estimates of how many people have had their
13 information collected. And for certain authorities, like
14 those permitting the targeted collection of call data
15 records or the communications of foreigners abroad, the
16 Government now also has to say how many times it has run
17 searches for Americans' data.

18 When the American people have access to that kind of
19 information, they can better judge the Government's
20 surveillance programs for themselves, and that is not just
21 my view. It is an opinion that is shared by Bob Litt,
22 General Counsel for the Office of the Director of National
23 Intelligence. While addressing Brookings last year, Mr.
24 Litt said, "The intelligence community recognizes that with
25 secrecy inevitably come both suspicion and the possibility

1 for abuse. I and many others firmly believe that there
2 would have been less public outcry from the Snowden leaks if
3 we had been more transparent about our activities
4 beforehand."

5 It seems to me that the same need for transparency
6 applies with equal force when we are talking about the
7 number of Americans whose phone calls or remails have been
8 collected, perhaps incidentally, under FISA Section 702.
9 Members of the Senate Intelligence Committee have asked for
10 the number of Americans affected. Civil society and civil
11 liberties groups have asked for the number, and just last
12 month, 14 members of the House Judiciary Committee asked for
13 just an estimate of the number of Americans affected, but
14 thus far, no one has received a satisfying answer.

15 Ms. Goitein, is it possible for the Government to
16 provide an exact count of how many United States persons
17 have been swept up in Section 702 surveillance? And if not
18 the exact count, what about an estimate?

19 Ms. Goitein. I think it would be very difficult to
20 provide an exact count with any accuracy at all. And I do
21 not think anyone has asked for that. Senator Wyden
22 initially asked for an estimate. I think I heard him use
23 the word "ballpark" at one point. That should be possible.
24 And with a couple of the programs, it should be fairly
25 straightforward. With PRISM it is a little trickier, but

1 that is why the civil liberties community has offered to
2 work with the intelligence community to try to find a
3 privacy-protective way of generating the estimate. So it
4 should be possible, and I think it is vital because I hear
5 public statements by officials over and over that this
6 program is targeted at foreigners and that the collection of
7 Americans' communications is incidental. These are terms of
8 art with very specific legal meanings, but most Americans
9 are not lawyers; and when they hear this, they will
10 reasonably assume that Americans' communications--that not
11 many Americans' communications are collected.

12 So I think having this estimate is important to pierce
13 through the legalese and give Americans a truer sense of
14 what the program entails, which they need in order to make
15 their own decision and participate in the democratic
16 process.

17 Senator Franken. Because Ms. Brand brought this up in
18 terms of people's confidence in this whole thing, to what
19 extent is that the issue, and to what extent is the issue
20 actually, when we Senator Blumenthal was speaking, that the
21 operational and transparency sort of be hand in glove so
22 that the operation of this is more consistent with the
23 Constitution?

24 Mr. Medine. I think it is both of those. I think that
25 for the American public to have confidence that this program

1 is abiding by the Constitution, especially when it turns its
2 focus to Americans' communications, and knowing how many
3 Americans' communications are being collected I think also
4 would illuminate the question of querying that information,
5 because I think it is a large amount of information over 5
6 years that is collected.

7 I would also add that our report on 702 I think has
8 also been helpful for Europeans as well. I was involved
9 recently in the privacy shield negotiations where the
10 Europeans had a misunderstanding of 702 and did not
11 appreciate, as our report pointed out, it is a targeted
12 program. It is not a bulk collection program. It is
13 targeted. There are a lot of targets, but there are a lot
14 of people out there that have valuable information. And I
15 think that was helpful, to ultimately resolve the
16 negotiations with the European Union on the data flow, to
17 understand this program does have a legal structure, it does
18 have oversight, and there is a targeting process.

19 Senator Franken. Well, my time is certainly up, and I
20 know Ms. Brand looked like she might want to answer that,
21 but I am way over, so, Mr. Chairman--

22 Ms. Brand. I more or less agreed with everything they
23 said.

24 Senator Franken. Okay. Well, there, that was
25 dispensed with very quickly. Okay. Thank you, Mr.

1 Chairman.

2 Chairman Grassley. I have one question, and then
3 Senator Feinstein has some questions she wants to ask. And
4 when I am done with my one question, I am going to go, and
5 Senator Feinstein or Senator Franken is going to finish the
6 meeting. So I want to thank all of you for participating,
7 and I am sure all of you are very willing to be resource
8 persons for us over the next few months as we get around to
9 working on reauthorization. But I hope you will not do like
10 a lot of people and wait for us to call you. If you have
11 got something we need to know, that you will talk to me or
12 other members of the Committee or particularly my staff, I
13 would invite that. But I want to thank you all for
14 participating in this hearing.

15 Ms. Brand, I have always believed that transparency in
16 Government leads to increased accountability. I noticed
17 that one of the Privacy and Civil Liberties Oversight
18 Board's recommendations was to provide additional
19 transparency surrounding the frequency of incidental
20 collection of U.S. persons' communications. I also
21 understand that in February 2016 the Board described this
22 recommendation as "being implemented."

23 The question is: Can you walk through the specifics of
24 what the Board recommended and provide us with some more
25 detail regarding the status of the implementation in the

1 executive branch?

2 Ms. Brand. Thank you, Senator Grassley. Yes, this was
3 one of the important recommendations that the PCLOB made in
4 terms of amending the way the program is operated. I agree
5 with what some of my fellow witnesses just said about the
6 importance of transparency in the program because it is hard
7 to judge the impact on U.S. persons of this program without
8 knowing the extent to which their communications are
9 collected. So the Government, we have had an ongoing
10 dialogue with the administration about how to get more
11 information in the public about this.

12 It is very difficult, as Ms. Goitein said, it is very
13 difficult if not impossible, to come up with an exact number
14 because when a foreign target is communicating with other
15 people, the Government does not automatically know the
16 nationality of the people with whom the target communicates.
17 And it would be extremely resource intensive to investigate
18 that and potentially more privacy intrusive than not
19 investigating it.

20 But we did think, recognizing all of those challenges,
21 we did think that there were some aspects of the program
22 that could be measured, and so we recommended five. They
23 were the number of telephone communications in which one
24 caller is located in the U.S.; the number of Internet
25 communications collected upstream with one end in the U.S.;

1 the number of communications concerning U.S. persons that
2 the NSA positively identifies as being a U.S. person
3 communication; the number of queries performed that use U.S.
4 person identifiers; and the number of instances in which the
5 NSA disseminates a report with U.S. person information in
6 it.

7 Those last two measures are ones that the Government
8 has now published some information on, so just on April 30,
9 the Saturday before last, the DNI issued its transparency
10 report, which it was required to do under the USA FREEDOM
11 Act; and whereas previously some of that information was
12 provided only to Congress, now it is public.

13 We are in an ongoing dialogue with the administration
14 about how it can release information responsive to our other
15 three recommendations, and they are working very hard to do
16 that. We were just in contact with the NSA last week about
17 that, and the staff is coming to talk to our staff next week
18 about it. So we are going to continue to press on that, and
19 we expect them to make more progress on that.

20 Chairman Grassley. Okay. Thank you.

21 Senator Feinstein?

22 Senator Feinstein. Thanks very much, Mr. Chairman.

23 Because of some of the discussion, I just wanted to
24 bring to everybody's attention two documents. The first is
25 a joint unclassified statement of Bob Litt, the General

1 Counsel for the Office of the Director of National
2 Intelligence; Stuart Evans, Deputy Assistant AG for
3 Intelligence; and Mike Steinbach, the Assistant Director of
4 the Counterterrorism Division of the FBI. On page 3, they
5 discuss targeting procedures, and I would just like to read
6 a short part:

7 "To ensure compliance with these provisions"--and they
8 have set up a number of steps in the preceding paragraph--
9 "Section 702 requires targeting procedures, minimization
10 procedures, and acquisition guidelines. These are designed
11 to ensure that the Government targets non-U.S. persons
12 outside the United States, and also that it does not
13 intentionally acquire domestic communications. Moreover,
14 the targeting procedures ensure that targeting of foreign
15 persons is not indiscriminate, but instead targeted at non-
16 U.S. persons outside the United States who are assessed to
17 posses, expected to receive, or who are likely to
18 communicate foreign intelligence information."

19 Now it goes on to say, "Because Congress understood
20 when it passed the FAA that a targeted non-U.S. person may
21 communicate with or discuss information concerning a U.S.
22 person, Congress also required that all collection be
23 governed by minimization procedures that restrict how the
24 intelligence community treats any person." In the best of
25 my knowledge, the FISA Court has to review these

1 minimization procedures annually and approve them, along
2 with this recertification of the program. This is page 3 of
3 that. I think it is interesting for everyone to read.

4 The second thing I wanted to cite is the Director of
5 National Intelligence's April 30th letter within an addenda
6 that is a response to the PCLOB recommendations, and I want
7 to read that because there are some interesting first time I
8 have seen these figures, and this is--I am reading from page
9 6 of that. "NSA's minimization procedures expressly
10 prohibit dissemination of information about U.S. persons in
11 any NSA report unless that information is necessary to
12 understand foreign intelligence information or assess its
13 importance, contains evidence of a crime"--that is an
14 exception--"or indicates a threat of death or serious bodily
15 injury. Even if one of these conditions applies, NSA will
16 often mask the information and will under any circumstances
17 include no more than the minimum amount of U.S. person
18 information necessary to understand the foreign intelligence
19 or to describe the crime or threat. In certain instances,
20 however, NSA makes a determination prior to releasing its
21 original report that the U.S. person's identity is
22 appropriate to disseminate in the first instance using the
23 same standards mentioned above."

24 And here are the numbers: In 2015, NSA disseminated
25 4,290 FAA Section 702 intelligence reports that included

1 U.S. person information. Of those 4,290 reports, the U.S.
2 person information was masked in 3,180 reports of those and
3 unmasked in 1,122 reports.

4 I know this went to the PCLOB, and it seems to me that
5 that is very responsive to the concern--is it Ms. "Go-lean"
6 or "Go-line"?

7 Ms. Goitein. It is "Goitein."

8 Senator Feinstein. Pardon me?

9 Ms. Goitein. "Goitein."

10 Senator Feinstein. "Goitein."

11 Ms. Goitein. Thank you.

12 Senator Feinstein. Excuse me. I am glad I asked.

13 Ms. Goitein. It is a tricky one.

14 Senator Feinstein. Ms. Goitein's comments. Would
15 anyone like to comment on that? I am looking at you, Mr.
16 Medine. Since the PCLOB receives this, I would appreciate a
17 PCLOB response.

18 Mr. Medine. Sure. Well, the Board has not addressed
19 it as a Board, but I think it is exactly the kind of
20 information the Board was seeking in terms of greater
21 transparency on how many U.S. person identities were
22 disseminated. And certainly we are aware that a lot of
23 times that information is masked and then ultimately
24 unmasked down the road.

25 One thing, if I could comment on the first document you

1 said about the focus of this program is on non-Americans,
2 there was a lot of misconception after the leaks in 2013
3 about what this program was about, and some people even
4 thought you only had to be 51 percent sure it was a non-
5 American in order to conduct surveillance, which would have
6 meant a lot of Americans' communications were intentionally
7 captured. And one of the things that--the Board dug deep on
8 that question and actually concluded that it is about a 99-
9 plus-percent chance it is a non-American because it is a
10 very rigorous process to determine who is or is not an
11 American.

12 The other thing we looked at is whether there is
13 suspected foreign intelligence value for the collection, and
14 there we did feel that there was a need for improvement
15 because the Government had not been documenting sufficiently
16 why it was looking at this information, and we thought it
17 was important for them to put it down on paper. But that is
18 the recommendation that they accepted and have now
19 implemented to make sure there is a greater rationale for
20 these collections.

21 Senator Feinstein. Thank you.

22 Mr. Wainstein, I just would like you to know I was on
23 this Committee when the wall was discussed in whatever year
24 it was, and there was tremendous concern about the wall
25 really preventing the kind of communication that was

1 necessary. I made the amendment on the definition at that
2 time that resulted in the reduction of the wall, and to this
3 day I think it is a very important change that was made that
4 enables information to be constituted.

5 I think in our concern we often--and because I guess I
6 see the intelligence, you get a sense that there is plotting
7 and there is conspiracy going on, and the FBI is
8 investigating ongoing cases. So we have even had--I think
9 it is an unclassified number, Mr. Olsen--about 1,000
10 investigations going on today in this country. So we should
11 not let down our guard because to do so is really to invite
12 disaster. And I think that--I actually believe, from the
13 time we began looking at this and with the PCLOB's help and
14 the information you have provided and the response to it,
15 that there is renewed transparency going on and there is
16 discussion that is helpful. But I think that the 702
17 program of the programs is really important, and it would be
18 most unfortunate and it would expose this country if that
19 program were made ineffective. So the key really is to do
20 what we can, and I think the FAA has done that, to provide--
21 and the masking and the unmasking and now everybody has the
22 numbers with respect to that for the year 2015.

23 So I just wanted to make those comments, and if anybody
24 has a comment--Ms. Goitein?

25 Ms. Goitein. Yes, I am twitching over here.

1 Senator Feinstein. Go ahead.

2 Ms. Goitein. Because I just wanted to respond to one
3 thing you said. Opposition to back-door searches is not a
4 call to rebuild the wall.

5 Senator Feinstein. Whoa, whoa. What do you call it?
6 What is a back-door search?

7 Ms. Goitein. A back-door search is when the FBI or any
8 other agencies targets a U.S. person for a search of data
9 that was collected under Section 702 which is supposed to be
10 targeted against foreigners overseas.

11 Senator Feinstein. Regardless of the minimization that
12 was properly carried out.

13 Ms. Goitein. Well, the data is searched in its
14 unminimized form, so the FBI gets raw data, the NSA and CIA
15 get raw data, and they search that raw data using U.S.
16 person identifiers. That is what I am referring to as
17 "back-door searches." I am happy to call it "U.S. person
18 queries," and trying to address U.S. person queries is not
19 calling to rebuild the wall. Any agency that comes across
20 threat information should share that information. Agencies
21 should work together to address the threat. What the Fourth
22 Amendment cannot tolerate is the Government collecting
23 information, communications, without a warrant, with the
24 intent of mining it for use in criminal cases against
25 Americans.

1 Senator Feinstein. That is where you and I differ. I
2 think that all of the data is collected lawfully. I do not
3 believe it is collected unlawfully.

4 Ms. Goitein. I agree.

5 Senator Feinstein. If you have a case where the data
6 is collected unlawfully, I would sure like to see it.

7 Ms. Goitein. But, unfortunately, it is not that simple
8 because collection and then how the data is treated are both
9 parts of the same scheme that is evaluated for its
10 constitutionality. And what makes the collection at the
11 front end lawful--and Judge Bates has said this, on the FISA
12 Court. What makes it lawful to collect without a warrant is
13 in part restrictions on how that data can be used on the
14 back end.

15 Senator Feinstein. Okay. Let us have somebody respond
16 to that.

17 Ms. Brand. May I respond, Senator Feinstein?

18 Senator Feinstein. Yes, go ahead.

19 Ms. Brand. I think you are on to something very
20 important when you mention minimization because there are
21 extensive rules and protections that surround the use of
22 U.S. person queries. So at the CIA and NSA, for example,
23 the PCLOB's report went into extensive detail about how and
24 under what circumstances those agencies may conduct a U.S.
25 person query, what Ms. Goitein refers to as a "back-door

1 search." They have to be designed to return foreign
2 intelligence information. There is documentation of the
3 justification. The Board recommended some improvements for
4 that which the agencies are implementing. There is
5 extensive oversight after the fact on U.S. person queries by
6 the Justice Department.

7 And then with respect to the FBI, the FBI does not
8 track U.S. person queries separately from non-U.S. person
9 queries, but queries are documented, and the person who
10 conducted them is documented.

11 At the FBI, where the protections come in is in any use
12 of information. So in the extremely unlikely, perhaps
13 theoretical event that 702 information will be responsive to
14 a query in a regular criminal investigation, that
15 information could not be viewed by the analyst who conducts
16 the query unless they are trained in using FISA information.
17 The Attorney General has to approve any use of that
18 information in a criminal proceeding, which includes
19 something like a wiretap application, as I understand it.
20 And if someone's communications collected under 702 are used
21 against him in a criminal proceeding, he has to be notified.
22 And we know that that does happen because there was just a
23 reported case out of the U.S. District Court in Colorado
24 where a defendant did a motion to suppress information
25 collected under 702 after the Government notified him that

1 it had been collected. So that policy change was late in
2 coming, but it is now happening. So I think it is very
3 important to keep all those limitations in mind.

4 Senator Feinstein. Thank you. I appreciate that.

5 Mr. Olsen?

6 Mr. Olsen. If I could just very briefly make maybe a
7 broader point, which is the targeting procedures, Senator,
8 that you identified in the first document you read, the
9 transparency figures in the DNI's report, I think really
10 highlight, along with Ms. Brand's and most of the discussion
11 today, the success that the FISA Amendments Act and Section
12 702 represents, that as we sit here today this is a law that
13 reflected a careful balance in 2008 and that has since been
14 enhanced to tweak that balance, I think in very careful
15 ways, a report that is really unprecedented in terms of its
16 thoroughness and detailed nature, the PCLOB report leading
17 to those changes.

18 So as we sit here today, we have a very carefully
19 calibrated law that has been a major success from an
20 intelligence standpoint, and I do reject the notion of back-
21 door searches. I think it is a misnomer to call searches of
22 lawfully collected data that every judge who has looked at
23 it--including the FISA Court judge and district court judges
24 have upheld when they have had the chance to review those
25 searches, that is not a back-door search. That is the way

1 the law was intended to be used under the careful
2 limitations that the minimization procedures impose. So I
3 think this is a very good news story at the end of the day.

4 Senator Feinstein. Thank you very much. I appreciate
5 that, because we have looked at this, and there are a number
6 of opinions from some of your colleagues on the subject that
7 have been studied. And I really think it is lawful and well
8 balanced, and, you know, I hate to say it but very
9 necessary. In my view, it is only intelligence lawfully
10 collected that is able to prevent another attack in this
11 country. And I hope there will be more declassified
12 examples before the year turns and we are in 2017 and faced
13 with the reauthorization. So thank you.

14 Senator Franken, would you take over and ask your
15 questions and adjourn the meeting, please?

16 Senator Franken. [Presiding.] I would be delighted
17 to.

18 Senator Feinstein. Thank you.

19 Senator Franken. I want to thank the Senator from
20 California whose work on intelligence has been so important
21 and for her thoughtful questions.

22 I am going to adjourn this in a second, but I just want
23 to--you know, what is interesting, I thought, about this
24 line of questioning at the end here, which goes sort of to
25 the core of all of this, which is that we have had some very

1 important information from 702 that has thwarted terrorist
2 attacks. And so this is absolutely crucial. And I believe
3 that, by and large, with some exceptions, that our
4 intelligence community has acted in good faith.

5 The question here really is going back to the Framers
6 and going back to their fear about what happens when a
7 Government is not acting in as good faith as I think that
8 our intelligence community by and large has. And so this
9 use of information that we get through 702 can be misused.

10 Ms. Goitein mentioned parallel construction, which is--
11 and, again, this is--the Framers wrote the Constitution
12 because they did not like the British at the time. I think
13 everyone knows that, right? I do not have to go through
14 that history? And so they were worried about maybe some
15 people running the executive branch of the Government that
16 were not as trustworthy as others. And so that is the
17 reason that we look at how that 702 information which is
18 collected about people who are not the targets and who are
19 Americans, how that information is--what the rules are so
20 that is not misused. That is my understanding of this.

21 Ms. Goitein, I saw you reach for the button.

22 Ms. Goitein. I have got to tame this finger a little
23 bit because it keeps reaching for the button. But I do
24 think there are situations in which having oversight and
25 rules and policies about procedures for how searches are

1 done, all those things, there are cases where that is
2 absolutely vital. When you are talking about a warrant and
3 the basic requirement of getting a warrant to access
4 Americans' communications, you cannot substitute procedures
5 for a warrant. And to quote Justice Roberts in the Riley
6 case, which required a warrant to search cell phones, "the
7 Founders did not fight a revolution to gain the right to
8 government agency protocols." And so I would like to leave
9 everyone with that thought.

10 Senator Franken. Well, can we end on that? Okay. I
11 am just a little late. I volunteered to do this, and I am
12 going to now. I am going to adjourn--we are going to keep
13 the record open for another 7 days. Is that right? And we
14 are now adjourned.

15 [Whereupon, at 11:39 a.m., the Committee was
16 adjourned.]

17

18

19

20

21

22

23

24

25

C O N T E N T S

STATEMENT OF:	PAGE
The Honorable Kenneth L. Wainstein, Partner, Cadwalader, Wickersham & Taft LLP, Washington, D.C.	9
The Honorable Matthew G. Olsen, President, Consulting, IronNet Cybersecurity, Fulton, Maryland, and Former Director, National Counterterrorism Center	18
Elizabeth Goitein, Co-Director, Liberty & National Security Program, Brennan Center for Justice at New York University School of Law, Washington, D.C.	24
The Honorable David Medine, Chairman, Privacy and Civil Liberties Oversight Board, Washington, D.C.	29
The Honorable Rachel L. Brand, Board Member, Privacy and Civil Liberties Oversight Board, Washington, D.C.	34