

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs
Operated Pursuant to Section 215 of the USA
PATRIOT Act and Section 702 of the Foreign
Intelligence Surveillance Act

July 9, 2013

The workshop was held at the Renaissance Mayflower
Hotel, 1127 Connecticut Avenue NW, Washington,
D.C. 20036 commencing at 9:30 a.m.

Reported by: Lynne Livingston

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

BOARD MEMBERS

- David Medine, Chairman
- Rachel Brand
- Patricia Wald
- James Dempsey
- Elizabeth Collins Cook

PANEL I

Legal/Constitutional Perspective

- Steven Bradbury, formerly DOJ Office of Legal Counsel
- Jameel Jaffer, ACLU
- Kate Martin, Center for National Security Studies
- Hon. James Robertson, Ret., formerly District Court and Foreign Intelligence Surveillance Court
- Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

PANEL II

Role of Technology

Steven Bellovin, Columbia University Computer
Science Department

Marc Rotenberg, Electronic Privacy Information
Center

Ashkan Soltani, Independent Researcher and
Consultant

Daniel Weitzner, MIT Computer Science and
Artificial Intelligence Lab

PANEL III

Policy Perspective

James Baker, Formerly DOJ Office of Intelligence
and Policy Review

Michael Davidson, Formerly Senate Legal Counsel

Sharon Bradford Franklin, The Constitution Project

Elizabeth Goitein, Brennan Center for Justice

Greg Nojeim, Center for Democracy and Technology

Nathan Sales, George Mason School of Law

1 PROCEEDINGS

2 MR. MEDINE: Good morning, and welcome to
3 the third public meeting held by the Privacy and
4 Civil Liberties Oversight Board.

5 I want to first introduce my fellow board
6 members Rachel Brand, Pat Wald, Beth Cook and Jim
7 Dempsey.

8 PCLOB, as we are often known, is an
9 independent bipartisan agency within the Executive
10 Branch. We were recommended by the 9/11
11 Commission and created by Congress.

12 The board's primary missions are to
13 review and analyze actions by the Executive Branch
14 to protect the nation from terrorism and ensuring
15 the need for such actions is balanced with the
16 need to protect privacy and civil liberties and to
17 ensure that liberty concerns are appropriately
18 considered in the development and implementation
19 of laws, regulation and policies related to
20 protect the nation from terrorism.

21 Essentially PCLOB is both an advisory and
22 it has an advisory and oversight role with respect

1 to our country's counterterrorism efforts.

2 I wanted to thank our many panelists
3 throughout the day for agreeing to participate in
4 this workshop and share their views about these
5 important programs with the board.

6 I also wanted to thank Sue Reingold, the
7 board's chief administrative officer and Diane
8 Janosek, our chief legal officer for their
9 tireless efforts in making this event possible.

10 Our focus today will be two federal
11 counterterrorism programs, the Section 215 program
12 under the USA PATRIOT Act and the Section 702
13 program under the FISA Amendments Act.

14 The purpose of the workshop is to foster
15 a public discussion of legal, constitutional and
16 policy issues relating to these programs. PCLOB
17 has agreed to provide the President and Congress a
18 public report on these two programs, along with
19 any recommendations it may have.

20 A few ground rules for today's workshop,
21 we expect that the discussion will be based on
22 unclassified or declassified information.

1 However, some of the discussion will inevitably
2 touch on leaked classified documents or media
3 reports of classified information.

4 In order to promote a robust discussion
5 speakers may choose to reference these classified
6 documents or information but they should keep in
7 mind that in some cases these documents still
8 remain classified, therefore while discussing them
9 speakers in a position to do so are urged to avoid
10 confirming the validity of the documents or
11 information.

12 There will be three panels today. The
13 first will focus on legal issues, the second on
14 technical aspects, and the third on policy.

15 After the first panel we will be taking a
16 lunch break. Two board members will moderate each
17 panel and will pose questions and additional board
18 members may have follow-up questions.

19 Panelists are urged to keep their
20 responses brief to permit the greatest possible
21 exchange of views.

22 At the end of the day there will be some

1 time for members of the audience to make
2 statements about these two programs.

3 This workshop is being recorded and a
4 transcript will be posted on what we hope will be
5 PCLOB's website active this evening, and as well
6 as on regulations.gov.

7 Those who wish to submit written comments
8 about these issues are welcome to do so, and
9 comments may be submitted at regulations.gov or by
10 mail until August 1st.

11 I want to start by level setting the
12 discussion. My description that follows of the
13 two programs is based on information that's been
14 publicly disclosed by the federal government. It
15 should not be interpreted as saying new about
16 these programs. It's merely a summary of the
17 unclassified remarks by federal government
18 officials.

19 PCLOB has not come to any conclusions
20 regarding the accuracy or completeness of this
21 information or the two programs' legal
22 justification.

1 There are a couple of things in common
2 between the two programs. Both are designed,
3 among other things, to identify terrorists and if
4 possible prevent terrorist plots. Both require
5 orders from the Foreign Intelligence Surveillance
6 Court, but the criteria for such orders may differ
7 for each program.

8 In both it's possible that even with the
9 best intentions the government may end up
10 collecting or accessing information beyond what
11 was authorized leading to questions about how such
12 information should be handled.

13 And of course both programs have been the
14 subject of leaks by Mr. Snowden.

15 In terms of the specific programs, the
16 first is based on Section 215 of the USA PATRIOT
17 Act, which was reauthorized by Congress in 2011.
18 Sometimes this is referred to as the 215 Business
19 Records Collection Program.

20 One of the things the government collects
21 under 215 is telephone metadata pursuant to court
22 order authorized by the Foreign Intelligence

1 Surveillance Act under a provision that allows the
2 government to obtain business records for
3 intelligence and counterterrorism purposes.

4 The government's argued that the
5 collection of this information must be broad in
6 scope because more narrow collection would limit
7 the government's ability to screen for a identify
8 terrorism-related communications.

9 The metadata that's been collected
10 describes telephone calls such as the telephone
11 number making the call, the telephone number
12 dialed, the date and time the call was made and
13 the length of the call.

14 The government takes the position that
15 these are considered business records of the
16 telephone companies.

17 This program does not collect the
18 contents of any communications, nor the identity
19 of the persons involved with the communication.
20 Intelligence community representatives have stated
21 that cell phone location information is not
22 collected, such as GPS or cell tower information.

1 In approving the program, the FISA Court
2 has issued two orders. One order, which is the
3 type of order that was leaked, is an order to the
4 telephone providers directing them to turn
5 information over to the government.

6 It's been asserted that the other order
7 spells out the limitations what the government can
8 do with the information after it's been collected,
9 who has access to it and for what purpose it can
10 be accessed and how long it can be retained.

11 Court orders must be issued every 90 days
12 for the program to continue.

13 Concerns have been raised that once large
14 quantities of metadata about telephone calls have
15 been collected it could be subjected to
16 sophisticated analysis to drive information that
17 could not otherwise be determined.

18 This type of analysis is not permitted
19 under this program. Instead the metadata can only
20 be queried when there is a reasonable suspicion
21 that a particular telephone number is associated
22 with specified foreign terrorist organizations.

1 Even then the only purpose for which the data can
2 be queried is to identify contacts.

3 In other words, the input and output of
4 this program is limited to metadata. In practice
5 only a small portion of the data that's collected
6 is actually ever reviewed because the vast
7 majority of data is never going to be responsive
8 to terrorism-related queries.

9 For example, in 2012 fewer than 300
10 identifiers were approved for searching this data.

11 The rationale for this program is that
12 because all the metadata is collected because if
13 you want to find the needle in the haystack you
14 need to have the haystack.

15 Follow-up investigations that result from
16 the analysis of metadata such as electronic
17 surveillance of particular U.S. telephone numbers
18 requires a court order based on probable cause.

19 I'm turning now to the second program
20 under Section 702. It involves the government's
21 collection of foreign intelligence information
22 from electronic communication service providers

1 under court supervision pursuant to Section 702 of
2 the Foreign Intelligence Surveillance Act. It's
3 been referred to as PRISM, which is a misnomer.
4 PRISM does not refer to a data collection program,
5 it's instead the name of a government database.

6 Under Section 702, which was reauthorized
7 by Congress in December 2012, information is
8 obtained with FISA Court approval with the
9 knowledge of the provider, and based on a written
10 directive from the Attorney General and the
11 Director of National Intelligence to acquire
12 foreign intelligence information.

13 The law permits the government to target
14 a non-U.S. person, that is somebody who is not a
15 citizen or a permanent resident alien, located
16 outside the United States for foreign intelligence
17 purposes without obtaining a specific warrant for
18 each target.

19 The law prohibits targeting somebody
20 outside of the United States in order to obtain
21 information about somebody in the United States.
22 In other words, Section 702 prohibits reverse

1 targeting of U.S. persons.

2 The law also does not permit
3 intentionally targeting any U.S. citizen or other
4 U.S. person, or intentionally target any person
5 known to be in the United States.

6 In order to obtain FISA Court approval
7 there must be first an identification of the
8 foreign intelligence purposes for the collection,
9 such as for prevention of terrorism, hostile cyber
10 activities or nuclear proliferation, and
11 procedures for ensuring individuals targeted for
12 collection are reasonably believed to be U.S.
13 persons located outside of the United States.

14 There must be also approval of the
15 government's procedures for what it will do with
16 the information about a U.S. person or someone in
17 the United States if it gets that information
18 through this collection.

19 Court approved minimization procedures,
20 which have also been the subject of a leak,
21 determine what can be kept and what can be
22 disseminated to other government agencies.

1 Dissemination of information about U.S.
2 persons is expressly prohibited unless the
3 information is necessary to understand foreign
4 intelligence, assess its importance, is evidence
5 of a crime, or indicates an imminent threat of
6 death or serious bodily harm.

7 The intelligence community asserts the
8 communications collected under this program have
9 provided insight into terrorist networks and
10 plans, including information on terrorist
11 organizations strategic planning efforts,
12 contributing to impeding the proliferation of
13 weapons of mass destruction and related
14 technologies and successful efforts to mitigate
15 cyber threats.

16 We will turn now to our first panel which
17 will focus on legal and constitutional
18 perspectives on the two programs. Board members
19 Rachel Brand and Pat Wald will moderate the panel.

20 MS. BRAND: All right, thank you, David.
21 Good morning, everyone, thank you for coming.

22 I'm Rachel Brand, one of the members of

1 the board. My colleague Patricia Wald and I are
2 moderating the first panel which is focusing on
3 the legality of the two types of surveillance that
4 David described. The policy implications of those
5 types of surveillance will be discussed at a later
6 panel.

7 We have a panel of five distinguished
8 experts to give us their views on these issues.
9 I'll introduce them in a moment. Each of them
10 will have up to five minutes to give opening
11 remarks.

12 Our general counsel Diane Janosek is in
13 the front row with cards, red, green, yellow, so
14 for your benefit on the panel.

15 Then each panelist will have up to two
16 minutes to give responsive remarks, reflections on
17 what the other panelists have said. Pat and I
18 will then ask a series of questions to the panel,
19 and for the last 15 minutes our colleagues on the
20 board will have a chance to ask questions as well.

21 So our panelists are, in alphabetical
22 order, Steve Bradbury, who is a partner at a law

1 firm here in D.C. and was the head of the Office
2 of Legal Counsel at the Justice Department from
3 2005 to 2009.

4 Jameel Jaffer is the Deputy Legal
5 Director with the ACLU and is currently involved
6 in a constitutional challenge in court to one of
7 the programs we're talking about today.

8 Kate Martin is the Director of the Center
9 for National Security Studies.

10 James Robertson is a former U.S. District
11 Judge and also served on the Foreign Intelligence
12 Surveillance Court.

13 And Ken Wainstein at the end is a partner
14 at Cadwalader, Wickersham and Taft and served
15 previously as the Homeland Security Advisor as the
16 Head of the National Security Division at the
17 Justice Department and as a U.S. Attorney here in
18 Washington.

19 So Steve, we'll start with you.

20 MR. BRADBURY: Thanks, Rachel. I
21 appreciate the opportunity to participate today.

22 I'm going to focus my opening remarks on

1 the telephone metadata program. As the government
2 has stated, and David summarized, this program is
3 supported by a Section 215 business records order,
4 which must be reviewed and reapproved by the
5 federal judges who sit on the FISA Court every 90
6 days.

7 And I understand that fourteen different
8 federal judges have approved this order since
9 2006.

10 The metadata acquired consists of the
11 transactional information that phone companies
12 retain for billing purposes. It includes only
13 data fields showing which phone numbers called
14 which numbers and the time and duration of the
15 calls.

16 This order does not give the government
17 access to any information about the content of
18 calls or any other subscriber information, and it
19 doesn't enable the government to listen to
20 anyone's phone calls.

21 Access to the data is limited under the
22 terms of the court order. Contrary to some news

1 reports, there's no data mining or random sifting
2 of the data permitted.

3 The database may only be accessed through
4 queries of individual phone numbers and only when
5 the government has reasonable suspicion that the
6 number is associated with a foreign terrorist
7 organization.

8 If it appears to be a U.S. number the
9 suspicion cannot be based solely on activities
10 protected by the First Amendment. Any query of
11 the database requires approval from a small circle
12 of designated NSA officers.

13 A query will simply return a list of any
14 numbers the suspicious number has called and any
15 numbers that have called it, and when those calls
16 occurred. That's all.

17 The database includes metadata going back
18 five years to enable an analysis of historical
19 connections.

20 Of course any connections that are found
21 to numbers inside the United States will be of
22 most interest because the analysis may suggest the

1 presence of a terrorist cell in the U.S.

2 Based in part on that information the FBI
3 may seek a separate FISA order for surveillance of
4 a U.S. number but that surveillance would have to
5 be supported by individualized probable cause.

6 The NSA's Deputy Director, as David
7 mentioned, has testified that in all of 2012 there
8 were fewer than 300 queries of the database, and
9 only a tiny fraction of the data has ever been
10 reviewed by analysts.

11 The database is kept segregated and is
12 not accessed for any other purpose. And NSA
13 requires the government -- and FISA, excuse me,
14 requires the government to follow procedures
15 overseen by the court to minimize any unnecessary
16 dissemination of U.S. numbers generated from the
17 queries.

18 In addition to court approval, the 215
19 order is also subject to oversight by the
20 Executive Branch and Congress. FISA mandates
21 periodic audits by inspectors general and
22 reporting to the intelligence and judiciary

1 committees of Congress.

2 When Section 215 was reauthorized in 2011
3 I understand the leaders of Congress and members
4 of these committees were briefed on this program,
5 and all members of Congress were offered the
6 opportunity for a similar briefing.

7 Now let me address the statutory and
8 constitutional standards. Section 215 permits the
9 acquisition of business records that are, quote,
10 relevant to an authorized investigation.

11 Here the telephone metadata is relevant
12 to counterterrorism investigations because the use
13 of the database is essential to conduct the link
14 analysis of terrorist phone numbers that I've
15 described. And this type of analysis is a
16 critical building block in these investigations.

17 In order to connect the dots we need the
18 broadest set of telephone metadata we can
19 assemble, and that's what this program enables.

20 The legal standard of relevance in
21 Section 215 is the same standard used in other
22 contexts. It does not require a separate showing

1 that every individual record in the database is
2 relevant to the investigation.

3 The standard is satisfied if the use of
4 the database as a whole is relevant. It's
5 important to remember that the Fourth Amendment
6 does not require a search warrant or other
7 individualized court order in this context.

8 A government request for business records
9 is not a search within the meaning of the Fourth
10 Amendment. Government agencies have authority
11 under many federal statutes to issue
12 administrative subpoenas without court approval
13 for documents that are relevant to an authorized
14 inquiry.

15 In addition, grand juries have broad
16 authority to subpoena records potentially relevant
17 to whether a crime has occurred, and grand jury
18 subpoenas also don't require court approval.

19 In addition, the Fourth Amendment does
20 not require a warrant when the government seeks
21 purely transactional information or metadata, as
22 distinct from the content of communications.

1 This information is voluntarily made
2 available to the phone company to complete the
3 call and for billing purposes. And courts have
4 therefore said there's no reasonable expectation
5 that it's private.

6 I would stress however that Section 215
7 is more restrictive than the constitution demands
8 because it requires the approval of a federal
9 judge.

10 And while the 215 order for metadata is
11 extraordinary in terms of the amount of data
12 acquired. It's also extraordinarily protective in
13 terms of the strict limitations placed on
14 accessing the data.

15 For these reasons I think the program is
16 entirely lawful and conducted in a manner that
17 appropriately respects the privacy and civil
18 liberties of Americans. Thank you.

19 MS. BRAND: Thank you, Steve. Jameel.

20 MR. JAFFER: Thanks for the invitation to
21 participate.

22 Since these programs were disclosed much

1 of the public debate has focused on issues of
2 policy, and I think that's understandable. No
3 government has ever trained this kind of
4 surveillance power upon its own citizens.

5 Until quite recently none had the
6 technological capacity to do that. We need to
7 think carefully about how the exploitation of new
8 technology could affect liberties that generations
9 of Americans have fought to protect.

10 What I'd like to underscore today is that
11 the recently disclosed surveillance programs
12 aren't just unwise, they're unconstitutional as
13 well.

14 And I'm going to focus principally on the
15 215 program with the hope that we'll be able to
16 return to 702 later on.

17 Under the 215 program the NSA collects
18 metadata about every phone call made or received
19 by a resident of the United States.

20 Some news reports indicate that the NSA
21 is collecting Internet metadata as well, making a
22 note of every website an American visits and every

1 email he or she receives.

2 The program is a massive dragnet, one
3 that raises many of the concerns associated with
4 general warrants, that is many of the concerns
5 that led to the adoption of the Fourth Amendment
6 in the first place.

7 You might say that these Section 215
8 orders are general warrants for a digital age.
9 The President and the DNI has emphasized that the
10 government is collecting metadata, not content.
11 But the suggestion that metadata collection is
12 somehow beyond the reach of the Constitution is
13 wrong.

14 For Fourth Amendment purposes the crucial
15 question isn't whether the government is
16 collecting metadata or content, but whether it is
17 invading reasonable expectations of privacy. And
18 here it clearly is.

19 The Supreme Court's recent decision in
20 Jones is instructive. In that case a unanimous
21 court held that long-term surveillance of an
22 individual's location constituted a search under

1 the Fourth Amendment.

2 The justices reached that conclusion for
3 different reasons, but at least five justices were
4 of the view that the surveillance infringed a
5 reasonable expectation of privacy.

6 Justice Sotomayor observed that tracking
7 an individual's movements over an extended period
8 allows the government to generate, quote, a
9 precise comprehensive record that reflects a
10 wealth of detail about her familial, political,
11 professional, religious and sexual associations.

12 The same can be said of the tracking now
13 taking place under Section 215. Call records can
14 reveal personal relationships, medical issue, and
15 political and religious affiliations. Internet
16 metadata may be even more revealing, allowing the
17 government to learn which websites a persons
18 visited, precisely which article she read, whom
19 she corresponds with, and who those people
20 correspond with.

21 The long-term surveillance of metadata
22 constitutes a search for the same reasons that the

1 long-term surveillance of location was found to
2 constitute a search in Jones.

3 In fact, the surveillance that was found
4 unconstitutional in Jones was narrower and
5 shallower than the surveillance now taking place
6 under Section 215.

7 The location tracking in Jones was meant
8 to further a specific criminal investigation into
9 a specific crime and the government collected
10 information about one person's location over a
11 period of less than a month.

12 What the government has implemented under
13 Section 215 is an indiscriminate program that has
14 already swept up the communications of millions of
15 people over a period of seven years.

16 Some have argued that Section 215, the
17 program under Section 215 is lawful under Smith v.
18 Maryland, which upheld the installation of a pen
19 register in a criminal investigation.

20 But the pen register in Smith was very
21 primitive. It tracked the numbers being dialed
22 but it didn't indicate which calls were completed,

1 let alone the duration of the calls, and the
2 surveillance was directed at a single criminal
3 suspect over a period of less than two days. The
4 police weren't casting a net over the whole
5 country.

6 Another argument that's been offered in
7 defense of the metadata program is that though the
8 NSA collects an immense amount of information, it
9 examines only a tiny fraction of it.

10 But the Fourth Amendment is triggered by
11 collection of information, not simply by the
12 querying of it. The same is true of the First
13 Amendment because the chilling effect of
14 government surveillance stems from the collection
15 of information, not merely the analysis of it.

16 The Constitution isn't indifferent to the
17 government's accumulation of vast quantities of
18 sensitive information about American's lives,
19 neither should the board be.

20 Indeed it's worth remembering in this
21 context that other countries have aspired to total
22 awareness of their citizens' associations,

1 movements and beliefs. The experiences of those
2 countries should serve as a caution to us, not as
3 a road map.

4 Thank you again for inviting me to
5 participate, and I look forward to the board's
6 questions.

7 MS. BRAND: Thank you. Kate.

8 MS. MARTIN: Thank you also for inviting
9 me and giving me this opportunity to participate
10 today.

11 I want to take this opportunity to raise
12 some overarching concerns which I hope the board
13 will address before making specific
14 recommendations about necessary changes to either
15 Section 702 or 215, and begin by quoting Senator
16 Sam Ervin, who in 1974 as the author of the
17 Privacy Act noted that the more the government
18 knows about us, the more power it has over us.
19 When the government knows all of our secrets we
20 stand naked before official power. The Bill of
21 Rights then becomes just so many words.

22 I think it is not debatable that secrecy

1 increases the danger that the government will
2 overreach, nor is it debatable that foreign
3 intelligence activities depend to some degree on
4 secrecy and that a democracy must continually work
5 to figure out ways to provide for the national
6 defense, while respecting civil liberties and
7 preserving constitutional governments.

8 The increase in technological
9 surveillance capabilities, global connectedness
10 and the reliance on electronic communications in
11 daily life has made doing this more complex and
12 even more important.

13 I want to ask however whether or not the
14 expansion of secret government surveillance and
15 secret legal authorities, especially in the last
16 twelve years requires us to ask whether we are
17 witnessing the serious erosion of our
18 constitutional system of checks and balances, and
19 the rise of a system of secret law decreed by
20 courts, carried out in secret, enabling the
21 creation of massive secret government databases of
22 American's personal and political lives.

1 As you know quite well, the system of
2 checks and balances relies upon, first, the
3 existence of a Congress which engages in and is
4 influenced by a public debate.

5 It relies upon the existence of courts
6 which hear two sides to a question and know their
7 opinions are subject to appeal and subject to
8 public critique.

9 And finally, an Executive Branch who will
10 be called to account should they ignore or violate
11 the law.

12 And fundamentally all of this depends
13 upon the existence of an informed and engaged
14 press and public.

15 So why does it matter? I think it
16 matters fundamentally for two reasons. First is
17 that the system is set up in order to prevent the
18 government from breaking the law and to ensure
19 that if it does so that will become known and the
20 Executive Branch will be held to account for doing
21 so.

22 Secondly, the system is meant to prevent,

1 as Jameel outlined, the government from using its
2 surveillance capabilities to target its political
3 opponents, to chill political dissent, and to
4 limit the political debate and options in this
5 country.

6 This is not a theoretical concern. Of
7 course in my lifetime it has happened many times
8 already in this country.

9 Perhaps later on I could detail what I
10 find to be the shocking revelation of the history
11 of these programs, beginning in 2001 and resulting
12 in where we are today, where we only learned
13 through unauthorized leaks that there is at least
14 one secret opinion authorizing the massive
15 collection of telephony metadata.

16 We still don't know what the secret law
17 is about the collection of massive amounts of
18 Internet metadata. Although we know that
19 presumably this administration has stopped that,
20 we have no idea whether or not there is law that
21 would permit that to resume.

22 I think that the question that we need to

1 ask is whether or not the system of checks and
2 balance needs to be reaffirmed so that it acts as
3 a safeguard against these two harms.

4 There is, I think the history of the
5 debates on these issues over the past few years
6 demonstrate that the debate has been incomplete.
7 It has been informed by inaccurate information at
8 best supplied by the government, if not
9 deliberately.

10 Finally I just want to note that I've
11 worked on these FISA issues for almost a quarter
12 of a century and I think that probably of the many
13 civil liberties voices that have been raised in
14 objection to these programs, I am maybe one of the
15 least likely to be labeled an alarmist.

16 MS. BRAND: Thank you. I know you have
17 more you wanted to get to, and David may have
18 mentioned this too, but any of the panelists and
19 anyone in the public can submit written comments
20 to the board, so if you have a fuller statement
21 that you'd like to submit, you're welcome to do
22 that.

1 Judge Robertson.

2 MR. ROBERTSON: Thank you. I should
3 probably first state that I am a member, I am now
4 and have been a member of the Liberty and Security
5 Committee of the Constitution Project, which wrote
6 a report in September of 2012 expressing some
7 alarm about these programs. And I signed that
8 report and stand by it, but that's not primarily
9 what I want to talk about today.

10 I did sit on the FISA Court for a few
11 years. I asked to be appointed to the FISA Court,
12 frankly to see what it was up to. And I came away
13 from it deeply impressed by the careful,
14 scrupulous, even fastidious work that the Justice
15 Department people, and the NSA, and FBI agents
16 involved with it did.

17 The FISA Court was not a rubber stamp.
18 The fact, the numbers that are quoted about how
19 many reports, how many warrants get approved do
20 not tell you how many were sent back for more work
21 before they were approved.

22 So I know at firsthand, and I wish I

1 could assure the American people that the FISA
2 process has integrity and that the idea of
3 targeting Americans with surveillance is anathema
4 to the judges of the FISA Court, which they call
5 the FISC.

6 But I have a couple of related points to
7 make. First, the FISA process is ex parte, which
8 means it's one sided, and that's not a good
9 thing.

10 And secondly, under the FISA Amendment
11 Act, the FISA Court now approves programmatic
12 surveillance, and that I submit and will discuss
13 for a few minutes, I do not consider to be a
14 judicial function.

15 Now judges are learned in the law and all
16 that, but anybody who has been a judge will tell
17 you that a judge needs to hear both sides of a
18 case before deciding.

19 It's quite common, in fact it's the norm
20 to read one side's brief or hear one side's
21 argument and think, hmm, that sounds right, until
22 we read the other side.

1 Judging is choosing between adversaries.

2 I read the other day that one of my former FISA
3 Court colleagues resisted the suggestion that the
4 FISA approval process accommodated the executive,
5 or maybe the word was cooperated. Not so, the
6 judge replied. The judge said the process was
7 adjudicating.

8 I very respectfully take issue with that
9 use of the word adjudicating. The ex parte FISA
10 process hears only one side and what the FISA
11 process does is not adjudication, it is approval.

12 Which brings me to my second and I think
13 closely related point. The FISA approval process
14 works just fine when it deals with individual
15 applications for surveillance warrants because
16 approving search warrants and wiretap orders and
17 trap and trace orders and foreign intelligence
18 surveillance warrants one at a time is familiar
19 ground for judges.

20 And not only that, but at some point a
21 search warrant or wiretap order, if it leads on to
22 a prosecution or some other consequence is usually

1 reviewable by another court.

2 But what happened about the revelations
3 in late 2005 about NSA circumventing the FISA
4 process was that Congress passed the FISA
5 Amendments Act of 2008 and introduced a new role
6 for the FISC, which was to approve surveillance
7 programs.

8 That change, in my view, turned the FISA
9 Court into something like an administrative agency
10 which makes and approves rules for others to
11 follow.

12 Again, that's not the bailiwick of
13 judges. Judges don't make policy. They review
14 policy determinations for compliance with
15 statutory law but they do so in the context once
16 again of adversary process.

17 Now the great paradox of this
18 intelligence surveillance process of course is the
19 undeniable need for security. Secrecy, especially
20 to protect what the national security community
21 calls sources and methods.

22 That is why the Supreme Court had to

1 refuse to hear Clapper versus Amnesty
2 International. The plaintiffs could not prove
3 that their communications were likely to be
4 monitored so they had no standing. That is a
5 classic catch-22 of Supreme Court jurisprudence.

6 But I submit that this process needs an
7 adversary, if it's not the ACLU or Amnesty
8 International, perhaps the PCLOB itself could have
9 some role as kind of an institutional adversary to
10 challenge and take the other side of anything that
11 is presented to the FISA Court.

12 Thank you.

13 MS. BRAND: Thank you, Judge. Ken.

14 MR. WAINSTEIN: Okay, good morning,
15 everybody. I'd like to thank the board for
16 inviting me here to speak on these very important
17 issues.

18 I'd like to focus my remarks today on the
19 FISA Amendments Act and the authority in Section
20 702.

21 MS. BRAND: Ken, can you pull the mic
22 over to you.

1 MR. WAINSTEIN: I'm sorry. As I said,
2 I'd like to focus my remarks today on the FISA
3 Amendments Act and the Section 702 authority that
4 David has described earlier.

5 The recent disclosures regarding the
6 PRISM Program have raised questions in some
7 quarters about the appropriateness and legality of
8 the government's collection of Internet
9 communications traffic, with some expressing
10 surprise that collection of that type and that
11 scale is taking place.

12 A review of the text of the FISA
13 Amendments Act and the historical record reveals
14 however that that Internet collection appears to
15 be exactly what was contemplated when Congress
16 passed that statute in 2008.

17 I'd like to take a moment to remind
18 ourselves about the FAA, the FISA Amendments Act
19 and the reason it came into being in the first
20 place. In 1978 Congress undertook to create a
21 process by which electronic surveillance of
22 foreign powers or their agents must first be

1 approved by the FISA Court.

2 In doing so however Congress recognized
3 it had to balance the need for a judicial review
4 process for domestic surveillance against the
5 government's need to freely conduct surveillance
6 overseas where constitutional protections do not
7 apply.

8 It sought to accomplish this objective by
9 imposing in the FISA statute a court approval
10 requirement on surveillances directed against
11 persons within the U.S. and leaving the
12 intelligence community free to surveil overseas
13 targets without the undue burden of court
14 process.

15 With the change in technology over the
16 years since FISA was passed however that foreign
17 domestic distinction started to break down. And
18 the government found itself expending significant
19 manpower in generating FISA Court applications for
20 surveillances against persons outside the United
21 States, the very category of surveillances that
22 Congress specifically intended to exclude when it

1 imposed the FISA Court approval process
2 requirement in 1978.

3 As this problem got worse, particularly
4 after the 9/11 attacks, the government found
5 itself increasingly unable to cover its
6 surveillance needs.

7 Congress, to its credit, took up this
8 issue in the spring of 2007 and over the next
9 fifteen months or so numerous government
10 officials, including Steve Bradbury, myself and
11 others, spent countless hours testifying and
12 meeting with members and staff up on the hill, and
13 after thorough analysis and deliberations Congress
14 ultimately provided relief in the form of the FISA
15 Amendments Act, which passed in the summer of
16 2008.

17 Section 702 of the FAA created a new
18 process, a new process by which categories of
19 foreign surveillance targets can be approved for
20 surveillance.

21 Under this process, the Attorney General
22 and the DNI provide the FISA Court annual

1 certifications identifying the target categories
2 and certifying that all statutory requirements for
3 surveillance of those targets have been met.

4 The government in turn designs targeting
5 procedures which are the operational steps that it
6 takes to determine whether each individual
7 surveillance target is outside the United States,
8 as well as minimization procedures that David
9 described, that limit the handling and
10 dissemination of any information relating to U.S.
11 persons.

12 The government then submits the
13 certifications, as well as the targeting and
14 minimization procedures for review by the FISA
15 Court and the FISA Court confirms whether all
16 statutorily required steps have been taken in
17 compliance with FISA and the Fourth Amendment.

18 Now this process succeeds in bringing the
19 operation of FISA back in line with its original
20 intent. It still provides that any surveillance
21 targeting a U.S. person here or abroad, or
22 targeting any person believed to be inside the

1 United States must be conducted pursuant to an
2 individualized FISA Court order.

3 However, it allows the government to
4 conduct surveillance of foreign targets overseas
5 without the need to secure individualized court
6 approval. And it does so while at the same time
7 giving the FISA Court an important role in
8 ensuring that this authority is used only against
9 those non-U.S. persons who are reasonably believed
10 to be located outside the U.S.

11 In addition, the FAA tasks various levels
12 of government with conducting significant and
13 meaningful oversight over this authority.

14 The authority procedures and oversight
15 prescribed by the FAA have been in place since
16 2008 and just last year they were reauthorized.

17 Prior to its reauthorization the
18 intelligence committees of both houses were
19 briefed on the classified details of its
20 implementation, and that same briefing was made
21 available to all members.

22 As this history demonstrates the FAA was

1 a carefully calibrated piece of legislation that
2 addressed an urgent operational need while at the
3 same time maintaining the privacy protections that
4 the original FISA statute afforded to domestic
5 communications.

6 With the recent public disclosures about
7 the PRISM Program we are now seeing the statute in
8 action. Not surprisingly we're seeing exactly
9 what was contemplated when Congress carefully
10 considered and passed the FAA, which is a program
11 that focuses on the surveillance of foreign
12 national security targets, which is where the
13 Executive Branch has its greatest latitude, that
14 is conducted well within the bounds of the Fourth
15 Amendment, that is carried out with the knowledge
16 and engagement of all three branches of government
17 and that is monitored with multiple levels of
18 oversight.

19 And that is exactly what Congress and the
20 American people asked for in the legislative
21 process that resulted in the passage of the FAA.

22 I appreciate the opportunity to address

1 these issues here today and I look forward to any
2 questions that the board may have.

3 MS. WALD: Thank you. We're now going to
4 enter into the second phase of our program and
5 that is, each person on the panel gets two minutes
6 to respond to any of the comments or to make their
7 own comments upon what other panelists have said.
8 So we'll get the going, Steve.

9 MR. BRADBURY: Thank you, Judge Wald.
10 Just real quick responding to a few points that
11 Jameel made first.

12 Jameel said that he thought no other
13 country conducts surveillance like the NSA. I
14 don't think anybody here should leave today
15 assuming that statement is correct.

16 In terms of the 215 telephone metadata
17 collection, he described it as a dragnet. I think
18 of a dragnet as a collection of mass amounts of
19 content communications, not metadata. I think
20 there's a critical difference between content and
21 metadata, and I think the Constitution recognizes
22 that.

1 He talked about the Jones case which is
2 the GPS tracking device that's put on a particular
3 car for a particular individual. Well that case
4 involved, as he described it, tracking of an
5 individual, the government doggedly following
6 around and tracking a particular individual.

7 Here in the collection of the metadata
8 there's no targeting or tracking of an individual
9 until a suspicious number is put into the
10 database.

11 And the targeting under the 702 order is
12 only focused on non-U.S. persons believed to be
13 outside the U.S.

14 He described the Smith versus Maryland
15 case as simply a case involving a primitive device
16 and focused on an individual. Well, this case has
17 been applied by the lower courts more broadly and
18 also the fact that it was focused on an individual
19 there I think is more constitutionally significant
20 than a general collection of metadata.

21 I want to talk for just a minute about
22 some of the comments that Kate and Judge Robertson

1 made about secrecy and the rise of secret law and
2 also the role of the court with programmatic
3 orders, etcetera.

4 I think it's important to understand the
5 constitutional background. As Ken alluded, before
6 1978 surveillance for foreign intelligence
7 purposes was conducted by the president without
8 court approval. And the courts have consistently
9 said that the president has authority to undertake
10 such surveillance without court approval where the
11 target is a foreign intelligence threat.

12 And FISA -- that led to abuses, but FISA
13 was created as a compromise between the branches
14 to enable that kind of surveillance but to involve
15 Article III courts in the review and approval, and
16 Congress in the oversight, creating the
17 intelligence oversight committee.

18 MS. WALD: Steve, I'm going to have to be
19 very tough. You've covered an enormous amount and
20 I'm sure --

21 MR. BRADBURY: Thank you.

22 MS. WALD: You can pick up in the

1 individual questions, which will come about later.

2 Thank you. Jameel.

3 MR. JAFFER: So let me just start by
4 expressing a degree of frustration about something
5 that Mr. Wainstein said.

6 So when we were before the Supreme Court
7 in *Amnesty v Clapper* last year, the government
8 repeatedly said, and they said this in the lower
9 courts as well, they repeatedly said that the
10 assertion that the NSA was engaged in large scale
11 surveillance of Americans' international
12 communications under Section 702 was speculative
13 and even paranoid.

14 And now the program has been disclosed
15 and everybody can see that the NSA is engaged in
16 exactly that. And the intelligence community, and
17 I would include Mr. Wainstein in that category,
18 the intelligence community's position now is that,
19 well, this is what was contemplated by the
20 statute. Everybody knows that this is what the
21 statute was all about.

22 And you know, there's a certain

1 frustration I feel in this sort of moving target.
2 You know, a year ago it was speculative and
3 paranoid and now there's nothing to see here.

4 And it would trouble me less if it
5 weren't part of a pattern in which the Executive
6 Branch officials and members of the larger
7 intelligence community have repeatedly misled the
8 public about the scope of these surveillance laws
9 and the safeguards that are in place or aren't in
10 place to protect individual's privacy.

11 And on a related topic I think it's just
12 very important, Mr. Bradbury points out quite
13 rightly that under 702 the government can target
14 only foreign nationals outside the United States
15 but nobody should take that to mean that
16 Americans' communications aren't being collected.

17 In the course of collecting the
18 communications of people outside the United States
19 the NSA collects Americans' communications. And
20 not just their international communications, but
21 their domestic communications as well.

22 That too, that assertion I just made was

1 something characterized by the government in
2 Amnesty v. Clapper as speculative and paranoid but
3 the minimization procedures that have been
4 disclosed over the last few weeks I think make
5 clear that that's exactly what's taking place.

6 MS. WALD: Kate.

7 MS. MARTIN: So I just want to reiterate
8 that I think Ken illustrated the importance of the
9 history in looking at these programs. I would
10 disagree with his, and Steve's as well,
11 description of that history.

12 I think that as Jameel mentioned, the
13 important question here is not under what
14 circumstances can the NSA collect and use
15 communications by foreigners overseas.

16 The important question that we've always
17 tried to focus on is under what circumstances is
18 the NSA going to collect and use in secret
19 information about Americans usually gathered
20 inside the United States, including both metadata,
21 which is extremely revealing of their associations
22 and private life, and the content of their

1 communications, especially communications with
2 people located overseas.

3 To repeatedly focus on or to state that
4 the purpose of this surveillance is about
5 foreigners overseas I think is confusing at best
6 about the real issues that face the American
7 people.

8 I just, I think the other issue that's
9 underlying here is that it's not only a question
10 of collection of course but it's a question of how
11 the government uses the information. Many of
12 those regulations are secret about how the NSA or
13 the FBI is allowed to use them.

14 To the extent that there are public
15 regulations they're extremely complex to figure
16 out which set of regulations applies to which set
17 of information, and that fundamentally I think
18 they don't address the problem that the government
19 is in a position perhaps to use information about
20 Americans against Americans. And that's the issue
21 that needs to be addressed.

22 MS. WALD: Jim.

1 MR. ROBERTSON: Perhaps two quick
2 points. It is certainly true that a government
3 request for business records is not a search, but
4 I think we all need to pay attention to what
5 Jameel said about this subject and about the Jones
6 case, because modern technology enables analysis
7 of metadata that was not possible before.

8 It reminds me of something that Ben
9 Bradlee is supposed to have said about Woodward
10 and Bernstein. He said if you give those guys
11 enough steel wool they will knit a stove.

12 Secondly, as to Ken Wainstein's point
13 that we got exactly what Congress asked for.
14 That's true, but the brouhaha after the Snowden
15 leaks, and this meeting indeed establishes what I
16 think is true that we need to have a more wide
17 open debate about this in our society and
18 thankfully we're beginning to have the debate, and
19 this meeting is part of it.

20 MS. WALD: Ken.

21 MR. WAINSTEIN: Thank you. I'd like to
22 start off by responding to Jameel's suggestion

1 that I or others misled him in any way about the
2 collection of U.S. person communications. That
3 contention's flat wrong.

4 I spent fourteen, fifteen months with
5 Steve and others up on Capitol Hill explaining the
6 intricacies of the procedure that ended up being
7 adopted, or a formula which ended up being adopted
8 in the FISA Amendments Act.

9 We answered every conceivable question on
10 the record and in meetings, in forums like this
11 with privacy groups about the implications of this
12 collection, and it was abundantly clear to
13 everybody, and we said numerous times that this
14 will be focusing on foreign targets overseas
15 collecting their communications, whether those
16 communications were overseas or also if they happen
17 to come into the United States.

18 So what he's getting at is the concept of
19 incidental collection. While you're targeting a
20 foreign person, a non-U.S. person overseas, you'll
21 get that person if he and she is talking to
22 somebody in an overseas country. You'll also get

1 that communication if he or she calls somebody in
2 the United States.

3 That's authorized collection and the
4 collection of that U.S. person's communication is
5 acceptable. That's what happens in any form of
6 authorized collection.

7 If you look at Title III, which is the
8 criminal rule that allows criminal wiretaps, the
9 same thing happens. If I'm a criminal suspect a
10 court authorizes a Title III wiretap on me, the
11 government's also going to get the communications
12 between me and the pizza delivery man when I call
13 to get pizza, not only with other criminal
14 colleagues.

15 So that incidental collection is a
16 reality of any kind of surveillance and it's
17 something that was fully vetted and made clear to
18 the American people.

19 And then the second point I'd very
20 quickly make, which is, you know, Kate talked
21 about the collection and the use of this
22 information in secret and the concern about how

1 this information is used.

2 I think one thing that's not touched on
3 sufficiently is the value of oversight. You can
4 take a look at the FAA in itself it prescribed
5 four or five or six different types of oversight.
6 And all these programs are carefully overseen by
7 the FISA Court, by Congress and importantly within
8 the Executive Branch itself and that oversight is
9 very important and meaningful in terms of
10 preventing abuses. Thank you.

11 MS. BRAND: Okay, thank you all. Pat and
12 I will now ask some questions of the panel. We
13 sort of agreed in a sidebar here that since we
14 have a bit of time, I think we started a little
15 early, we can be a little bit more flexible with
16 the length of your responses to these questions,
17 but let's try to keep it not beyond three minutes
18 maybe. But we don't need to be so strict about
19 it.

20 My first question deals with the
21 relevance standard in Section 215. I'm
22 particularly interested in all of your views about

1 that. So each of us will throw a question open to
2 all of you so you can answer in turn, if you
3 want. If you want to pass on the question, that's
4 fine too.

5 Section 215 authorizes an order for
6 tangible things that are relevant to an ongoing
7 FISA investigation. And I have several sort of
8 sub-questions related to that.

9 One is whether relevance can attach as
10 the government seems to be asserting to the entire
11 set of data or whether relevance needs to attach
12 to any particular record that's collected.

13 And relatedly whether Congress, which one
14 of those things Congress understood itself to be
15 passing when it enacted Section 215, the kind of
16 haystack approach or the relevance attaching to a
17 particular record.

18 And then relatedly, and some of those of
19 you with criminal backgrounds, I'd be especially
20 interested how that compares to the way relevance
21 is understood in the criminal context or even in
22 the civil litigating context. Is this

1 understanding of relevance broader? Should it be
2 broader?

3 So Steve, if you want to start with that.

4 MR. BRADBURY: Thanks, Rachel. Well, I
5 began to touch on that I think in my opening
6 remarks.

7 And of course individual members of
8 Congress might say, well, I didn't have in mind
9 this specific concept when I voted for something
10 that says relevant.

11 But I think in adopting the word relevant
12 Congress embraced a broader context in which that
13 word is used embraced frequently and commonly in
14 other situations, administrative subpoenas, for
15 example, civil investigative demand by agencies
16 that regulate industries can be extremely broad in
17 concept of relevance.

18 Civil litigation, a lot of folks who are
19 involved in civil litigation understand that a
20 party in litigation gets a broad right. For
21 example, it could encompass an entire database of
22 information where particular items of data in that

1 database may be useful in the litigation and the
2 parties work out an arrangement that maintains
3 that database so that it can be searched for
4 potentially useful documents. That's under a
5 concept of relevance.

6 Grand juries have an extremely broad
7 concept of relevance when they can go after any
8 materials that are potentially relevant.

9 For example, after the Boston bombing
10 where if there was a concern about follow-on
11 attacks or collaborators, a grand jury could
12 subpoena without court approval all airline
13 manifests of flights in and out, passengers flying
14 in and out of Boston in a particular period of
15 time because one of those people on one of those
16 flights might have been relevant. Communications
17 similarly.

18 So I think the concept of what's relevant
19 to an investigation is naturally understood to be
20 broad in lots of contexts and I think it's
21 reasonable that that's what was incorporated in
22 the statute when Congress adopted it.

1 MR. JAFFER: Well, I agree with some of
2 that, that relevance is, you know, a relatively
3 broad standard, but there are haystacks and there
4 are haystacks.

5 And if you just think about the examples
6 that Mr. Bradbury just provided, for example, this
7 hypothetical situation where a grand jury
8 subpoenas the flight manifests in and out of
9 Boston for a particular period of time, I mean
10 that is not anywhere near the scope of the program
11 we're talking about here.

12 And I think, you know, I can say with
13 confidence, and I'm sure that everybody on this
14 panel will agree with me, that there is no
15 subpoena out there, there's no case out there in
16 which any court has approved on a relevance
17 standard surveillance on this scale.

18 This is, this takes us across a new
19 frontier, maybe several new frontiers. This is
20 orders of magnitude broader than any surveillance
21 that has ever been approved under a civil or a
22 criminal subpoena.

1 MS. BRAND: Can I just ask a quick
2 follow-up to that since this panel is focused on
3 the legality of the alleged current programs.
4 Where would you draw the line then if this
5 haystack is too broad but if your argument is not
6 that each individual record collected needs to
7 itself be relevant, what line do I exercise with
8 the FISC engage in?

9 MR. JAFFER: Well, I don't think that
10 it's possible to set out a line with any more
11 clarity than to refer to relevance.

12 The surprising thing here is not that the
13 court is applying a relevance standard, but that
14 it isn't, that in spite of the statute's clear
15 language that requires it to apply the same
16 standard that applies with respect to ordinary
17 subpoenas, the court has approved the government
18 to collect everything. It has allowed the
19 government to collect everything.

20 And you know, I think it's fair enough to
21 say that relevance doesn't require the kind of
22 specificity that probable cause does.

1 But everybody agrees that relevance is
2 supposed to be a limit, and I think it's quite
3 obvious that relevance isn't doing that work with
4 respect to this kind of order.

5 MS. MARTIN: On the question of what did
6 Congress and the American people understand with
7 regard to the use of the word relevance, I think
8 it's pretty clear that until this past month the
9 American people had no idea that Section 215
10 relevance was being used to collect all of
11 telephone metadata on Americans' phone calls, and
12 I assume that it was also being used to collect
13 all of the Internet metadata.

14 And I think the mere fact that, not only
15 did we not know that, but our assumption during
16 the debates on the FISA Amendments Act was that
17 that was not happening, that that had been part of
18 President Bush's warrantless program, it had been
19 revealed and that it stopped.

20 I think a further indication of that is
21 that in the bible, which I commend to you, on this
22 statute written by Mr. Chris and Mr. Wilson, their

1 description of Section 215 orders during the
2 relevant time period describes a very limited
3 number of orders.

4 And if you were to read that description
5 you would never suspect that the government was
6 using 215 orders to collect millions or billions
7 of records on Americans.

8 And finally in response to the question,
9 Rachel, about well, what should be the standard?
10 Of course 215 is about all different kinds of
11 records. Some of them are more revealing than
12 others. Communications metadata, both telephone
13 and Internet I think are among the most revealing
14 kinds of records covered by 215.

15 One possibility is to go back to what was
16 in the law before 2001 and require a showing that
17 the collection of communications metadata is
18 connected to a specific suspect, a specific
19 incident, a specific plan. That requirement was
20 deleted.

21 And finally on the analogy to the
22 criminal context, I strongly object to that

1 analogy. In the criminal subpoena context there
2 are two key factors that are not present here.

3 One is that at least after the subpoena
4 is served and sometimes during the service of the
5 subpoena, it's public, and that leads to all kinds
6 of restraints on its use, objections to use,
7 etcetera.

8 And secondly, there is the possibility of
9 true adversarial adjudication in the way that
10 Judge Robertson talked about it in a criminal
11 subpoena. That does not exist under Section 215
12 and will not exist even if you allow the recipient
13 of the 215 order to go to the FISA Court, because
14 the recipient of the 215 order is not the party
15 that has the interest in the order. The persons
16 whose information is being sought are the persons
17 who need to have that right to show up in court.

18 MS. BRAND: My question about the
19 criminal context wasn't so much whether it's a
20 completely apt analogy but whether the relevance
21 standard is the same.

22 I mean do you have a view on that,

1 whether the word relevant or relevance in 215 and
2 the concept of relevance in the criminal context
3 or in a civil litigating context are the same?

4 MS. MARTIN: You know, I don't know, but
5 I don't think it's a relevant question, with all
6 due respect. With all due respect.

7 MR. ROBERTSON: Well, I think your
8 relevance question is a great question and I would
9 love to know whether the FISA Court ever has
10 considered the question when it reviewed the
11 program.

12 Relevance is usually raised, it usually
13 comes into question in a legal proceeding if
14 there's an objection, but there's nobody there to
15 object.

16 MR. WAINSTEIN: I'd just like to I guess
17 make two quick points. One, add to something that
18 Steve mentioned about you know, the statements
19 that we've heard from members or former members of
20 Congress saying, you know, gee, I didn't intend
21 when I voted to 215 that it would apply in this
22 way.

1 You know, that's just, just to make it
2 clear, that's not unique to this situation that
3 former or current members of Congress might now be
4 voicing some concern that the way a statute is
5 applied is not exactly as they conceived of it
6 before passage of that statute.

7 You saw that with the authorization for
8 use of military force back in 2001. I've seen it
9 throughout my career with, for example, statutes
10 like the Racketeering Influence Corrupt
11 Organization Act, RICO, which was initially passed
12 and many members thought it was going to be
13 focused on primarily, if not exclusively, on
14 traditional organized crime.

15 And then it has now been applied to a
16 much broader swath of criminal activity, with many
17 people saying, gee, I didn't think when we passed
18 that statute that that's the way it was going to
19 be applied. So just to make it clear, this is not
20 an anomaly, this is a fairly common phenomenon.

21 And then I guess the second point I'd
22 want to make is as to Kate's point. She argues

1 that the criminal grand jury subpoena is different
2 and you can have more comfort in the government's
3 use of those subpoenas and their interpretation of
4 relevance for purposes of using one because these
5 subpoenas will see the light of day ultimately.

6 And that's true for some cases, no
7 question. Those cases where a grand jury subpoena
8 is issued and that grand jury process ripens into
9 an indictment which then goes to trial and the
10 evidence is tested in court, then there's a good
11 chance those subpoenas are going to be turned over
12 in discovery and then tested in a suppression
13 hearing or at trial.

14 But that's not always the case. There
15 are a lot of grand jury subpoenas that I've issued
16 over the years that never see the light of day
17 because that sequence of events doesn't happen.

18 So just to make clear, that's not sort of
19 a perfectly distinguishing feature that would
20 break down the analogy between the grand jury
21 subpoena and 215 which Steve made. Thanks.

22 MS. WALD: Okay. I'd like to delve a

1 little bit into the constitutionality of some of
2 the facets of constitutional analysis of one or
3 both programs, which will give you a chance to
4 elaborate on some things that you may not have
5 been able to catch up on the earlier segments.

6 We already talked a little bit about U.S.
7 v Jones and whether some of the opinions of the
8 Supreme Court justices, and in fact the majority
9 opinion of the D.C. Circuit, which preceded the
10 Supreme Court which suggested that in fact when
11 you have an extensive surveillance of location in
12 that case, but in a sense kind of metadata over a
13 long period of time, it reveals enough of a
14 person's personal life so that it may indeed
15 constitute a search requiring Fourth Amendment
16 compliance.

17 But there are a couple of other aspects
18 and constitutionality that have been brought up,
19 if you want to touch on them.

20 One is, I think this was raised by
21 Senator Feinstein in some of the hearings, and
22 that is whether or not there are less intrusive

1 alternatives.

2 In other words, it was brought up
3 specifically with regard to 215 that do you have
4 to seize, does the government have to, in the
5 alleged program, seize the data or require that it
6 have the data? Would it be less intrusive if it
7 queried the data which was existing in the hands
8 of the communications providers?

9 And in fact, the Executive Order 12333
10 which governs intelligence conduct activities
11 generally, speaks of requiring the least intrusive
12 collection technique feasible.

13 Whether or not it specifically applies to
14 215, we can debate that, but the general principle
15 why isn't it sufficient that they query the
16 communications companies which have the data,
17 rather than requiring that they get all the data.

18 And indeed there's possible
19 constitutional question about, and I think Kate
20 may have raised this, if the alleged program
21 that's under 215 is okay on telephone metadata
22 then are there any inherent limits in 215?

1 I mean are there other kinds of metadata,
2 the fact of bank records, the fact of various
3 other kinds of records, are there inherent limits
4 there?

5 Now what I have left out but I'm going to
6 save it for my next question is the whole FISA
7 Court area and what might possibly, following up
8 on Jim's analysis, could anything be done? Is it
9 better that we not have the government, we not
10 have the court getting into programmatic analysis
11 at all? If not, where are our protections going
12 to be?

13 But that's the question for another day.
14 In this case I'm giving a lot of grist for your
15 mill.

16 Steve.

17 MR. BRADBURY: Thanks. Is that last
18 question for another day or the next question?

19 MS. WALD: No, the FISA question.

20 MR. BRADBURY: I have a lot to say about
21 that so I hope you do ask that.

22 MS. WALD: Well, I'll ask it now but in

1 that case everybody gets six minutes.

2 MR. BRADBURY: Well, on the Jones case I
3 already talked about that.

4 But on your question, Judge Wald, about
5 the database and would it be less intrusive if the
6 telephone companies just maintained the database
7 and what can we get with a business records order,
8 I don't think it's a question of intrusiveness.

9 I don't think it would be less intrusive.
10 It would be far less efficient, far more costly,
11 and perhaps less effective. You'd have to have
12 multiple databases at the different telephone
13 companies.

14 And they don't for business purposes
15 retain this data for as long as the government
16 needs it. This is just business record data they
17 retain for billing purposes. They don't have a
18 separate national security reason for keeping it.

19 So we'd have to create a database. They
20 don't have all the servers and everything. So the
21 government is going to have to create the
22 database, which evidently under this alternative

1 would be housed with the private company, have to
2 pay for it.

3 And of course the government would still
4 have to control the querying because you're not
5 going to tell the telephone company what queries
6 you're going to do to the database. That's
7 national security investigatory information. They
8 don't need to know that.

9 And so it's far more efficient. The
10 government already has facilities in place and it
11 can segregate them. It can ensure that all of the
12 protections are honored and that the data is not
13 being accessed for other reasons, etcetera. So
14 it's really an efficiency question.

15 In terms of --

16 MS. WALD: Just one slight follow-up
17 question, a subordinate question. Is that, are
18 some of those criteria you talked about, in your
19 view more sort of convenience kind of things or
20 are they necessity because when we're talking
21 about constitutional analysis are they necessary
22 to the feasibility or purpose for which the

1 program is related.

2 I mean the cost and that kind of thing
3 sound a lot like convenience factors.

4 MR. BRADBURY: Well, I do think there are
5 very real practical and feasibility requirements.
6 I don't think the Constitution would see a
7 difference between the data being housed with the
8 government or the data being housed elsewhere but
9 the government controlling it and controlling
10 access and ensuring it's preserved, etcetera.

11 But 215 is focused on business records so
12 you have to be talking about the kind of data or
13 database information that a business is
14 maintaining for its own business purposes.

15 So that may be very different with
16 respect to the email that people have alluded to,
17 email metadata under 215. Telephone companies
18 maintain these call detail records for billing
19 purposes and it may be very different in other
20 contexts.

21 So I don't think you can just easily say,
22 oh, well they must be using this for other things

1 too. These are business records that have to be
2 in existence in a separate business, for separate
3 business purpose.

4 Shall I leave the FISA Court questions
5 for later?

6 MS. WALD: Let's do everything but FISA
7 and then come back and do FISA.

8 MS. BRAND: Let's do constitutional now
9 and then save FISA for another round.

10 MS WALD: Well, that is part of FISA.

11 MR. JAFFER: So just to point out the
12 obvious, I think that the least restrictive means
13 question is an important question and a question
14 that the board should be asking.

15 But it assumes that the government has
16 some overriding national security interest to get
17 access to the information in the first place, that
18 this information is somehow crucial to protecting
19 the national security.

20 And that is something that I think many
21 people have been pressing the intelligence
22 community to corroborate, but thus far nothing

1 convincing has been said to establish that this
2 information is actually crucial.

3 I understand that at one point the
4 government pointed to the Zazi case. The Zazi case
5 turns out not to have turned on that kind of
6 information at all.

7 If there is some case out there to which
8 this information was in fact crucial, I don't
9 think the government has pointed to it yet.

10 But, you know, to go back to the
11 question. If we assume that the information is in
12 fact crucial then I think it's crucial to ask the
13 question about the least restrictive means of
14 getting the information.

15 And on that question I do have a problem
16 with this centralized database, the creation of
17 this centralized database in the hands of the
18 NSA. And here I'll take the opportunity just to
19 agree with something that Mr. Wainstein said
20 earlier which is that authorities created for one
21 purpose, it's not uncommon at all to find out
22 later that they were used for some other purpose.

1 That happens all the time, and the same
2 thing is likely to happen with this database.
3 Even if it's true right now that the government
4 queries it very rarely, that the queries are quite
5 narrow, and that only 300 queries have been made
6 thus far, even if all of that is true, and even if
7 all of that satisfies you about the privacy
8 safeguards that are in place right now, you don't
9 know what those privacy safeguards are going to
10 look like three years from now or five years from
11 now.

12 If there is another significant terrorist
13 attack you can imagine the pressure that members
14 of Congress will come under to change the
15 parameters or the intelligence community will come
16 under to change the parameters that govern access
17 to the database.

18 And that massive database of American's
19 most sensitive information will be forever
20 available to the intelligence community to access
21 under whatever standards prevail at that
22 particular point in time.

1 So that's just to say that there are
2 problems that arise from the existence of this
3 kind of centralized database.

4 MS. MARTIN: So I think the truth of the
5 matter is, as you know, that the Supreme Court
6 hasn't answered these questions, that if you start
7 from the understanding that in order for the
8 government to seize or obtain information inside
9 the United States it needs to meet Fourth
10 Amendment requirements, then you end up in one
11 place.

12 If of course there are many situations in
13 which the Fourth Amendment has been held not to
14 apply to government seizures of information. I
15 think that as Jameel says the ability for the
16 government to obtain information and create
17 massive databases raises serious constitutional
18 issues not yet addressed by the court.

19 They're not just Fourth Amendment issues,
20 they are also First Amendment issues about the
21 impact that that has on people's exercise of their
22 First Amendment rights.

1 I think the other constitutionally
2 significant fact is that the seizures are being
3 done in secret. And I know that some of us who
4 worked on the 1994 amendments to FISA which
5 allowed secret searches of American's homes and
6 offices, but in a particularized way with a
7 particularized warrant objected though to that
8 authority because it allowed secret searches of
9 American's homes and offices which would never be
10 revealed to the people whose homes and offices had
11 been searched.

12 That 1994 amendment was enacted before
13 the Supreme Court held in the criminal context
14 that notice of a search was constitutionally
15 required and not just required as a matter of the
16 criminal law.

17 So one of the questions is the
18 applicability of that basic understanding to this
19 kind of search and seizure.

20 And I think on the question of less
21 intrusive alternatives that Jameel is correct, but
22 the initial question is what is the purpose? Less

1 intrusive than what?

2 There is no doubt that if the government
3 is able to create as large a database as possible
4 and use as sophisticated analytics as possible
5 that it will be able to generate information that
6 will be useful from time to time in combating
7 terrorism. There is no doubt about that. And in
8 fact, we've seen that in other countries. I don't
9 think that's the question.

10 I think it's a much more complex
11 question. I think it requires looking at the
12 actual threats that the United States poses,
13 including the scope of those threats, looking at
14 the different ways to meet those threats and
15 looking at the different alternatives that exist
16 other than creating a database that's always
17 available to query.

18 MR. ROBERTSON: I don't have I think a
19 very useful view on least restrictive alternatives
20 or on permanent databases versus accessing the
21 databases that are in the hands of the vendors.

22 But I have to tell you that what keeps

1 running through my mind as this conversation is
2 going on is that this is not only a First
3 Amendment problem and a Fourth Amendment problem,
4 but NRA members, a Second Amendment problem. It
5 is exactly the argument you'll get from the NRA
6 about permanent records of gun ownership. Think
7 about that.

8 MS. MARTIN: Which are not permitted of
9 course.

10 MR. WAINSTEIN: I'm not going to bite on
11 the Second Amendment issue. I'll leave that one
12 for another day and another panel.

13 But I do want, you know, Jameel expressed
14 some agreement with me, and we can't allow too
15 much agreement between Jameel and me so I'm going
16 to have to put a stop to that.

17 But he did, he made the point that, yes,
18 you put legislation in place and it adapts to the
19 situation and it adapts to the needs at that time.
20 That's the way legislation is supposed to be
21 imposed and that's why you have courts to make
22 sure that any adaptations remain true to the

1 original intent of the original legislation.

2 But I guess what I find concerning is the
3 notion that if you have a strong but lawful and
4 appropriate investigative tool in place now, that
5 you should think twice about maintaining it
6 because of some speculative concern that down the
7 road it could be misused.

8 I think that's a recipe for disaster. I
9 think if we were to take that approach we'll end
10 up walking right back into another 9/11. I don't
11 think that's exactly what was suggesting, but that
12 is a concern you see in some of the opinions out
13 there in the real world.

14 I think what instead we need to do is
15 exactly what I believe we learned over the last
16 decade, which is the value of oversight. And
17 oversight, as a government employee, I'll tell you
18 it drove me crazy because I spent half my life
19 running up to Congress answering questions,
20 talking to the FISA Court about their various
21 concerns and questions. And I would have much
22 preferred to stay in my office and work. And many

1 of my former colleagues who are here today
2 probably feel the same way.

3 But we learned the importance of that
4 oversight and making sure that these things, these
5 legislative tools stayed true to the legislation,
6 true to the Constitution. But also because it
7 helped to ensure the confidence of the American
8 people when they knew that that oversight was
9 effective and strong they had confidence in those
10 tools.

11 So instead of taking the approach of
12 scaling back on the strength of appropriate
13 investigative tools now out of some speculative
14 concern of misuse in the future, just make sure
15 you build in the safeguards and the oversight that
16 will prevent that kind of misuse.

17 MS. BRAND: Thank you. I'm going to go
18 back to the statute again, and I apologize if this
19 seems like a quiz, but I want to get the benefit
20 of your views, to the extent that you can provide
21 them.

22 So if you look at section -- my question

1 is whether Section 215 can be interpreted to allow
2 the government to get ongoing production of not
3 yet created business records?

4 So the document that purports to be a
5 leaked 215 order would authorize, would require
6 the company to provide on a daily basis records at
7 a future date. So they haven't yet been created.

8 And the language of Section 215
9 authorizes that production of any tangible things,
10 etcetera, even though this doesn't use the term
11 business records, everyone understands this to be
12 a business records provision.

13 Later in the section there's a proviso
14 that it can only require the production of a
15 tangible thing if such a thing can be obtained
16 with a subpoena duces tecum, etcetera, grand jury
17 subpoena. So I'd like your thoughts on that.

18 And relatedly there is two sections
19 earlier in FISA, there's a pen trap provision,
20 right, which also is based on a relevance
21 standard. Pen traps, as everyone knows, are
22 inherently sort of ongoing and real time, unlike a

1 business records subpoena.

2 In light of the existence of that
3 provision and the limitations of the language in
4 215, do you think that if this leaked order is
5 actually correct, the language of 215 permits
6 that?

7 MR. BRADBURY: Yes, I think it does. I
8 don't think the statute in talking about tangible
9 items distinguishes when the tangible item is
10 created.

11 I think there are a lot of production
12 orders under a relevance standard that require
13 ongoing production of relevant materials. That's
14 common in litigation. It can be common in
15 administrative investigation.

16 The items are created and are records by
17 the time they're turned over, and the order is
18 focused on a known existing category of records
19 that are constantly being refreshed. But they are
20 tangible, they are in existence. They are
21 business records when they're obtained under the
22 order. So I don't think that's a distinction the

1 statute requires or points to.

2 In terms of pen registers, trap and trace
3 devices, that's a different technology. That's
4 for when communications are occurring you're
5 picking up the addressing information, the calling
6 party number, etcetera. So those pen registers
7 would be somewhere out in the network or on the
8 switches, etcetera, in real time collecting all of
9 the calling party number type information when
10 calls are being placed.

11 And this is a business records order
12 because it's actually with the telephone company
13 it's much more efficient to go to their existing
14 databases where they maintain this, the
15 information you're looking for, for billing
16 purposes.

17 Can I just say one quick thing? Jameel
18 has used the word surveillance in describing this
19 215 order. This is not surveillance.

20 Surveillance is a defined term under FISA. That
21 includes getting the content of communications
22 usually when they're being transmitted across a

1 wire, for example.

2 This is not content, this is just
3 metadata. It is not surveillance and it's not
4 accurate to use the word surveillance. Thanks.

5 MR. JAFFER: I think that people can
6 decide for themselves whether it's surveillance or
7 not, in the same way they can decide for
8 themselves whether or it's torture or not. You
9 know, the statutes can define these things but the
10 terms also have ordinary usage.

11 You know, I have a different view of how
12 the statute can be read. I don't think that the
13 statute was meant to allow the government to
14 require the production of records on an ongoing
15 basis.

16 If you take grand jury subpoenas as the
17 relevant comparison, I don't think it's typical
18 for grand jury subpoenas to require ongoing
19 production in that way.

20 And if you look at the legislative
21 history of the statute there is no hint in the
22 legislative history that anybody considered the

1 possibility that this statute could be used for
2 the purposes it's now being used for.

3 In fact, there was this testimony that
4 then Attorney General John Ashcroft gave to
5 Congress I think way back in 2004. It must have
6 been 2004. And he was asked about the outer
7 limits of the Section 215 authority, and at one
8 point somebody asked, you know, could it even be
9 used to require the production of DNA? And he
10 said yes, I suppose it could. And that was sort
11 of the outer limit.

12 But nobody ever suggested, nobody even
13 asked the question, you know, could it be used to
14 require ongoing production of any of these things
15 you just said it could be used to compel the
16 production of. Nobody even contemplated that
17 possibility.

18 So you know, I don't think that the
19 statute can be read that way. I don't think that
20 members of Congress who are advocates of this
21 particular provision thought it would be read that
22 way.

1 And Representative Sensenbrenner, who is
2 often thought of as the grandfather or the father
3 of this provision has spoken out over the last few
4 weeks saying that it had never occurred to him
5 that it would be used in this way.

6 So I think that there's really very, very
7 little to support the proposition that the statute
8 is now being used for the purposes it was designed
9 for.

10 MS. MARTIN: It seems pretty clear that
11 the government has argued that Section 215 can be
12 read this way and that the FISA Judge has agreed
13 with that argument.

14 And I would, in order to evaluate and
15 respond to that argument, I think it should be
16 disclosed and then we can have a discussion about
17 whether or not that interpretation by the
18 government and the FISA Court is a reasonable or a
19 correct one, especially given the existence of
20 overlapping authorities under FISA for pen trap
21 collection.

22 MR. ROBERTSON: I'll pass to Ken.

1 MR. WAINSTEIN: I'll just second what
2 Steve said.

3 MS. WALD: Okay, back to FISA. This is a
4 three part question. Maybe we'll open with Jim
5 and then everybody will get a chance, but since he
6 covered this in his opening remarks.

7 My initial question is whether or not
8 judicial, effective judicial review is necessary
9 to the constitutionality of a program or a
10 statute. That's a general overview question, as
11 one of the ingredients.

12 But Jim, you felt that the court really
13 had no legitimate role in passing on programmatic
14 issues, as opposed to the individual
15 applications.

16 And so to you, I'm directing the
17 question, what would you put in their place? If
18 you took that particular kind of review away from
19 the FISA Court would you be happy with just
20 leaving it with congressional oversight and
21 internal governmental, or what would you do?

22 And the third question to all of you,

1 including Jim, it's been suggested and in some of
2 the comments today too, that maybe you could beef
3 up the FISA Court by having some kind of an ex
4 parte, whether you call it amicus, ex parte,
5 somebody representing the interests of the people
6 involved who don't even know that they're the
7 subject of a FISA Court proceeding, how that would
8 work.

9 But one other, the other one would be on
10 appeals. I mean technically the only people that
11 can appeal a FISA order of this type is the
12 government, if it doesn't get what it wants, or
13 the holder of the records, although many of them
14 complain that they feel that they are hindered
15 because they don't even have access to the secret
16 targeted, original targeting record, so that all
17 they're getting are tasking orders. And so they
18 don't know. They don't feel that they're equipped
19 to do that, even if it was in their interest to do
20 it.

21 But even more specifically the question
22 has been raised in Congress about, and Kate raises

1 it again, is there some way that we can find out
2 what the FISA Court does, because the majority of
3 its opinions are secret.

4 I think in the last congressional
5 reauthorization last December there was a request
6 made and sort of a promise given that they would
7 see, the government would see whether or not some
8 form of redacted order, some form of redacted
9 orders or opinions could be given, but as yet that
10 hasn't happened.

11 The question of whether there's some form
12 of declassification which would give us the
13 benefit of what the legal analysis is, especially
14 when you are dealing with a program of great
15 magnitude such as the 215, alleged 215 program
16 appears to be.

17 Okay, take it away.

18 MR. ROBERTSON: Well, that's about a
19 quint part question I think.

20 MS. WALD: I sneaked it in.

21 MR. ROBERTSON: But let me take the last
22 part of it first. I was frankly stunned when I

1 read the other day that Eric Lichtblau story --

2 Sorry. I was stunned when I read Eric
3 Lichtblau's story about the common law that's
4 being developed within the FISA Court because I
5 frankly have no familiarity with that. And
6 everybody needs to understand that it was eight
7 years ago that I was on the FISA Court.

8 But in my experience there weren't any
9 opinions. You approved a warrant application or
10 you didn't, period.

11 I think there was one famous opinion that
12 was reviewed and reversed by the court of review
13 back in 1902. But a body of law and a body of
14 precedent growing up within FISA is not within my
15 experience. And I don't know what the answer to
16 that question is, how we get hold of it.

17 I'm more comfortable dealing with your
18 question about should there be some sort of an
19 institutional amicus or opponent that deals with
20 FISA issues.

21 And I think I would like to say the
22 answer is yes. My problem is I don't know what it

1 would be or exactly how it would work.

2 I wasn't kidding when I suggested that
3 perhaps some tweaking of the statute establishing
4 the PCLOB might make the PCLOB that institution.
5 But you're not going to ask for that and I don't
6 know who it would be.

7 There is, for example, within the defense
8 department a group of people who are dedicated to
9 the defense of detainees at Guantanamo. They are
10 defense lawyers defending detainees that are being
11 prosecuted by the other part of the defense
12 department.

13 So it is, there is some precedent for
14 it. Whether there would be some institutional
15 office adverse to the office that brings these
16 applications to FISA or not, I don't know but it's
17 conceivable.

18 I'm going to pass on your question of the
19 big constitutionality. I don't think the FISA
20 Court itself, I'm not even sure they have the
21 jurisdiction to pass on the constitutionality of
22 the statute that they're carrying out. But I'm

1 not aware of any constitutional challenge to the
2 FISA statute that's ever been brought before the
3 FISA Court itself. It's got to be handled I think
4 by Article III courts.

5 I don't know if that answers all of your
6 questions.

7 MS. WALD: Well, it goes part way. Thank
8 you.

9 MR. ROBERTSON: Part way.

10 MS. WALD: The rest of the panel,
11 anybody that wants to take a whack at any part of
12 the quartite question.

13 MR. BRADBURY: Sure, I'll take a whack.
14 In terms of whether judicial review is required by
15 the Constitution, well to the extent the Fourth
16 Amendment in a particular situation requires a
17 warrant supported by particularized probable cause
18 approved by a judge, then yes, judicial review is
19 necessary.

20 And of course in the classic warrant
21 context it usually is ex parte. The government
22 comes in with an application with an affidavit and

1 a judge signs a warrant without an opinion often,
2 typically.

3 And the FISA Court is analogous to that
4 model. And there are a few very small number of
5 opinions but as Judge Robertson suggested, most of
6 the time it's an elaborate application, it goes
7 back and forth, and then it's finally approved by
8 the court with the judge's signature. There may
9 be memos internally at the court analyzing issues.

10 I do think that Bob Litt, the general
11 counsel of the DNI said in a congressional hearing
12 the other day that they're scrambling, and I
13 imagine they are, to declassify as many
14 applications and prepare white papers and explain
15 legal analysis to the extent consistent with
16 national security. And I think they're doing
17 that.

18 In terms of replacing the court
19 involvement, I think that again we need to
20 understand the constitutional background is that
21 foreign intelligence surveillance until 1978
22 occurred without court involvement.

1 It was a unilateral action of the
2 Executive Branch that led to lots of abuses and
3 something the authority being used focused on
4 domestic targets.

5 FISA was a big compromise between the
6 branches to bring courts in, and to the extent
7 feasible and consistent with national security, to
8 involve a court, like a warrant type situation in
9 approving surveillance, types of surveillance that
10 used to happen without any court approval.

11 And then to create the intelligence
12 committees on Congress for so Congress could be
13 briefed in, in secure facilities, etcetera.

14 And that's, it is a very unusual animal
15 and I agree with Judge Robertson that it raises
16 some significant questions, for example, with
17 programmatic approvals under 702.

18 But prior to 702, the FISA Court was
19 overwhelmed with individualized orders focused on
20 foreign targets. It was just the court didn't
21 understand why it was spending so much time
22 worrying about non-U.S. persons' privacy outside

1 the United States.

2 So the 702 process was intended to make
3 it easier where it's just focused on foreign
4 targets to collect those communications in and out
5 of the United States to those targets.

6 So it's workable. I think it's a great
7 story that Congress passed this legislation. And
8 when Congress did pass it and consider it, all
9 members of Congress were given the opportunity to
10 be briefed on all the classified details of these
11 programs and all the members of the intelligence
12 committees were briefed.

13 Finally on the amicus participation, I'm
14 not sure that's feasible because the amicus would
15 have to know the classified details of the
16 particular surveillance request and what's up.

17 I mean the court is witting of all, of
18 lots of detailed classified information supporting
19 the probable cause determination or the reasonable
20 suspicion determination and the context of the
21 surveillance. The amicus couldn't, there's not a
22 feasible way for --

1 MS. WALD: Even with a security
2 clearance? I mean for instance in the detainee
3 analogy that somebody raised, I mean the
4 government has a defense layer, as it were, and
5 they do have security clearance, I don't know,
6 that allow them to --

7 MR. BRADBURY: That's right. But number
8 one, the defense lawyer is only given access to
9 what the government is going -- is what's relevant
10 to that particular prosecution.

11 And the government of course always has
12 the choice not to prosecute if the disclosure of
13 some particular information to defense counsel is
14 too worrisome.

15 In this context we're talking about doing
16 surveillance of the most sensitive threats based
17 on the most sensitive national security
18 information, and the Executive Branch is only
19 making it available to the court and to the
20 congressional committees because it's required to
21 by statute.

22 And it's so sensitive that you'd need to

1 have an amicus that's really a permanent. It
2 would probably have to be an officer of the
3 government, whether of the court or of the
4 Executive Branch that would be fully participating
5 in the process and cleared into the same things
6 that the court receives.

7 MS. BRAND: Just to inject one other idea
8 into your comments perhaps, and this has sort of
9 been alluded to, but the federal public defender's
10 office is part of the judiciary essentially,
11 employees of the judiciary hired to oppose the
12 government and I wondered if something like, a
13 model like that would be feasible?

14 MS. WALD: How about some other panel
15 members on anything they want.

16 MR. JAFFER: So I think in the usual case
17 before the FISA Court it would be good to have
18 somebody with access to classified information who
19 could play an adversarial role within the process
20 that already takes place.

21 I'm not convinced that with respect to
22 broader legal questions like is it consistent with

1 the Fourth Amendment for the government to collect
2 all American's telephony metadata. I'm not
3 convinced that that kind of question has to be
4 decided behind closed doors.

5 I don't see why the court couldn't
6 articulate that question publicly, notify the
7 public that it was going to consider the legal
8 implications of a proposal to collect all
9 American's telephony metadata, and allow anyone
10 who wanted to, to file an amicus brief.

11 I think that Mr. Bradbury starts from, I
12 think it's clear, a different assumption than I
13 do. His assumption is that everything that is
14 classified and that has been classified is
15 properly classified, and that is not my view.

16 My view is that a lot of these programs,
17 well, some of the programs that have been
18 disclosed over the last few weeks and the last few
19 years should never have been secret in the first
20 place. They should have been disclosed to the
21 public, at least the general parameters of the
22 program should have been disclosed to the public,

1 both because it's important that the political
2 leaders who put these programs in place be held
3 accountable, but also so that the judicial process
4 can actually function in the way that it's
5 supposed to in an adversarial fashion.

6 And then you know just to expand on
7 something that Judge Robertson said earlier, you
8 know if we're asking the question whether FISA,
9 whether the oversight of the FISA Court is
10 sufficient I think it's important to keep in mind
11 that there are structural limitations on what the
12 FISA Court can do.

13 So even apart from these questions about,
14 you know, is it appropriate that the Chief Justice
15 of the Supreme Court appoints all of the FISA C
16 judges, even apart from questions like that there
17 are structural limitations on what the FISA Court
18 can do.

19 And some of those have to do with the
20 court's jurisdiction. The court doesn't have the
21 jurisdiction to consider First Amendment
22 implications of the government's proposed

1 surveillance. It doesn't have the jurisdiction to
2 consider the facial validity of a statute like the
3 FISA Amendments Act. And the court itself has
4 said that in one of the opinions that was made
5 public a few years ago.

6 And the court doesn't have the authority
7 to consider the constitutionality of the limits
8 on its own jurisdiction.

9 One of the arguments we made in *Amnesty v*
10 *Clapper*, which was our constitutional challenge to
11 the FISA Amendments Act was that the role that the
12 court was playing with respect to surveillance
13 under Section 702 was different from the role
14 that Article III courts are permitted to play
15 under the Constitution.

16 They weren't considering individualized
17 suspicion allegations. They weren't making
18 determinations of probable cause. The government
19 wasn't appearing before the court identifying
20 proposed surveillance targets or proposed
21 facilities to be targeted.

22 Instead the court was making these, and

1 is making these judgments about the
2 appropriateness of the government's programmatic
3 procedures relating to targeting and minimization.
4 And that's something that no Article III court has
5 ever done in the past and is quite foreign to the
6 kinds of things that Article III judges are
7 accustomed to doing.

8 That argument we made before, initially
9 before a judge in the Southern District of New
10 York, but it wasn't heard because our plaintiffs
11 were found ultimately to lack standing.

12 But the point, the narrow point I'm
13 trying to make is just that that is a question
14 that the FISA Court doesn't even have the
15 jurisdiction to consider. The fact that other
16 courts aren't considering it, I think makes it all
17 even more problematic.

18 MS. MARTIN: So I don't know the answer
19 to your question, Judge, but I do think it's
20 important to distinguish and probably limit the
21 role of the FISA Court.

22 I think that it was created, as Judge

1 Robertson said, to issue warrants in the way that
2 judges have always issued warrants.

3 The fact that it is now creating a body
4 of common law is extraordinary, and I'm not sure
5 that is an appropriate function of the court.

6 The fact that that body of common law is
7 being created in secret of course compounds the
8 problem of it being created ex parte.

9 And the fact that the administration,
10 although I take that their promise to try to
11 disclose more information is sincere, I wish that
12 they would work on that before they described to
13 the New York Times and the Wall Street Journal
14 legal opinions which are still classified. We
15 could use the legal opinions themselves.

16 But fundamentally I think we need some
17 kind of system where a traditional Article III
18 court, not the FISA Court, is looking at these
19 questions that have to do with what does the law
20 allow and what's constitutional.

21 And I just in that connection want to
22 push back on the notion that somehow this might be

1 legal even without court involvement because it
2 was done that way before 1978. I disagree with
3 that.

4 But I think more importantly is that we
5 mustn't forget that during the Bush Administration
6 when the FISA statute was exclusive, it explicitly
7 said you may not conduct this kind of surveillance
8 except pursuant to a FISA Court order, and if you
9 do so it is a crime.

10 The Bush Administration in secret
11 violated those provisions and made up a series of
12 flimsy legal arguments for doing so. But most of
13 all, forgot to tell the American people that it
14 was taking the new view that it was no longer
15 bound by FISA. And we only found that out as a
16 result of leaks to the press, which is not the way
17 the system should work, you know.

18 And similarly, just because Mr. Wainstein
19 keeps talking about the efficacy of oversight
20 here. We have a situation during this
21 administration where two members of the oversight
22 committees have repeatedly raised questions about

1 what was happening. They have been repeatedly
2 blocked from bringing those questions to the
3 public. And now here we are as a result of an
4 unauthorized leak.

5 MS. WALD: Okay, Kate. Ken, you get the
6 last word, right of reply.

7 MR. WAINSTEIN: Okay, thank you very
8 much, Judge. I'd like to address the amicus idea,
9 the idea that there should possibly be some other
10 party that would take the side of the person who's
11 to be surveilled in a particular FISA
12 application.

13 A couple of points to keep in mind. One
14 is something that Steve mentioned a few moments
15 ago. Keep in mind that the notion of a judge
16 receiving and assessing an application for a
17 search is not new.

18 As Steve said, this is exactly what we do
19 in the criminal side. When I go to judges like I
20 did with Judge Robertson to get a search warrant
21 as a prosecutor, or to get a Title III wiretap
22 warrant against somebody, that was done ex parte.

1 It was the prosecutor, maybe the agent and nobody
2 on the other side, nobody representing the person
3 whose house is to be searched or the person whose
4 telephone calls were to be listened in to. And
5 that's the paradigm and I think it's important to
6 keep that in mind.

7 You might see, you might be able to sense
8 a theme of mine, which is that this construct on
9 the national security side for these investigative
10 activities all is drawn from parallels and origins
11 on the criminal side. So this idea of an ex parte
12 consideration of warrants is not something that's
13 out of the ordinary. In fact, that is the norm.

14 And the point of that of course is that
15 we trust judges. We trust the judges to look, you
16 know, scrutinize the showing, and in the case of a
17 warrant to make sure that there's probable cause
18 to support that warrant.

19 And I can tell you from experience that
20 judges on the FISA Court, they are Article III
21 judges they are, you know, contrary to what some
22 people have suggested not at all in the

1 government's pocket. They are very independent
2 and they put us through our paces to make sure
3 that what we give them measures up to their
4 standards and the standards in the law.

5 But keeping those two points in mind, the
6 idea of some sort of counter-party is an
7 intriguing one. I think Steve's right that there
8 are a lot of practical issues with that in terms
9 of the sensitivity of the information that the
10 FISA Court judges see. They see the most
11 sensitive information in the intelligence
12 community.

13 But to the extent that that would help
14 establish greater public confidence in the
15 process, I think is something that the board and
16 others should look at, whether it's practical or
17 not, it's hard to say.

18 In addition, Kate mentioned the concern
19 about the transparency. You know, same point
20 there. To the extent that the government can be
21 more transparent with its legal theories, or if
22 the FISA Court, and I don't know whether it can

1 because I haven't seen any of these opinions, but
2 if the FISA Court can disclose some sanitized
3 version of these opinions, it's just good for
4 public education, but it's good because these
5 programs only work so long as we have the
6 confidence in the American public that they're
7 being conducted honestly and reasonably and
8 consistent with the Statute.

9 MS. WALD: Thank you.

10 MS. BRAND: Thank you. My clock here
11 says 11:17. We're scheduled to go to 11:30, I
12 believe. Do the other members of the panel have
13 questions?

14 MR. MEDINE: Yeah, I have a question
15 about the 702 program. Steve and Kate have
16 touched on it.

17 Under that program by definition the
18 target is non-U.S. persons outside the United
19 States, but of course inevitably some of those
20 conversations are with U.S. persons in the United
21 States.

22 My question is whether that raises a

1 Fourth Amendment issue by collecting and using
2 that information involving U.S. persons, and if
3 so, are the minimization procedures in place
4 sufficient to meet Fourth Amendment concerns?

5 MR. BRADBURY: Well, I guess I'm going to
6 go back a little bit to history again. There's
7 been some discussion, Ken mentioned changing
8 technology, you know prior to 1978 and when FISA
9 was first enacted almost all international
10 communications in and out of the United States
11 were carried by satellite, not even covered by
12 FISA.

13 Over time that migrated to fiber optic
14 cables in and out of the U.S. Suddenly if you're
15 conducting that surveillance on a wire in the
16 U.S., even though it's international
17 communication, suddenly it's covered by FISA,
18 individualized orders required. And that was
19 okay. It was workable.

20 But then 9/11 hit, huge problem. We
21 suddenly needed to know about all suspicious
22 communications from thousands of potential

1 terrorist dots outside of the United States. When
2 are they communicating in or out of the U.S.

3 Of course that led to the President's
4 special authority to conduct that surveillance.
5 Very controversial, the disclosures, the debates.

6 Congress grappled with it, ultimately
7 resolved on a statutory solution, 702, which again
8 is targeted at non-U.S. persons reasonably
9 believed to be outside the United States.

10 But it is particularly focused on
11 communications in and out of the United States
12 because just as it was right after 9/11 when the
13 President gave that authorization, those are the
14 most important communications you want to know
15 about if you're talking about a foreign terrorist
16 suspect communicating to somebody you don't know
17 inside the United States, potential planning,
18 etcetera.

19 And 702 enables court involvement,
20 review, approval of procedures to ensure the
21 targeting is focused outside the United States but
22 I don't think the Fourth Amendment and the

1 particularized warrant requirement of the Fourth
2 Amendment would apply to those communications if
3 you're targeting a non-U.S. person reasonably
4 believed to be outside the United States just
5 because some of the communications happen to come
6 in and out of the U.S. if you're not focused on a
7 U.S. person whose privacy interests you're
8 attempting to invade.

9 And whenever you do get into that sphere
10 FISA specifically requires individualized
11 surveillance orders that are very much like
12 warrants, supported by probable cause.

13 Although I still wouldn't say they're
14 warrants because it's not probable cause to
15 believe a crime is being committed or has been
16 committed. It's focused on use of a facility.

17 And it's also important to remember that
18 702 is not limited to terrorism and
19 counterterrorism. What Congress authorized in 702
20 is any foreign intelligence gathering purpose, so
21 it can be much broader. And it's not, it's
22 actually much broader than the President's special

1 authorization in that regard.

2 MR. JAFFER: Well, the government
3 conceded in *Amnesty v Clapper* that surveillance
4 that takes place under 702 implicates the Fourth
5 Amendment and requires the government to establish
6 reasonableness. And in fact, they filed a summary
7 judgement brief in the district court explaining
8 their view that the statute was reasonable, in
9 part because of the minimization procedures that
10 you just referenced.

11 You know at the time we didn't have the
12 minimization procedures so it was very difficult
13 for us to answer that argument.

14 Now we do have the minimization
15 procedures, and one thing that's clear from the
16 minimization procedures is that the use of these
17 words, incidental and inadvertent is highly
18 misleading.

19 The collection of American's
20 communications under this statute is not
21 incidental or inadvertent. As Mr. Bradbury just
22 said, those are the communications that the

1 government was most interested in. The
2 minimization procedures allow the government to
3 retain all of that information, if it's foreign
4 intelligence information, forever. Even if it's
5 not foreign intelligence information for up to
6 five years.

7 The procedures allow the government to
8 collect and retain and disseminate attorney,
9 client communications. There are some are
10 restrictions for communications between attorneys
11 and clients who have been indicted in the United
12 States, but that's a very narrow category compared
13 to the larger category of attorney, client
14 communications more generally.

15 So the statute was designed to allow the
16 government to access American's communications.
17 The procedures reflect that design. And the
18 government has conceded that the Fourth Amendment
19 is not irrelevant to the question of whether this
20 statute is lawful or not.

21 So the I think you're asking the right
22 question. My view is the answer to your question

1 is the minimization procedures are insufficient,
2 insufficient to protect American's privacy.

3 MR. MEDINE: Steve you want a rebuttal?

4 MR. BRADBURY: Can I just say one quick
5 thing? If I said this I misspoke. I did not mean
6 to say the Fourth Amendment is irrelevant or does
7 not apply.

8 I think what I said, what I meant to say
9 is the warrant requirement in the Fourth Amendment
10 wouldn't apply. It would still have to be
11 reasonable under the Fourth Amendment, and that's
12 a special analysis in the foreign intelligence
13 context.

14 MS. MARTIN: Well, I would agree that the
15 Fourth Amendment applies and I think there's a
16 serious question about the applicability of the
17 warrant requirement when the seizure is taking
18 place in the United States, the seizure is
19 deliberately intended to obtain the communications
20 contents of Americans located in the United
21 States.

22 And the argument that was made during

1 consideration of 702 is that the reason why you
2 didn't need a warrant was that an American talking
3 in the United States to somebody else doesn't know
4 whether or not their conversation is being
5 eavesdropped on because that other person could be
6 the subject of a warrant and could be wiretapped.

7 But what you do know and what you, I
8 think, have a right to know is that if you're
9 communicating inside the United States with
10 someone, the government's not collecting the
11 contents unless it has a warrant on you or a
12 warrant on the person you're talking to. And so
13 that's not the case under 702.

14 Then the question becomes, well, what
15 about the practicalities? How do we do this? And
16 I would urge the board to look at proposals that
17 have been talked about by ex-NSA officials which
18 basically would set up a system where by the
19 information might be acquired by the computers but
20 before the government could access the
21 communications of Americans, it would need to go
22 back to the FISA Court and make a probable cause

1 showing and get a FISA warrant.

2 MR. ROBERTSON: That indeed is one of the
3 recommendations of the Constitution Project report
4 that I mentioned when I made my opening remarks.

5 This concept of minimization,
6 minimization is one of the great classic
7 euphemisms of our time. Nobody really knows
8 exactly what it means and I think the board could
9 profitably study that subject in great detail and
10 for weeks.

11 MR. WAINSTEIN: I'd just like to clarify
12 one point Kate mentioned and I might have the
13 phrasing a little bit wrong, but you know, some of
14 these surveillances under 702 could be intended to
15 collect communications of person in the U.S.

16 Just to make clear, there's actually a
17 specific provision in 702 that says you cannot do
18 reverse targeting. I think, David, you mentioned
19 that.

20 So that you cannot, the NSA cannot target
21 somebody who's overseas for the purpose of
22 collecting a communication within the United

1 States. What 702 does permit, and this is I think
2 Kate and I are on the same page on this, is you
3 can target somebody who's overseas, knowing that
4 you're going to collect his or her communications
5 with other people overseas, but also with
6 communications that are inside the United States,
7 which often, as Steve mentioned, are the most
8 valuable or most concerning communications because
9 they might indicate the existence of the plot.

10 But just you have to keep in mind that if
11 you were to try to impose a warrant requirement,
12 we discussed all this in the lead-up to 702. If
13 you try to impose a warrant requirement of some
14 kind to protect the communications of the U.S.
15 person who might be communicating with someone
16 who's rightly targeted overseas, then that same
17 notion would apply to, presumably apply to our
18 12333 collection around the world.

19 You know, and FISA was drafted
20 specifically to work around that collection to
21 make sure that didn't get hindered by the FISA
22 order requirement. And obviously the same thing

1 could to Title III. And so it would be a major
2 paradigm shift in our collections.

3 MR. MEDINE: A quick response from Kate.

4 MS. MARTIN: I just want to, I think Ken
5 and I would agree that the reverse targeting
6 provision in 702 prevents the government from
7 using 702 surveillance in order to obtain the
8 communications of a specific known American.

9 But if the intent of the government is to
10 target someone overseas in order to find out and
11 obtain the communications of people that are in
12 the United States who are talking to somebody
13 overseas, that is the purpose of 702.

14 MS. BRAND: We're almost out of time for
15 this panel but I know Beth has one question. I
16 don't know if Jim has a question, but if we can --

17 MR. DEMPSEY: I'll just make a comment
18 but go ahead.

19 MS. BRAND: Okay, then go ahead. If we
20 could just make it very, very brief.

21 MS. COLLINS COOK: I was actually at the
22 risk of assigning homework going to ask that you

1 all consider my question and if you are so moved
2 provide information afterwards to keep us on
3 track.

4 This is following on some of what we've
5 been talking about, and Kate, you came close to
6 what I was thinking about. But looking at what
7 happened in 2006 with multi-point or roving
8 surveillance, when there was some uncertainty as
9 to how an authorization that was granted by the
10 court would be implemented in a given case, a
11 return requirement was imposed.

12 And my question is whether or not when
13 you're dealing with these more programmatic or
14 bulk authorizations whether it would be
15 appropriate to impose a return requirement through
16 a statutory provision. So whether it's for 702 or
17 whether it would be for this, to use y'all's
18 phrase, programmatic collection under 215 of
19 business records.

20 So I would appreciate your thoughts on
21 that and I will also pose this to panel three, so
22 y'all should come back for panel three and

1 hopefully folks will have some opinions on that.

2 MR. MEDINE: And just to add to Beth's
3 point, 702 provides for judicial review of
4 directives and the question is can the judge's
5 actually review specific targeting requests or
6 only just the broad program as well? And if not,
7 should they be able to under 702?

8 Jim.

9 MR. DEMPSEY: Thank you very much to all
10 the witnesses.

11 I have an observation and I have some
12 homework as well. My observation is up until the
13 very end we really only heard one concrete
14 recommendation for what might be changed, which
15 was Judge Robertson's suggestion which a number of
16 the witnesses engaged with about creating at least
17 for some of the activities of the FISA Court some
18 adversarialness to the process.

19 I'll just say that I really think it's
20 incumbent upon the civil liberties community, of
21 which I consider myself part I guess, but really
22 incumbent upon the civil liberties community to

1 develop some concrete recommendations for moving
2 forward here.

3 It might be that your bottom line is the
4 215 program is inappropriate and should be ended
5 completely. But I think that whether it's 702 or
6 215, you really have to get more granular and more
7 specific in terms of some concrete suggestions.

8 Now at the tail end we started to get to
9 another one here which was this idea that's
10 apparently reflected in the Constitution Project
11 report about acquisition versus then a second
12 search, a search, the particularized search.
13 That's another concrete change.

14 I'll say one thing to Steve and to Ken.
15 I think it's very important for people like you to
16 engage in that process as well. And again, Ken
17 started to at the end in terms of engaging with
18 the idea about the adversarial process.

19 The way this was set up it was a little
20 bit we have two critics of the programs and two
21 defenders of the programs. I really think that
22 there's a role for former government officials to

1 play. It can't be that everything is perfect. It
2 can't be that no changes can be made, that no
3 additional improvements or checks and balances or
4 controls, etcetera can be made.

5 And a little bit I know you're put in
6 this position of somebody says it's terrible and
7 you've got to say it's great. I really think both
8 the civil liberties community has to be more
9 specific in its criticisms and its forward looking
10 suggestions, and I think former government
11 officials, including those who helped design these
12 programs have, I think, a role to play in offering
13 concrete suggestions for how to improve them.

14 And then my sort of follow-up, my
15 homework assignment, I guess to take Beth's term,
16 I would like to see more specific engagement on
17 the question of minimization.

18 Judge Robertson is a hundred percent
19 correct in terms of the misunderstanding at least,
20 or the use of that term in a way that it becomes a
21 mantra and no one really has dug in on that.
22 There is a document online, whether it's valid or

1 not, whether it's still right or not, I think
2 there's a document online that, assuming that
3 minimization procedures looked like what is in
4 that document, what's the reaction to them? How
5 do they play out here? Is it good, is it bad, is
6 it indifferent?

7 Secondly, I think there's some follow-up
8 to be done on the legislative history of Section
9 215. Everybody talks about relevance. Relevance
10 didn't come into the statute until 2005. In 2001
11 the statute said the documents are sought for an
12 authorized investigation. Relevance came in
13 2005.

14 And I think it's worth thinking about
15 what was the possible intent of Congress in
16 shifting from sought for an investigation to
17 specific and articulable facts giving reason to
18 believe that they are relevant to an
19 investigation. Did that have any impact? Should
20 it be viewed as having an impact?

21 And then on the Zazi case I would like to
22 see some, whatever there is on the public record

1 in terms of Jameel had mentioned that. I'd like
2 to see somebody dig in a little bit and spell that
3 out for us.

4 MS. BRAND: Thank you. Thank you, Jim.
5 We're out of the time, unfortunately. But thank
6 you to all the panelists for being here.

7 As I mentioned before, anyone on the
8 panel or in the audience is welcome to submit
9 written comments. Diane Janosek or Sue Reingold
10 can give you the details on how to do that. Thank
11 you.

12 MR. MEDINE: And thanks. We're going to
13 take an hour break for lunch and we'll resume at
14 12:30.

15 (Off the record)

16

17

18

19

20

21

22

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that this is a verbatim transcription of the proceedings; that this transcript is a correct and accurate record of the proceedings, to the best of my knowledge, ability and belief.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

AS WITNESS my hand and notarial seal this _____ day of _____ 2013.

Lynne Livingston

Notary Public

My Commission Expires December 10th, 2014

A	120:11	56:14 82:15	alarm 33:7	52:8 60:16
ability 9:7 75:15 124:8	act 1:7,8 5:12,13 8:17 9:1 12:2	adopted 52:7,7 57:22	alarmist 32:15	76:4 100:3,11
able 23:15 66:5 77:3,5 105:7 119:7	28:17 34:11	adopting 56:11	alien 12:15	american 23:22
abroad 41:21	36:5 37:19	adoption 24:5	allegations 100:17	34:1 43:20
abundantly 52:12	38:3,13,18	adversarial 62:9 97:19 99:5	alleged 59:3 67:5,20 89:15	50:6 53:18
abuses 46:12 54:10 94:2	40:15 52:8	120:18	allow 62:12 78:14 81:1	60:6,9 80:7
acceptable 53:5	60:16 64:11	adversarialness 119:18	allowing 62:12 84:13 96:6	103:13 107:6
access 10:9 17:17,21 71:10	action 43:8 94:1 124:11	adversaries 35:1	98:9 102:20	114:2 117:8
72:17 74:16,20	actions 4:13,15	adversary 36:16 37:7,9	112:2,7,15	americans 22:18
88:15 96:8	active 7:5	adverse 91:15	allowed 50:13 59:18 76:5,8	23:9 27:18
97:18 112:16 114:20	activities 13:10 18:9 29:3	advisor 2:18 16:15	allowing 25:16	29:22 34:3
accessed 10:10 18:3 19:12 70:13	119:17	advisory 4:21 4:22	allows 9:1 25:8 42:3 53:8	47:11 48:16,19
accessing 8:10 22:14 77:20	activity 64:16	advocates 85:20	alluded 46:5 71:16 97:9	49:19 50:20,20
accommodated 35:4	acts 32:2	affect 23:8	alphabetical 15:21	60:11 61:7
accomplish 39:8	actual 77:12	affidavit 92:22	alternative 69:22	74:18 76:5,9
account 30:10 30:20	adaptations 78:22	affiliations 25:15	alternatives 67:1 76:21 77:15,19	98:2,9 111:19
accountable 99:3	adapts 78:18,19	afforded 43:4	amendment 18:10 21:5,10 21:19 24:5,14	112:16 113:2
accumulation 27:17	add 63:17 119:2	age 24:8	25:1 27:10,13	113:20 114:21
accuracy 7:20	addition 19:18 21:15,19 42:11	agencies 13:22 21:10 56:15	34:10 41:17	amicus 88:4
accurate 84:4 124:7	106:18	agency 4:9 36:9	43:15 66:15	90:19 95:13,14
accustomed 101:7	additional 6:17 121:3	agent 105:1	75:10,13,19,20	95:21 97:1
aclu 2:13 16:5 37:7	address 20:7 28:13 43:22	agents 33:15 38:22	75:22 76:12	98:10 104:8
acquire 12:11	50:18 104:8	ago 48:2 90:7 100:5 104:15	78:3,3,4,11	amnesty 37:1,7 47:7 49:2
acquired 17:10 22:12 114:19	addressed 43:2 50:21 75:18	agree 58:1,14 73:19 94:15	92:16 98:1	100:9 111:3
acquisition 20:9	addressing 83:5	113:14 117:5	99:21 108:1,4	amount 22:11 27:8 46:19
	adjudicating 35:7,9	agreed 5:17 54:13 86:12	109:22 110:2	amounts 31:17 44:18
	adjudication 35:11 62:9	agreeing 5:3	111:5 112:18	analogous 93:3
	administration 31:19 102:9	agreement 78:14,15	113:6,9,11,15	analogy 61:21 62:1,20 65:20 96:3
	103:5,10,21	agrees 60:1	amendments 5:13 36:5 37:19 38:3,13 38:18 40:15	analysis 10:16 10:18 11:16 18:18,22 20:14 20:15 27:15 40:13 51:6 66:2 68:8,10 70:21 89:13 93:15 113:12
	administrative 5:7 21:12 36:9	ahead 117:18,19		analysts 19:10
		airline 57:12		analytics 77:4
				analyze 4:13

analyzing 93:9	59:15 63:21	argued 9:4	associations	authorized 8:11
anathema 34:3	75:14 110:2	26:16 86:11	25:11 27:22	8:22 20:10
animal 94:14	113:7,10	argues 64:22	49:21	21:13 53:3,6
annual 40:22	116:17,17	argument 27:6	assume 60:12	110:19 122:12
anomaly 64:20	applying 59:13	34:21 59:5	73:11	authorizes
answer 55:2	appointed 33:11	78:5 86:13,15	assumes 72:15	53:10 55:5
90:15,22	appoints 99:15	101:8 111:13	assuming 44:15	81:9
101:18 111:13	appreciate	113:22	122:2	authorizing
112:22	16:21 43:22	arguments	assumption	31:14
answered 52:9	118:20	100:9 103:12	60:15 98:12,13	available 22:2
75:6	approach 55:16	arrangement	assure 34:1	42:21 74:20
answering	79:9 80:11	57:2	attach 55:9,11	77:17 96:19
79:19	appropriate	article 25:18	attaching 55:16	avenue 1:16
answers 92:5	79:4 80:12	46:15 92:4	attack 74:13	avoid 6:9
anybody 34:16	99:14 102:5	100:14 101:4,6	attacks 40:4	aware 92:1
44:14 84:22	118:15	102:17 105:20	57:11	awareness 27:22
92:11	appropriately	articulable	attempting	
anyones 17:20	4:17 22:17	122:17	110:8	B
apart 99:13,16	appropriaten...	articulate 98:6	attention 51:4	back 18:17
apologize 80:18	38:7 101:2	artificial 3:10	attorney 12:10	33:20 41:19
apparently	approval 12:8	ashcroft 85:4	16:17 40:21	61:15 64:8
120:10	13:6,14 18:11	ashkan 3:7	85:4 112:8,13	72:7 73:10
appeal 30:7	19:18 21:12,18	asked 33:11	attorneys	79:10 80:12,18
88:11	22:8 35:4,11	43:20 51:13	112:10	85:5 87:3
appeals 88:10	35:13 39:9	85:6,8,13	audience 7:1	90:13 93:7
appearing	40:1 42:6 46:8	asking 72:14	123:8	102:22 108:6
100:19	46:10,15 57:12	99:8 112:21	audits 19:21	114:22 118:22
appears 18:8	94:10 109:20	aspects 6:14	august 7:10	background
38:14 89:16	approvals 94:17	66:17	author 28:16	46:5 93:20
applicability	approve 36:6	aspired 27:21	authorities	backgrounds
76:18 113:16	approved 11:10	assemble 20:19	29:15 73:20	55:19
application 90:9	13:19 17:8	asserted 10:6	86:20	bad 122:5
92:22 93:6	33:19,21 39:1	asserting 55:10	authority 21:10	bailiwick 36:12
104:12,16	40:19 58:16,21	assertion 47:10	21:16 37:19	baker 3:14
applications	59:17 90:9	48:22	38:3 42:8,13	balance 32:2
35:15 39:19	92:18 93:7	asserts 14:7	42:14 46:9	39:3
87:15 91:16	approves 34:11	assess 14:4	76:8 85:7 94:3	balanced 4:15
93:14	36:10	assessing 104:16	100:6 109:4	balances 29:18
applied 45:17	approving 10:1	assigning	authorization	30:2 121:3
64:5,15,19	35:16 94:9	117:22	64:7 109:13	baltimore 124:4
applies 50:16	apt 62:20	assignment	111:1 118:9	bank 68:2
59:16 67:13	area 68:7	121:15	authorizations	based 5:21 7:13
113:15	arent 23:12 48:9	associated 10:21	118:14	8:16 11:18
apply 39:7	48:16 101:16	18:6 24:3	authorize 81:5	12:9 18:9 19:2

81:20 96:16	blocked 104:2	54:11 59:1	20:9 21:8 51:3	case 24:20 34:18
basic 76:18	board 1:3 2:1	62:18 72:8	69:7,14,16	45:1,3,15,15
basically 114:18	4:4,5 5:5 6:16	80:17 97:7	71:11,13,14	45:16 51:6
basis 81:6 84:15	6:17 14:18	107:10 117:14	72:1,2,3 81:3	58:15 65:14
beef 88:2	15:1,20 27:19	117:19 123:4	81:11,12 82:1	66:12 68:14
began 56:5	28:12 32:20	break 6:16	82:21 83:11	69:1,2 73:4,4,7
beginning 31:11	37:15 44:2	39:17 65:20	118:19	97:16 105:16
51:18	72:14 106:15	123:13		114:13 118:10
belief 124:8	114:16 115:8	breaking 30:18	C	122:21
beliefs 28:1	boards 4:12 5:7	brennan 3:18	c 1:17 16:1 66:9	cases 6:7 65:6,7
believe 79:15	28:5	brief 6:20 34:20	99:15	casting 27:4
107:12 110:15	bob 93:10	98:10 111:7	cables 108:14	catch 66:5
122:18	bodily 14:6	117:20	cadwalader	catch22 37:5
believed 13:12	body 90:13,13	briefed 20:4	16:14	categories 40:18
41:22 42:9	102:3,6	42:19 94:13	calibrated 43:1	41:1
45:12 109:9	bombing 57:9	95:10,12	call 9:11,12,13	category 39:21
110:4	boston 57:9,14	briefing 20:6	22:3 23:18	47:17 82:18
bellovin 3:3	58:9	42:20	25:13 34:4	112:12,13
ben 51:8	bottom 120:3	bring 94:6	53:12 71:18	cause 11:18 19:5
benefit 15:14	bound 103:15	bringing 41:18	88:4	59:22 92:17
80:19 89:13	bounds 43:14	104:2	called 17:13	95:19 100:18
bernstein 51:10	bradbury 2:11	brings 35:12	18:14,15 30:10	105:17 110:12
best 8:9 32:8	15:22 16:20	91:15	calling 83:5,9	110:14 114:22
50:5 124:8	40:10 44:9	broad 9:5 21:15	calls 9:10 10:14	caution 28:2
beth 4:6 117:15	46:21 48:12	56:16,20 57:6	17:15,18,20	cell 9:21,22 19:1
beths 119:2	56:4 58:6	57:20 58:3	18:15 26:22	center 2:14 3:6
121:15	68:17,20 69:2	59:5 119:6	27:1 36:21	3:18,19 16:8
better 68:9	71:4 82:7	broader 56:1,2	53:1 60:11	centralized
beyond 8:10	92:13 96:7	56:12 58:20	83:10 105:4	73:16,17 75:3
24:12 54:17	98:11 108:5	64:16 97:22	cant 78:14 121:1	century 32:12
bible 60:21	111:21 113:4	110:21,22	121:2	certain 47:22
big 91:19 94:5	bradford 3:17	broadest 20:18	capabilities 29:9	certainly 51:2
bill 28:20	bradlee 51:9	broadly 45:17	31:2	certification
billing 17:12	branch 4:10,13	brought 66:18	capacity 23:6	124:1
22:3 69:17	19:20 30:9,20	67:2 92:2	capitol 52:5	certifications
71:18 83:15	43:13 48:6	brouhaha 51:14	car 45:3	41:1,13
billions 61:6	54:8 94:2	build 80:15	cards 15:13	certify 124:5,9
bipartisan 4:9	96:18 97:4	building 20:16	career 64:9	certifying 41:2
bit 54:14,15	branches 43:16	bulk 118:14	careful 33:13	chairman 2:3
66:1,6 108:6	46:13 94:6	burden 39:13	carefully 23:7	challenge 16:6
115:13 120:20	brand 2:4 4:6	bush 103:5,10	43:1,9 54:6	37:10 92:1
121:5 123:2	14:19,20,22	bushs 60:18	carried 29:20	100:10
bite 78:10	22:19 28:7	business 8:18	43:15 108:11	chance 15:20
block 20:16	32:16 37:13,21	9:2,15 17:3	carrying 91:22	65:11 66:3

87:5	classified 6:2,3	12:4 13:8,12	committee 33:5	48:7 72:22
change 36:8	6:5,8 42:19	13:18 24:11	46:17	74:15,20
39:15 74:14,16	95:10,15,18	27:11,14 31:15	committees 20:1	106:12 119:20
120:13	97:18 98:14,14	31:17 38:8,10	20:4 42:18	119:22 121:8
changed 119:14	98:15 102:14	38:14 44:17,18	94:12 95:12	communities
changes 28:14	clear 49:5 52:12	45:7,20 50:10	96:20 103:22	47:18
121:2	53:17 59:14	52:2,12,19	common 8:1	companies 9:16
changing 108:7	60:8 64:2,19	53:3,4,6,15,21	34:19 64:20	17:11 67:16
characterized	65:18 86:10	61:17 67:12	82:14,14 90:3	69:6,13 71:17
49:1	98:12 111:15	86:21 111:19	102:4,6	company 22:2
checks 29:18	115:16	116:18,20	commonly	70:1,5 81:6
30:2 32:1	clearance 96:2,5	118:18	56:13	83:12
121:3	cleared 97:5	collections	communicating	compared
chief 5:7,8 99:14	clearly 24:18	117:2	109:2,16 114:9	112:12
chill 31:3	client 112:9,13	collects 8:20	116:15	compares 55:20
chilling 27:13	clients 112:11	23:17 27:8	communication	comparison
choice 96:12	clock 107:10	48:19	9:19 11:22	84:17
choose 6:5	close 118:5	collins 2:7	53:1,4 108:17	compel 85:15
choosing 35:1	closed 98:4	117:21	115:22	complain 88:14
chris 60:22	closely 35:13	columbia 3:3	communicatio...	complete 22:2
circle 18:11	collaborators	combating 77:6	9:8,18 14:8	completed 26:22
circuit 66:9	57:11	come 7:19 47:1	21:22 26:14	completely
circumstances	colleague 15:1	52:17 72:7	29:10 37:3	62:20 120:5
49:14,17	colleagues 15:19	74:14,15 110:5	38:9 43:5	completeness
circumventing	35:3 53:14	118:22 122:10	44:19 47:12	7:20
36:3	80:1	comes 63:13	48:16,18,19,20	complex 29:11
citizen 12:15	collect 9:17	92:22	48:21 49:15	50:15 77:10
13:3	49:14,18 59:18	comfort 65:2	50:1,1 52:2,15	compliance
citizens 23:4	59:19 60:10,12	comfortable	52:16 53:11	36:14 41:17
27:22	61:6 95:4 98:1	90:17	57:16 61:12,17	66:16
civil 1:3 4:4,16	98:8 112:8	coming 14:21	67:8,16 83:4	compounds
22:17 29:6	115:15 116:4	commencing	83:21 95:4	102:7
32:13 55:22	collected 9:9,22	1:17	108:10,22	comprehensive
56:15,18,19	10:8,15 11:5	commend 60:21	109:11,14	25:9
58:21 63:3	11:12 14:8	comment	110:2,5 111:20	compromise
119:20,22	26:9 48:16	117:17	111:22 112:9	46:13 94:5
121:8	55:12 59:6	comments 7:7,9	112:10,14,16	computer 3:3,9
clapper 37:1	collecting 8:10	32:19 44:6,7	113:19 114:21	computers
47:7 49:2	23:21 24:10,16	45:22 88:2	115:15 116:4,6	114:19
100:10 111:3	48:17 52:15	97:8 123:9	116:8,14 117:8	conceded 111:3
clarify 115:11	83:8 108:1	commission	117:11	112:18
clarity 59:11	114:10 115:22	4:11 124:19	community 9:20	conceivable
classic 37:5	collection 8:19	committed	14:7 36:20	52:9 91:17
92:20 115:6	9:5,6 11:21	110:15,16	39:12 47:16	conceived 64:5

concept 52:18 56:9,17 57:5,7 57:18 63:2 115:5	55:13,14 56:8 56:12 57:22 60:6 63:20 64:3 74:14	24:22	contexts 20:22 57:20 71:20	96:13 124:10
concern 31:6 53:22 57:10 64:4 79:6,12 80:14 106:18	79:19 85:5,20 88:22 94:12,12 95:7,8,9 109:6 110:19 122:15	constitutes 25:22	continually 29:4	counterparty 106:6
concerning 79:2 116:8	congressional 87:20 89:4 93:11 96:20	constitution 3:17 22:7 24:12 27:16 33:5 44:21 71:6 80:6 92:15 100:15 115:3 120:10	continue 10:12	counterterror... 5:1,11 9:3 20:12 110:19
concerns 4:17 10:13 24:3,4 28:12 79:21 108:4	connect 20:17	constitutional 2:10 5:15 14:17 16:6 20:8 29:7,18 39:6 46:5 66:2 67:19 70:21 72:8 75:17 92:1 93:20 100:10 102:20	contrary 17:22 105:21	countless 40:11
conclusion 25:2	connectedness 29:9	constitutional... 66:1,18 87:9 91:19,21 100:7	contributing 14:12	countries 27:21 28:2 77:8
conclusions 7:19	connecticut 1:16	constitutionally 45:19 76:1,14	control 70:4	country 27:5 31:5,8 44:13 52:22
concrete 119:13 120:1,7,13 121:13	connection 102:21	construct 105:8	controlling 71:9 71:9	countys 5:1
conduct 20:13 39:5 42:4 67:10 103:7 109:4	connections 18:19,20	consultant 3:8	controls 121:4	county 124:4
conducted 22:16 42:1 43:14 46:7 107:7	consequence 35:22	contacts 11:2	controversial 109:5	couple 8:1 34:6 66:17 104:13
conducting 42:12 108:15	consider 34:13 95:8 98:7 99:21 100:2,7 101:15 118:1 119:21	contemplated 38:15 43:9 47:19 85:16	convenience 70:19 71:3	course 8:13 18:20 31:7 36:18 48:17 50:10 56:7 61:10 70:3 75:12 78:9 92:20 96:11 102:7 105:14 107:19 109:3
conducts 44:13	consideration 105:12 114:1	content 17:17 21:22 24:10,16 44:19,20 49:22 83:21 84:2	convinced 97:21 98:3	court 2:16,16 8:6,21 10:1,11 11:18 12:1,8 13:6,19 16:6 16:12 17:5,22 19:15,18 21:7 21:12,18 24:21 33:10,11,17 34:4,11 35:3 36:1,9,22 37:5 37:11 39:1,9 39:13,19 40:1 40:22 41:15,15 42:2,5,7 46:2,8 46:10 47:6 53:10 54:7 57:12 58:16 59:13,17 62:13 62:17 63:9
confidence 58:13 80:7,9 106:14 107:6	considered 4:18 9:15 43:10 63:10 84:22	contentions 52:3	convincing 73:1	
confirming 6:10	considering 100:16 101:16	contents 9:18 113:20 114:11	cook 2:7 4:6 117:21	
confirms 41:15	consistent 93:15 94:7 97:22 107:8	context 21:7 27:21 36:15 55:21,22 56:12 61:22 62:1,19 63:2,3 76:13 92:21 95:20 96:15 113:13	cooperated 35:5	
confusing 50:5	consistently 46:8		correct 44:15 76:21 82:5 86:19 121:19 124:6	
congress 4:11 5:17 8:17 12:7 19:20 20:1,3,5 30:3 36:4 38:15,20 39:2 39:22 40:7,13 43:9,19 46:16 51:13 54:7	consists 17:10		corroborate 72:22	
	constantly 82:19		corrupt 64:10	
	constitute 26:2 66:15		cost 71:2	
	constituted		costly 69:10	
			couldnt 95:21 98:5	
			counsel 2:12 3:16 15:12 16:2 93:11	

65:10 66:8,10 68:7,10 72:4 75:5,18 76:13 79:20 86:18 87:12,19 88:3 88:7 89:2 90:4 90:7,12 91:20 92:3 93:3,8,9 93:18,22 94:8 94:10,18,20 95:17 96:19 97:3,6,17 98:5 99:9,12,15,17 99:20 100:3,6 100:12,19,22 101:4,14,21 102:5,18,18 103:1,8 105:20 106:10,22 107:2 109:19 111:7 114:22 118:10 119:17	119:16 creation 29:21 73:16 credit 40:7 crime 14:5 21:17 26:9 64:14 103:9 110:15 criminal 26:8,19 27:2 53:8,8,9 53:13 55:19,21 58:22 61:22 62:1,10,19 63:2 64:16 65:1 76:13,16 104:19 105:11 criteria 8:6 70:18 critical 20:16 44:20 criticisms 121:9 critics 120:20 critique 30:8 crucial 24:14 72:18 73:2,8 73:12,12 current 59:3 64:3 currently 16:5 cyber 13:9 14:15	71:7,8,12 database 12:5 18:3,11,17 19:8,11 20:13 21:1,4 45:10 56:21 57:1,3 69:5,6,19,22 70:6 71:13 73:16,17 74:2 74:17,18 75:3 77:3,16 databases 29:21 69:12 75:17 77:20,21 83:14 date 9:12 81:7 david 2:3 14:20 15:4 17:2 19:6 32:17 38:4 41:8 115:18 davidson 3:16 day 5:3 6:22 35:2 65:5,16 68:13,18 78:12 90:1 93:12 124:13 days 10:11 17:6 27:3 dealing 89:14 90:17 118:13 deals 35:14 54:20 90:19 death 14:6 debatable 28:22 29:2 debate 23:1 30:4 31:4 32:6 51:17,18 67:14 debates 32:5 60:16 109:5 decade 79:16 december 12:7 89:5 124:19 decide 84:6,7 decided 98:4	deciding 34:18 decision 24:19 declassification 89:12 declassified 5:22 declassify 93:13 decreed 29:19 dedicated 91:8 deeply 33:13 defenders 97:9 120:21 defending 91:10 defense 27:7 29:6 91:7,9,10 91:11 96:4,8 96:13 define 84:9 defined 83:20 definition 107:17 degree 29:3 47:4 deleted 61:20 deliberately 32:9 113:19 deliberations 40:13 delivery 53:12 delve 65:22 demand 56:15 demands 22:7 democracy 3:19 29:4 demonstrate 32:6 demonstrates 42:22 dempsey 2:6 4:7 117:17 119:9 department 3:4 16:2,17 33:15 91:8,12 depend 29:3 depends 30:12	deputy 16:4 19:6 described 15:4 20:15 38:4 41:9 44:17 45:4,14 102:12 describes 9:10 61:2 describing 83:18 description 7:12 49:11 61:1,4 design 112:17 121:11 designated 18:12 designed 8:2 86:8 112:15 designs 41:4 destruction 14:13 detail 25:10 31:9 71:18 115:9 detailed 95:18 details 42:19 95:10,15 123:10 detainee 96:2 detainees 91:9 91:10 determination 95:19,20 determinations 36:14 100:18 determine 13:21 41:6 determined 10:17 develop 120:1 developed 90:4 development 4:18 device 45:2,15
cover 40:5 covered 46:19 61:14 87:6 108:11,17 crazy 79:18 create 38:20 69:19,21 75:16 77:3 94:11 created 4:11 40:17 46:13 73:20 81:3,7 82:10,16 101:22 102:7,8 creating 46:16 77:16 102:3	D d 1:17 16:1 66:9 daily 29:11 81:6 danger 29:1 daniel 3:9 data 11:1,5,7,10 12:4 17:13,21 18:1,2 19:9 22:11,14 55:11 56:22 67:5,6,7 67:16,17 69:15 69:16 70:12	65:10 66:8,10 68:7,10 72:4 75:5,18 76:13 79:20 86:18 87:12,19 88:3 88:7 89:2 90:4 90:7,12 91:20 92:3 93:3,8,9 93:18,22 94:8 94:10,18,20 95:17 96:19 97:3,6,17 98:5 99:9,12,15,17 99:20 100:3,6 100:12,19,22 101:4,14,21 102:5,18,18 103:1,8 105:20 106:10,22 107:2 109:19 111:7 114:22 118:10 119:17	deciding 34:18 decision 24:19 declassification 89:12 declassified 5:22 declassify 93:13 decreed 29:19 dedicated 91:8 deeply 33:13 defenders 97:9 120:21 defending 91:10 defense 27:7 29:6 91:7,9,10 91:11 96:4,8 96:13 define 84:9 defined 83:20 definition 107:17 degree 29:3 47:4 deleted 61:20 deliberately 32:9 113:19 deliberations 40:13 delivery 53:12 delve 65:22 demand 56:15 demands 22:7 democracy 3:19 29:4 demonstrate 32:6 demonstrates 42:22 dempsey 2:6 4:7 117:17 119:9 department 3:4 16:2,17 33:15 91:8,12 depend 29:3 depends 30:12	deputy 16:4 19:6 described 15:4 20:15 38:4 41:9 44:17 45:4,14 102:12 describes 9:10 61:2 describing 83:18 description 7:12 49:11 61:1,4 design 112:17 121:11 designated 18:12 designed 8:2 86:8 112:15 designs 41:4 destruction 14:13 detail 25:10 31:9 71:18 115:9 detailed 95:18 details 42:19 95:10,15 123:10 detainee 96:2 detainees 91:9 91:10 determination 95:19,20 determinations 36:14 100:18 determine 13:21 41:6 determined 10:17 develop 120:1 developed 90:4 development 4:18 device 45:2,15

devices 83:3	discovery 65:12	101:14 114:3	E	encompass
dialed 9:12	discuss 34:12	doggedly 45:5	earlier 38:4 66:5	56:21
26:21	discussed 15:5	doing 29:11	73:20 81:19	ended 52:6,7
diane 5:7 15:12	116:12	30:20 39:2	99:7	120:4
123:9	discussing 6:8	60:3 93:16	early 54:15	engage 59:8
didnt 26:22 56:8	discussion 5:15	96:15 101:7	easier 95:3	120:16
63:20 64:17	5:21 6:1,4 7:12	103:12	easily 71:21	engaged 30:13
90:10 94:20	86:16 108:7	doj 2:11,17 3:14	eavesdropped	47:10,15
111:11 114:2	disseminate	domestic 39:4	114:5	119:16
116:21 122:10	112:8	39:17 43:4	education 107:4	engagement
differ 8:6	disseminated	48:21 94:4	effect 27:13	43:16 121:16
difference 44:20	13:22	dont 21:18	effective 69:11	engages 30:3
71:7	dissemination	31:16 36:13	80:9 87:8	engaging 120:17
different 17:7	14:1 19:16	44:14 50:18	efficacy 103:19	enormous 46:19
25:3 54:5	41:10	54:18 59:9	efficiency 70:14	ensure 4:17
61:10 65:1	dissent 31:3	63:4,5 69:8,9	efficient 69:10	30:18 70:11
69:12 71:15,19	distinct 21:22	69:14,17,20	70:9 83:13	80:7 109:20
77:14,15 83:3	distinction	70:8 71:6,21	efforts 5:1,9	ensuring 4:14
84:11 98:12	39:17 82:22	73:8 74:8 77:8	14:11,14	13:11 42:8
100:13	distinguish	77:18 79:10	eight 90:6	71:10
difficult 111:12	101:20	82:8,22 84:12	either 28:14	enter 44:4
dig 123:2	distinguished	84:17 85:18,19	elaborate 66:4	entire 55:10
digital 24:8	15:7	88:6,15,18,18	93:6	56:21
directed 27:2	distinguishes	90:15,22 91:5	electronic 3:5	entirely 22:16
39:10	82:9	91:16,19 92:5	11:16,22 29:10	equipped 88:18
directing 10:4	distinguishing	96:5 98:5	38:21	eric 90:1,2
87:16	65:19	101:18 106:22	elizabeth 2:7	erosion 29:17
directive 12:10	district 2:15	109:16,22	3:18	erwin 28:16
directives 119:4	16:10 101:9	117:16	email 24:1 71:16	especially 29:15
director 12:11	111:7	doors 98:4	71:17	36:19 50:1
16:5,8 19:6	division 2:18	dots 20:17 109:1	embraced 56:12	55:19 86:19
disagree 49:10	16:16	doubt 77:2,7	56:13	89:13
103:2	dna 85:9	drafted 116:19	emphasized	essential 20:13
disaster 79:8	dni 24:9 40:22	dragnet 24:2	24:9	essentially 4:21
disclose 102:11	93:11	44:17,18	employee 79:17	97:10
107:2	document 81:4	draw 59:4	employees 97:11	establish 73:1
disclosed 7:14	121:22 122:2,4	drawn 105:10	enable 17:19	106:14 111:5
22:22 23:11	documents 6:2,6	drive 10:16	18:18 46:14	establishes
47:14 49:4	6:7,10 21:13	drove 79:18	enables 20:19	51:15
86:16 98:18,20	57:4 122:11	duces 81:16	51:6 109:19	establishing
98:22	doesnt 17:19	due 63:6,6	enabling 29:20	91:3
disclosure 96:12	59:21 65:17	dug 121:21	enacted 55:15	etcetera 46:3
disclosures 38:5	81:10 88:12	duration 17:14	76:12 108:9	62:7 70:13
43:6 109:5	99:20 100:1,6	27:1		71:10 81:10,16

83:6,8 94:13 109:18 121:4	exercise 59:7 75:21	extraordinary 22:11 102:4	feasible 67:12 94:7 95:14,22 97:13	32:11 33:10,11 33:17 34:1,4,7 34:10,11 35:2 35:4,9,10,13 36:3,4,8 37:11 37:19 38:2,12 38:18 39:1,9 39:16,19 40:1 40:14,22 41:14 41:15,17,19 42:2,7 43:4 46:12,12 52:8 54:7 55:7 60:16 62:13 63:9 68:6,19 72:4,6,7,9,10 76:4 79:20 81:19 83:20 86:12,18,20 87:3,19 88:3,7 88:11 89:2 90:4,7,14,20 91:16,19 92:2 92:3 93:3 94:5 94:18 97:17 99:8,9,12,15 99:17 100:3,11 101:14,21 102:18 103:6,8 103:15 104:11 105:20 106:10 106:22 107:2 108:8,12,17 110:10 114:22 115:1 116:19 116:21 119:17
euphemisms 115:7	exist 62:11,12 77:15	extremely 49:21 50:15 56:16 57:6	feature 65:19	
evaluate 86:14	existence 30:3,5 30:13 72:2 75:2 82:2,20 86:19 116:9		federal 5:10 7:14,17 17:5,8 21:11 22:8 97:9	
evening 7:5		F		
event 5:9	existing 67:7 82:18 83:13	faa 38:18 40:17 42:11,15,22 43:10,21 54:4	feel 48:1 80:2 88:14,18	
events 65:17	exnsa 114:17	face 50:6	feinstein 66:21	
everybody 37:15 47:15,20 52:13 58:13 60:1 69:1 87:5 90:6 122:9	expand 99:6	facets 66:2	fellow 4:5	
evidence 14:4 65:10	expansion 29:14	facial 100:2	felt 87:12	
evidently 69:22	expect 5:21	facilities 70:10 94:13 100:21	fewer 11:9 19:8	
ex 34:7 35:9 88:3,4 92:21 102:8 104:22 105:11	expectation 22:4 25:5	facility 110:16	fiber 108:13	
exactly 38:15 43:8,19 47:16 49:5 51:13 64:5 78:5 79:11,15 91:1 104:18 115:8	expectations 24:17	fact 26:3 33:18 34:19 45:18 60:14 66:8,10 67:9 68:2,2 73:8,12 76:2 77:8 85:3 101:15 102:3,6 102:9 105:13 111:6	fields 17:13	
examines 27:9	expending 39:18	factor 26:3 33:18 34:19 45:18 60:14 66:8,10 67:9 68:2,2 73:8,12 76:2 77:8 85:3 101:15 102:3,6 102:9 105:13 111:6	fifteen 40:9 52:4	
example 11:9 56:15,21 57:9 58:6 64:9 84:1 91:7 94:16	experience 90:8 90:15 105:19	factors 62:2 71:3	figure 29:5 50:15	
examples 58:5	experiences 28:1	facts 122:17	file 98:10	
exchange 6:21	experts 15:8	fair 59:20	filed 111:6	
exclude 39:22	expires 124:19	fairly 64:20	finally 30:9 32:10 61:8,21 93:7 95:13	
exclusive 103:6	explain 93:14	familial 25:10	find 11:13 31:10 73:21 79:2 89:1 117:10	
exclusively 64:13	explaining 52:5 111:7	familiar 35:18	fine 35:14 55:4	
excuse 19:13	explicitly 103:6	familiarity 90:5	firm 16:1	
executive 4:9,13 19:20 30:9,20 35:4 43:13 48:5 54:8 67:9 94:2 96:18 97:4	exploitation 23:7	famous 90:11	first 4:5 6:13,15 8:16 13:7 14:16 15:2 18:10 24:6 27:12 30:2,16 33:3 34:7 38:19,22 44:11 54:20 72:17 75:20,22 78:2 89:22 98:19 99:21 108:9	
	expressed 78:13	far 69:10,10 70:9 72:22 74:6	firsthand 33:22	
	expressing 33:6 38:9 47:4	fashion 99:5	fisa 5:13 10:1 12:8 13:6 17:5 19:3,13,20	
	expressly 14:2	fastidious 33:14		
	extended 25:7	father 86:2		
	extensive 66:11	fbi 19:2 33:15 50:13		
	extent 50:14 80:20 92:15 93:15 94:6 106:13,20	feasibility 70:22 71:5		
	extraordinarily 22:12			flat 52:3 flexible 54:15

flight 58:8	101:5 109:15	27:9	23:8	9:2,14 10:5,7
flights 57:13,16	110:20 112:3,5	franklin 3:17	george 3:20	12:5,13 13:22
flimsy 103:12	113:12	frankly 33:12	getting 52:18	17:1,16,19
flying 57:13	foreigners 49:15	89:22 90:5	68:10 73:14	18:5 19:13,14
focus 5:10 6:13	50:5	free 39:12	83:21 88:17	21:8,10,20
14:17 16:22	forever 74:19	freely 39:5	give 15:8,10,16	23:3 24:10,15
23:14 37:18	112:4	frequently	17:16 51:10	25:8,17 26:9
38:2 49:17	forget 103:5	56:13	66:3 89:12	26:12 27:14
50:3	forgot 103:13	front 15:13	106:3 123:10	28:17,19 29:1
focused 23:1	form 40:14 53:5	frontier 58:19	given 86:19 89:6	29:14,21 30:18
45:12,16,18	89:8,8,11	frontiers 58:19	89:9 95:9 96:8	31:1 32:8
59:2 64:13	former 16:10	frustration 47:4	118:10	39:18 40:4,9
71:11 82:18	35:2 63:19	48:1	giving 28:9 42:7	41:4,12 42:3
94:3,19 95:3	64:3 80:1	fuller 32:20	68:14 122:17	42:12 43:16
109:10,21	120:22 121:10	fully 53:17 97:4	global 29:9	45:5 47:7
110:6,16	formerly 2:11	function 34:14	go 57:7 61:15	48:13 49:1
focuses 43:11	2:15,17 3:14	99:4 102:5	62:13 73:10	50:11,18 51:2
focusing 15:2	3:16	fundamentally	80:17 83:13	55:10 59:17,19
52:14	formula 52:7	30:12,16 50:17	104:19 107:11	61:5 67:4 68:9
folks 56:18	forth 93:7	102:16	108:6 114:21	69:15,21 70:3
119:1	forums 52:10	further 26:8	117:18,19	70:10 71:8,9
follow 19:14	forward 28:5	60:20 124:9	goes 65:9 92:7	72:15 73:4,9
36:11	44:1 120:2	future 80:14	93:6	74:3 75:8,14
following 45:5	121:9	81:7	going 11:7 16:22	75:16 77:2
68:7 118:4	foster 5:14		18:17 23:14	79:17 81:2
followon 57:10	fought 23:9	G	44:3,8 46:18	84:13 86:11,18
follows 7:12	found 18:20	gathered 49:19	49:18 53:11	88:12 89:7
followup 6:18	26:1,3 39:18	gathering	64:12,18 65:11	92:21 96:4,9
11:15 59:2	40:4 101:11	110:20	68:5,11 69:21	96:11 97:3,12
70:16 121:14	103:15	gee 63:20 64:17	70:5,6 74:9	98:1 100:18
122:7	four 54:5	general 12:10	78:2,10,15	106:20 111:2,5
force 64:8	fourteen 17:7	15:12 19:21	80:17 91:5,18	112:1,2,7,16
foreign 1:7 2:16	52:4	24:4,8 40:21	96:9 98:7	112:18 114:20
8:5,22 10:22	fourth 21:5,9,19	45:20 67:14	108:5 116:4	117:6,9 120:22
11:21 12:2,12	24:5,14 25:1	85:4 87:10	117:22 123:12	121:10
12:16 13:8	27:10 41:17	93:10 98:21	goitein 3:18	governmental
14:3 16:11	43:14 66:15	generally 67:11	good 4:2 14:21	87:21
18:6 29:2	75:9,13,19	112:14	34:8 37:14	governments
35:17 38:22	78:3 92:15	generate 25:8	65:10 97:17	9:4,7 11:20
39:16 40:19	98:1 108:1,4	77:5	107:3,4 122:5	13:15 27:17
42:4 43:11	109:22 110:1	generated 19:16	gov 7:6,9	29:7 38:8 39:5
46:6,11 48:14	111:4 112:18	generating	govern 74:16	53:11 65:2
52:14,20 93:21	113:6,9,11,15	39:19	government	99:22 101:2
94:20 95:3	fraction 19:9	generations	7:14,17 8:9,20	106:1 114:10

governs 67:10	94:10 110:5	38:13	idea 31:20 34:2	implementation
gps 9:22 45:2	happened 31:7	history 31:10	60:9 97:7	4:18 42:20
grand 21:15,17	36:2 89:10	32:4 42:22	104:8,9 105:11	implemented
57:6,11 58:7	118:7	49:9,11 84:21	106:6 120:9,18	26:12 118:10
65:1,7,8,15,20	happening	84:22 108:6	identification	implicates 111:4
81:16 84:16,18	60:17 104:1	122:8	13:7	implications
grandfather	happens 53:5,9	hit 108:20	identifiers 11:10	15:4 52:11
86:2	74:1	hmm 34:21	identify 8:3 9:7	98:8 99:22
granted 118:9	happy 87:19	hold 90:16	11:2	importance 14:4
granular 120:6	hard 106:17	holder 88:13	identifying 41:1	49:8 80:3
grappled 109:6	harm 14:6	homeland 2:18	100:19	important 5:5
great 36:17 63:8	harms 32:3	16:15	identity 9:18	21:5 29:12
89:14 95:6	hasnt 75:6 89:10	homes 76:5,9,10	ignore 30:10	37:16 42:7
115:6,9 121:7	havent 81:7	homework	ii 3:1	46:4 48:12
greater 106:14	107:1	117:22 119:12	iii 3:12 46:15	49:13,16 54:9
greatest 6:20	haystack 11:13	121:15	53:7,10 92:4	72:13 99:1,10
43:13	11:14 55:16	hon 2:15	100:14 101:4,6	101:20 105:5
green 15:13	59:5	honestly 107:7	102:17 104:21	109:14 110:17
greg 3:19	haystacks 58:3	honored 70:12	105:20 117:1	120:15
grist 68:14	58:4	hope 7:4 23:15	ill 15:9 68:22	importantly
ground 5:20	head 16:1,16	28:12 68:21	73:18 78:11	54:7 103:4
35:19	hear 30:6 34:17	hopefully 119:1	79:17 86:22	impose 116:11
group 91:8	34:20 37:1	hostile 13:9	87:1 92:13	116:13 118:15
groups 52:11	heard 63:19	hotel 1:16	117:17 119:19	imposed 40:1
growing 90:14	101:10 119:13	hour 123:13	120:14	78:21 118:11
guantanamo	hearing 65:13	hours 40:11	illustrated 49:8	imposing 39:9
91:9	93:11	house 2:18	im 11:19 14:22	impressed 33:13
guess 63:16	hearings 66:21	105:3	16:22 23:14	improve 121:13
64:21 79:2	hears 35:10	housed 70:1	38:1 46:18,20	improvements
108:5 119:21	held 1:15 4:3	71:7,8	53:9 54:21	121:3
121:15	24:21 30:20	houses 42:18	58:13 68:5,14	inaccurate 32:7
gun 78:6	75:13 76:13	huge 108:20	78:10,15 80:17	inadvertent
guys 51:10	99:2	hundred 121:18	87:16 90:17	111:17,21
<hr/>	help 106:13	hypothetical	91:18,20,22	inappropriate
H	helped 80:7	58:7	95:13 97:21	120:4
<hr/>	121:11	<hr/>	98:2 101:12	incident 61:19
half 79:18	hes 52:18	I	102:4 108:5	incidental 52:19
hand 124:12	highly 111:17	id 23:10 37:15	imagine 74:13	53:15 111:17
handled 8:12	hill 40:12 52:5	37:18 38:2,17	93:13	111:21
92:3	hindered 88:14	51:21 53:19	immense 27:8	include 47:17
handling 41:9	116:21	55:19 63:16	imminent 14:5	includes 17:12
hands 67:7	hint 84:21	64:21 65:22	impact 75:21	18:17 83:21
73:17 77:21	hired 97:11	81:17 104:8	122:19,20	including 14:10
happen 52:16	historical 18:18	115:11 123:1	impeding 14:12	40:10 49:20
65:17 74:2				

77:13 88:1 121:11 incomplete 32:6 incorporated 57:21 increase 29:8 increases 29:1 increasingly 40:5 incumbent 119:20,22 independent 3:7 4:9 106:1 indicate 23:20 26:22 116:9 indicates 14:5 indication 60:20 indicted 112:11 indictment 65:9 indifferent 27:16 122:6 indiscriminate 26:13 individual 18:4 21:1 35:14 41:6 45:3,5,6,8 45:16,18 47:1 56:7 59:6 87:14 individualized 19:5 21:7 42:2 42:5 94:19 100:16 108:18 110:10 individuals 13:11 24:22 25:7 48:10 industries 56:16 inevitably 6:1 107:19 influence 64:10 influenced 30:4 information 3:5 5:22 6:3,6,11	7:13,21 8:10 8:12 9:5,21,22 10:5,8,16 11:21 12:7,12 12:21 13:16,17 14:1,3,10 17:11,17,18 19:2 21:21 22:1 26:10 27:8,11,15,18 32:7 41:10 49:19 50:11,17 50:19 53:22 54:1 56:22 62:16 70:7 71:13 72:17,18 73:2,6,8,11,14 74:19 75:8,14 75:16 77:5 83:5,9,15 95:18 96:13,18 97:18 102:11 106:9,11 108:2 112:3,4,5 114:19 118:2 informed 30:13 32:7 infringed 25:4 ingredients 87:11 inherent 67:22 68:3 inherently 81:22 initial 76:22 87:7 initially 64:11 101:8 inject 97:7 input 11:3 inquiry 21:14 inside 18:21 41:22 49:20 75:8 109:17 114:9 116:6	insight 14:9 inspectors 19:21 installation 26:18 instance 96:2 institution 91:4 institutional 37:9 90:19 91:14 instructive 24:20 insufficient 113:1,2 integrity 34:2 intelligence 1:8 2:16 3:10,14 8:5,22 9:3,20 11:21 12:2,11 12:12,16 13:8 14:4,7 16:11 19:22 29:3 35:17 36:18 39:12 42:18 46:6,11,17 47:16,18 48:7 67:10 72:21 74:15,20 93:21 94:11 95:11 106:11 110:20 112:4,5 113:12 intend 63:20 intended 39:22 95:2 113:19 115:14 intent 41:20 79:1 117:9 122:15 intentionally 13:3,4 intentions 8:9 interest 18:22 62:15 72:16 88:19 interested 54:22	55:20 112:1 124:11 interests 88:5 110:7 internal 87:21 internally 93:9 international 37:2,8 47:11 48:20 108:9,16 internet 23:21 25:15 31:18 38:8,14 60:13 61:13 interpretation 65:3 86:17 interpreted 7:15 81:1 intricacies 52:6 intriguing 106:7 introduce 4:5 15:9 introduced 36:5 intrusive 66:22 67:6,11 69:5,9 76:21 77:1 intrusiveness 69:8 invade 110:8 invading 24:17 investigation 20:10 21:2 26:8,19 55:7 57:19 82:15 122:12,16,19 investigations 11:15 20:12,16 investigative 56:15 79:4 80:13 105:9 investigatory 70:7 invitation 22:20 inviting 28:4,8 37:16	involve 46:14 94:8 involved 9:19 16:5 33:16 45:4 56:19 88:6 involvement 93:19,22 103:1 109:19 involves 11:20 involving 45:15 108:2 irrelevant 112:19 113:6 isnt 24:15 27:16 59:14 60:3 67:15 issue 21:11 25:14 35:8 40:8 50:8,20 78:11 102:1 108:1 issued 10:2,11 65:8,15 102:2 issues 5:16 6:13 7:8 15:8 23:1 32:5,11 37:17 44:1 50:6 75:18,19,20 87:14 90:20 93:9 106:8 item 82:9 items 56:22 82:9 82:16 ive 20:14 32:10 64:8 65:15 <hr/> J <hr/> jaffer 2:13 16:4 22:20 47:3 58:1 59:9 72:11 84:5 97:16 111:2 jameel 2:13 16:4
---	--	---	---	--

22:19 31:1	judgments	106:5	101:18 103:17	lawyer 96:8
44:11,12 47:2	101:1	keeps 77:22	105:16,21	lawyers 91:10
49:12 51:5	judicial 34:14	103:19	106:19,22	layer 96:4
75:15 76:21	39:3 87:8,8	ken 16:13 37:13	108:8,21	leaders 20:3
78:13,15 83:17	92:14,18 99:3	37:21 46:5	109:14,16	99:2
123:1	119:3	49:8 51:12,20	111:11 114:3,7	leading 8:11
jameels 51:22	judiciary 19:22	86:22 104:5	114:8 115:13	leads 35:21 62:5
james 2:6,15	97:10,11	108:7 117:4	116:19 117:15	leadup 116:12
3:14 16:10	july 1:10	120:14,16	117:16 121:5	leak 13:20 104:4
janosek 5:8	juries 21:15	kenneth 2:17	knowing 116:3	leaked 6:2 10:3
15:12 123:9	57:6	kept 13:21	knowledge 12:9	81:5 82:4
jim 4:6 50:22	jurisdiction	19:11	43:15 124:8	leaks 8:14 31:13
87:4,12 88:1	91:21 99:20,21	key 62:2	known 4:8 13:5	51:15 103:16
117:16 119:8	100:1,8 101:15	kidding 91:2	30:19 82:18	learn 25:17
123:4	jurisprudence	kind 23:3 37:9	117:8	learned 31:12
jims 68:8	37:5	46:14 53:16	knows 28:18,19	34:15 79:15
john 85:4	jury 21:17 57:11	55:15 59:21	47:20 81:21	80:3
jones 24:20 26:2	58:7 65:1,7,8	60:4 66:12	115:7	leave 44:14 72:4
26:4,7 45:1	65:15,20 81:16	70:19 71:2,12		78:11
51:5 66:7 69:2	84:16,18	73:5 75:3	L	leaving 39:11
journal 102:13	justice 3:18 16:2	76:19 80:16	lab 3:10	87:20
judge 16:11	16:17 25:6	87:18 88:3	labeled 32:15	led 24:5 46:12
22:9 33:1	33:14 99:14	98:3 102:17	lack 101:11	94:2 109:3
34:16,17 35:6	justices 25:2,3	103:7 116:14	language 59:15	left 68:5
35:6 37:13	66:8	kinds 61:10,14	81:8 82:3,5	legal 2:10,11
44:9 45:22	justification	62:5 68:1,3	large 10:13	3:16 5:8,15
62:10 69:4	7:22	101:6	47:10 77:3	6:13 7:21
86:12 92:18	K	knew 80:8	larger 48:6	14:17 16:2,4
93:1,5 94:15	kate 2:14 16:8	knit 51:11	112:13	20:20 29:15
99:7 101:9,19	28:7 45:22	know 30:1,6	late 36:3	63:13 89:13
101:22 104:8	49:6 53:20	31:16,18 32:16	latitude 43:13	93:15 97:22
104:15,20	67:19 88:22	33:22 47:22	law 3:20 12:13	98:7 102:14,15
119:15 121:18	104:5 106:18	48:2 53:20	12:19 13:2	103:1,12
judgement	107:15 115:12	58:2,12 59:20	15:22 29:19	106:21
111:7	116:2 117:3	60:15 63:4,4,9	30:11,18 31:16	legality 15:3
judges 17:5,8	118:5	63:18,20 64:1	31:20 34:15	38:7 59:3
34:4,15 35:19	kates 64:22	70:8 73:10	36:15 46:1	legislation 43:1
36:13,13 93:8	keep 6:6,19	74:9 75:5 76:3	61:16 76:16	78:18,20 79:1
99:16 101:6	54:17 99:10	78:13 84:9,11	90:3,13 102:4	80:5 95:7
102:2 104:19	104:13,15	85:8,13,18	102:6,19 106:4	legislative 43:20
105:15,15,20	105:6 116:10	88:6,18 90:15	lawful 22:16	80:5 84:20,22
105:21 106:10	118:2	90:22 91:6,16	26:17 79:3	122:8
119:4	keeping 69:18	92:5 95:15	112:20	legitimate 87:13
judging 35:1		96:5 99:6,8,14	laws 4:19 48:8	length 9:13

54:16	120:19 121:5	58:20 89:15	75:5 76:15	106:18 108:7
level 7:11	123:2	mail 7:10	matters 30:16	115:4,12,18
levels 42:11	lives 27:18	maintain 71:18	mayflower 1:15	116:7 123:1,7
43:17	29:22	83:14	mean 48:15 58:9	mere 60:14
liberties 1:3 4:4	livingston 1:22	maintained 69:6	62:22 68:1	merely 7:16
4:16 22:18	124:3,16	maintaining	71:2 88:10	27:15
23:8 29:6	located 12:15	43:3 71:14	95:17 96:2,3	met 41:3
32:13 119:20	13:13 42:10	79:5	113:5	metadata 8:21
119:22 121:8	50:2 113:20	maintains 57:2	meaning 21:9	9:9 10:14,19
liberty 4:17 33:4	location 9:21	major 117:1	meaningful	11:4,12,16
lichtblau 90:1	24:22 26:1,7	majority 11:7	42:13 54:9	17:1,10 18:17
lichtblaus 90:3	26:10 66:11	66:8 89:2	means 34:8	20:11,18 21:21
life 29:11 49:22	long 10:10 66:13	making 5:9 9:11	72:12 73:13	22:10 23:18,21
66:14 79:18	69:15 107:5	23:21 28:13	115:8	24:10,11,16
lifetime 31:7	longer 103:14	80:4 96:19	meant 26:7	25:16,21 27:7
light 65:5,16	longterm 24:21	100:17,22	30:22 84:13	31:15,18 44:16
82:2	25:21 26:1	101:1	113:8	44:19,21 45:7
limit 9:6 31:4	look 28:5 44:1	man 53:12	measures 106:3	45:20 49:20
41:9 60:2	53:7 54:4	mandates 19:20	media 6:2	51:7 60:11,13
85:11 101:20	74:10 80:22	manifests 57:13	medical 25:14	61:12,17 66:12
limitations 10:7	84:20 105:15	58:8	medine 2:3 4:2	67:21 68:1
22:13 82:3	106:16 114:16	manner 22:16	107:14 113:3	71:17 84:3
99:11,17	looked 122:3	manpower	117:3 119:2	98:2,9
limited 11:4	looking 49:9	39:19	123:12	methods 36:21
17:21 61:2	77:11,13,15	mantra 121:21	meet 75:9 77:14	mic 37:21
110:18	83:15 102:18	map 28:3	108:4	michael 3:16
limits 67:22	118:6 121:9	marc 3:5	meeting 4:3	migrated 108:13
68:3 85:7	lot 56:18 65:15	martin 2:14	40:12 51:15,19	military 64:8
100:7	68:14,20 71:3	16:8 28:8 49:7	meetings 52:10	mill 68:15
line 41:19 59:4,7	82:11 98:16	60:5 63:4 75:4	member 33:3,4	millions 26:14
59:10 120:3	106:8	78:8 86:10	members 2:1	61:6
link 20:13	lots 57:20 94:2	101:18 113:14	4:6 6:16,18 7:1	mind 6:7 56:8
list 18:13	95:18	117:4	14:18,22 20:3	78:1 99:10
listen 17:19	love 63:9	maryland 26:18	20:5 40:12	104:13,15
listened 105:4	lower 45:17	45:14 124:4	42:21 48:6	105:6 106:5
litigating 55:22	47:8	mason 3:20	56:7 63:19,19	116:10
63:3	lunch 6:16	mass 14:13	64:3,12 74:13	mine 105:8
litigation 56:18	123:13	44:18	78:4 85:20	minimization
56:19,20 57:1	lynne 1:22 124:3	massive 24:2	95:9,11 97:15	13:19 41:8,14
82:14	124:16	29:21 31:14,17	103:21 107:12	49:3 101:3
litt 93:10		74:18 75:17	memos 93:9	108:3 111:9,12
little 54:14,15	M	materials 57:8	mentioned 19:7	111:14,16
66:1,6 86:7	m 1:17	82:13	32:18 49:12	112:2 113:1
108:6 115:13	magnitude	matter 30:15	63:18 104:14	115:5,6 121:17

122:3	69:12	78:19 90:6	45:9 61:3 83:6	officer 5:7,8
minimize 19:15	multipoint	neither 27:19	83:9 93:4 96:7	97:2
mining 18:1	118:7	net 27:4	119:15	officers 18:12
minute 45:21	mustnt 103:5	network 83:7	numbers 11:17	offices 76:6,9,10
minutes 15:10	N	networks 14:9	17:13,14 18:4	official 28:20
15:16,19 34:13	naked 28:20	never 11:7 61:5	18:14,15,21	officials 7:18
44:5 54:17	name 12:5	65:16 76:9	19:16 20:14	40:10 48:6
69:1	narrow 9:6 74:5	86:4 98:19	26:21 33:18	114:17 120:22
misleading	101:12 112:12	new 7:15 23:7	numerous 40:9	121:11
111:18	narrower 26:4	36:5 40:17,18	52:13	oh 71:22
misled 48:7 52:1	nathan 3:20	58:18,19 101:9	nw 1:16	okay 37:14
misnomer 12:3	nation 4:14,20	102:13 103:14	O	54:11 65:22
missions 4:12	national 2:14,17	104:17	object 61:22	67:21 87:3
misspoke 113:5	12:11 16:9,16	news 17:22	63:15	89:17 104:5,7
misunderstan...	29:5 36:20	23:20	objected 76:7	108:19 117:19
121:19	43:12 69:18	nojeim 3:19	objection 32:14	once 10:13
misuse 80:14,16	70:7 72:16,19	nonu 12:14 42:9	63:14	36:15
misused 79:7	93:16 94:7	45:12 52:20	objections 62:6	ongoing 55:6
mit 3:9	96:17 105:9	94:22 107:18	objective 39:8	81:2,22 82:13
mitigate 14:14	nationals 48:14	109:8 110:3	observation	84:14,18 85:14
model 93:4	naturally 57:19	norm 34:19	119:11,12	online 121:22
97:13	near 58:10	105:13	observed 25:6	122:2
moderate 6:16	necessary 14:3	notarial 124:12	obtain 9:2 12:20	open 51:17 55:1
14:19	28:14 70:21	notary 124:3,17	13:6 75:8,16	87:4
moderating	87:8 92:19	note 23:22 32:10	113:19 117:7	opening 15:10
15:2	necessity 70:20	noted 28:17	117:11	16:22 56:5
modern 51:6	need 4:15,16	notice 76:14	obtained 12:8	87:6 115:4
moment 15:9	11:14 20:17	notify 98:6	81:15 82:21	operated 1:6
38:17	23:6 31:22	notion 79:3	obtaining 12:17	operation 41:19
moments 104:14	36:19 39:3,5	102:22 104:15	obvious 60:3	operational 41:5
monitored 37:4	42:5 43:2 51:4	116:17	72:12	43:2
43:17	51:16 54:18	nra 78:4,5	obviously	opinion 31:14
month 26:11	62:17 70:8	nsa 18:12 19:12	116:22	66:9 90:11
60:8	79:14 93:19	23:17,20 27:8	occurred 18:16	93:1
months 40:9	96:22 102:16	33:15 36:3	21:17 86:4	opinions 30:7
52:4	114:2,21	44:13 47:10,15	93:22	66:7 79:12
morning 4:2	needed 108:21	48:19 49:14,18	occurring 83:4	89:3,9 90:9
14:21 37:14	needle 11:13	50:12 73:18	offered 20:5	93:5 100:4
moved 118:1	needs 32:2	115:20	27:6	102:14,15
movements 25:7	34:17 37:6	nsas 19:6	offering 121:12	107:1,3 119:1
28:1	40:6 50:21	nuclear 13:10	office 2:11 3:14	opponent 90:19
moving 48:1	55:11 59:6	number 9:11,11	16:1 79:22	opponents 31:3
120:1	69:16 75:9	10:21 18:6,8	91:15,15 97:10	opportunity
multiple 43:17		18:14 19:4		16:21 20:6

28:9,11 43:22 73:18 95:9	outlined 31:1	15:14,18 44:5	74:22 85:21	26:15 33:15
oppose 97:11	output 11:3	54:12 58:14	87:18 92:16	34:1 43:20
opposed 87:14	outside 12:16,20	59:2 78:12	95:16 96:10,13	48:18 50:2,7
optic 108:13	13:13 39:20	92:10 97:14	104:11	53:18 57:15
options 31:4	41:7 42:10	107:12 117:15	particularized	60:6,9 64:17
order 6:4 8:22	45:13 48:14,18	118:21,22	76:6,7 92:17	71:16 72:21
10:2,3,3,6	94:22 107:18	123:8	110:1 120:12	76:10 80:8
11:18 12:20	109:1,9,21	panelist 15:15	particularly	84:5 88:5,10
13:6 15:22	110:4	panelists 5:2	40:3 54:22	91:8 103:13
17:3,8,16,22	overarching	6:19 15:17,21	109:10	105:22 116:5
19:3,19 20:17	28:12	32:18 44:7	parties 57:2	117:11 120:15
21:7 22:10	overlapping	123:6	124:10	peoples 75:21
30:17 35:21	86:20	panels 6:12	partner 15:22	percent 121:18
42:2 45:11	overreach 29:2	papers 93:14	16:13	perfect 121:1
55:5 60:4	overriding	paradigm 105:5	party 56:20	perfectly 65:19
62:13,14,15	72:16	117:2	62:14 83:6,9	period 25:7
67:9 69:7 75:7	overseas 39:6,12	paradox 36:17	104:10	26:11,15 27:3
81:5 82:4,17	42:4 49:15	parallels 105:10	pass 55:3 86:22	57:14 58:9
82:22 83:11,19	50:2,5 52:14	parameters	91:18,21 95:8	61:2 66:13
86:14 88:11	52:16,20,22	74:15,16 98:21	passage 43:21	90:10
89:8 103:8	115:21 116:3,5	paranoid 47:13	64:6	periodic 19:21
116:22 117:7	116:16 117:10	48:3 49:2	passed 36:4	permanent
117:10	117:13	part 19:2 48:5	38:16 39:16	12:15 77:20
orders 8:5,6	overseen 19:15	51:19 60:17	40:15 43:10	78:6 97:1
10:2,11 24:8	54:6	72:10 87:4	64:11,17 95:7	permit 6:20
35:16,17 46:3	oversight 1:3	89:19,22 91:11	passengers	13:2 31:21
58:20 61:1,3,6	4:4,22 19:19	92:7,9,11	57:13	116:1
82:12 88:17	42:13,14 43:18	97:10 111:9	passing 55:15	permits 12:13
89:9 94:19	46:16,17 54:3	119:21	87:13	20:8 82:5
108:18 110:11	54:5,8 79:16	parte 34:7 35:9	pat 4:6 14:19	permitted 10:18
ordinary 59:16	79:17 80:4,8	88:4,4 92:21	15:17 54:11	18:2 78:8
84:10 105:13	80:15 87:20	102:8 104:22	patricia 2:5 15:1	100:14
organization	99:9 103:19,21	105:11	patriot 1:7 5:12	person 12:14
18:7 64:11	overview 87:10	participate 5:3	8:16	13:4,4,16
organizations	overwhelmed	16:21 22:21	pattern 48:5	41:21,22 44:5
10:22 14:11	94:19	28:5,9	pay 51:4 70:2	52:2,20,20,21
organized 64:14	ownership 78:6	participating	pclob 4:8,21	104:10 105:2,3
original 41:19		97:4	5:16 7:19 37:8	110:3,7 114:5
43:4 79:1,1	P	participation	91:4,4	114:12 115:15
88:16	paces 106:2	95:13	pclobs 7:5	116:15
origins 105:10	page 116:2	particular 10:21	pen 26:18,20	personal 25:14
outcome 124:11	panel 2:9 3:1,12	11:17 45:2,3,6	81:19,21 83:2	29:22 66:14
outer 85:6,11	6:15,17 14:16	55:12,17 56:22	83:6 86:20	persons 9:19
	14:19 15:2,6,7	57:14 58:9	people 25:19	13:1,13 14:2

25:17 26:10	100:14 121:1	potential 108:22	prevention 13:9	19:14 41:5,8
39:11,20 41:11	121:12 122:5	109:17	prevents 117:6	41:14 42:14
42:9 45:12	playing 100:12	potentially	previously	49:3 101:3
53:4 62:15,16	plot 116:9	21:16 57:4,8	16:15	108:3 109:20
66:14 94:22	plots 8:4	power 23:4	primarily 33:8	111:9,12,15,16
107:18,20	pocket 106:1	28:18,20	64:13	112:2,7,17
108:2 109:8	point 35:13,20	powers 38:22	primary 4:12	113:1 122:3
perspective 2:10	51:12 53:19	practical 71:5	primitive 26:21	proceeding
3:13	64:21,22 72:11	106:8,16	45:15	63:13 88:7
perspectives	73:3 74:22	practicalities	principally	proceedings 4:1
14:18	78:17 85:8	114:15	23:14	124:6,7
phase 44:4	101:12,12	practice 11:4	principle 67:14	process 34:2,7
phenomenon	105:14 106:19	preceded 66:9	prior 42:17	35:4,6,10,11
64:20	115:12 119:3	precedent 90:14	94:18 108:8	35:13 36:4,16
phone 9:21	pointed 73:4,9	91:13	prism 12:3,4	36:18 37:6
17:11,13,20	points 34:6	precise 25:9	38:6 43:7	38:21 39:4,14
18:4 20:14	44:10 48:12	precisely 25:18	privacy 1:3 3:5	40:1,18,18,21
22:2 23:18	51:2 63:17	preferred 79:22	4:3,16 22:17	41:18 43:21
60:11	83:1 104:13	prepare 93:14	24:17 25:5	65:8 95:2 97:5
phrase 118:18	106:5	prescribed	28:17 43:3	97:19 99:3
phrasing 115:13	police 27:4	42:15 54:4	48:10 52:11	106:15 119:18
pick 46:22	policies 4:19	presence 19:1	74:7,9 94:22	120:16,18
picking 83:5	policy 3:13,15	present 62:2	110:7 113:2	production 81:2
piece 43:1	5:16 6:14 15:4	presented 37:11	private 22:5	81:9,14 82:11
pizza 53:12,13	23:2 36:13,14	preserved 71:10	49:22 70:1	82:13 84:14,19
place 24:6 25:13	political 25:10	preserving 29:7	probable 11:18	85:9,14,16
26:5 38:11,20	25:15 29:22	president 5:17	19:5 59:22	professional
42:15 48:9,10	31:2,3,4 99:1	24:9 46:7,9	92:17 95:19	25:11
49:5 70:10	portion 11:5	60:18 109:13	100:18 105:17	profitably 115:9
72:17 74:8	pose 6:17	presidents 109:3	110:12,14	program 5:11
75:11 78:18	118:21	110:22	114:22	5:13 8:7,19
79:4 87:17	poses 77:12	press 30:14	probably 32:12	9:17 10:1,12
97:20 98:20	position 6:9	103:16	33:3 80:2 97:2	10:19 11:4,11
99:2 108:3	9:14 47:18	pressing 72:21	101:20	11:19 12:4
111:4 113:18	50:19 121:6	pressure 74:13	problem 40:3	14:8 17:1,2
placed 22:13	possibility 61:15	presumably	50:18 73:15	20:4,19 22:15
83:10	62:8 85:1,17	31:19 116:17	78:3,3,4 90:22	23:15,17 24:2
plaintiffs 37:2	possible 5:9	pretty 60:8	102:8 108:20	26:13,17 27:7
101:10	6:20 8:4,8 51:7	86:10	problematic	38:6 43:7,10
plan 61:19	59:10 67:18	prevail 74:21	101:17	44:4 47:14
planning 14:11	77:3,4 122:15	prevent 8:4	problems 75:2	58:10 60:18
109:17	possibly 68:7	30:17,22 80:16	procedure 52:6	63:11 67:5,20
plans 14:10	104:9	preventing	procedures	71:1 87:9
play 97:19	posted 7:4	54:10	13:11,15,19	89:14,15 98:22

107:15,17 119:6 120:4 programmatic 34:11 46:2 68:10 87:13 94:17 101:2 118:13,18 programs 1:5 5:5,11,16,18 7:2,13,16,21 8:2,13,15 14:18 16:7 22:22 23:11 31:11 32:14 33:7 36:7 49:9 54:6 59:3 66:3 95:11 98:16,17 99:2 107:5 120:20,21 121:12 prohibited 14:2 prohibits 12:19 12:22 project 3:17 33:5 115:3 120:10 proliferation 13:10 14:12 promise 89:6 102:10 promote 6:4 properly 98:15 proposal 98:8 proposals 114:16 proposed 99:22 100:20,20 proposition 86:7 prosecute 96:12 prosecuted 91:11 prosecution 35:22 96:10	prosecutor 104:21 105:1 protect 4:14,16 4:20 23:9 36:20 48:10 113:2 116:14 protected 18:10 protecting 72:18 protections 39:6 43:3 68:11 70:12 protective 22:12 prove 37:2 provide 5:17 29:5 40:22 80:20 81:6 118:2 provided 14:9 40:14 58:6 provider 12:9 providers 10:4 11:22 67:8 provides 41:20 119:3 provision 9:1 81:12,19 82:3 85:21 86:3 115:17 117:6 118:16 provisions 103:11 proviso 81:13 public 4:3 5:15 5:18 23:1 30:4 30:8,14 32:19 43:6 48:8 50:14 62:5 97:9 98:7,21 98:22 100:5 104:3 106:14 107:4,6 122:22 124:3,17 publicly 7:14 98:6	pull 37:21 purely 21:21 purports 81:4 purpose 5:14 10:9 11:1 19:12 50:4 70:22 72:3 73:21,22 76:22 110:20 115:21 117:13 purposes 9:3 12:17 13:8 17:12 22:3 24:14 46:7 65:4 69:14,17 71:14,19 83:16 85:2 86:8 pursuant 1:6 8:21 12:1 42:1 103:8 push 102:22 put 45:2,9 78:16 78:18 87:17 99:2 106:2 121:5	50:10 52:9 54:20 55:1,3 60:5 61:8 62:18 63:5,8,8 63:10,13 65:7 67:19 68:6,13 68:18,18,19 69:4,8 70:14 70:17,17 72:13 72:13,13 73:11 73:13,15 76:20 76:22 77:9,11 80:22 85:13 87:4,7,10,17 87:22 88:21 89:11,19 90:16 90:18 91:18 92:12 98:3,6 99:8 101:13,19 107:14,22 112:19,22,22 113:16 114:14 117:15,16 118:1,12 119:4 121:17 questions 6:17 6:18 8:11 15:18,20 28:6 38:6 44:2 47:1 54:12,16 72:4 75:6 76:17 79:19,21 92:6 94:16 97:22 99:13,16 102:19 103:22 104:2 107:13 quick 44:10 51:1 59:1 63:17 83:17 113:4 117:3 quickly 53:20 quint 89:19 quite 23:5 30:1 34:19 48:12	60:2 74:4 101:5 quiz 80:19 quote 20:9 25:8 quoted 33:18 quoting 28:15
R				
				rachel 2:4 4:6 14:19,22 16:20 56:4 61:9 racketeering 64:10 raise 28:11 raised 10:13 32:13 38:6 63:12 66:20 67:20 88:22 96:3 103:22 raises 24:3 75:17 88:22 94:15 107:22 random 18:1 rarely 74:4 rationale 11:11 reach 24:12 reached 25:2 reaction 122:4 read 25:18 34:20,22 35:2 61:4 84:12 85:19,21 86:12 90:1,2 reaffirmed 32:2 real 44:10 50:6 71:5 79:13 81:22 83:8 reality 53:16 really 70:14 86:6 87:12 97:1 115:7 119:13,19,21 120:6,21 121:7 121:21

reapproved 17:4	38:13 52:10 55:12,17 59:6	reingold 5:6 123:9	115:4	61:19 110:1 113:9,17
reason 38:19 69:18 114:1 122:17	69:16 88:16 122:22 123:15 124:7	reiterate 49:7	remember 21:5 110:17	116:11,13,22 118:11,15
reasonable 10:20 18:5 22:4 24:17 25:5 57:21 86:18 95:19 111:8 113:11	recorded 7:3	related 4:19 14:13 34:6 35:13 48:11 55:8 71:1	remembering 27:20	requirements 41:2 71:5 75:10
reasonableness 111:6	records 8:19 9:2 9:15 17:3 20:9 21:8,16 25:13 51:3 61:7,11 61:14 68:2,3 69:7 71:11,18 72:1 78:6 81:3 81:6,11,12 82:1,16,18,21 83:11 84:14 88:13 118:19	relatedly 55:13 55:18 81:18	remind 38:17 reminds 51:8	requires 11:18 18:11 19:13,14 22:8 29:16 59:15 77:11 83:1 92:16 110:10 111:5
reasonably 13:12 42:9 107:7 109:8 110:3	red 15:13	relating 5:16 41:10 101:3	renaissance 1:15	requiring 66:15 67:11,17
reasons 22:15 25:3,22 30:16 70:13	redacted 89:8,8	relationships 25:14	repeatedly 47:8 47:9 48:7 50:3 103:22 104:1	researcher 3:7
reauthorization 42:17 89:5	refer 12:4 59:11	relatively 58:2	replacing 93:18	resident 12:15 23:19
reauthorized 8:17 12:6 20:2 42:16	reference 6:5	relevance 20:20 54:21 55:9,11 55:16,20 56:1 56:17 57:5,7 58:2,16 59:11 59:13,21 60:1 60:3,7,10 62:20 63:1,2,8 63:12 65:4 81:20 82:12 122:9,9,12	replied 35:6 reply 104:6	resisted 35:3
rebuttal 113:3	referred 8:18 12:3	relevant 20:10 20:11 21:2,4 21:13,16 55:6 56:10,11 57:8 57:16,18 59:7 61:2 63:1,5 82:13 84:17 96:9 122:18	report 5:18 33:6 33:8 115:3 120:11	resolved 109:7
received 23:18	reflect 112:17	reliance 29:10	reported 1:22	respect 4:22 59:16 60:4 63:6,6 71:16 97:21 100:12
receives 24:1 97:6	reflected 120:10	relief 40:14	reporting 19:22	respectfully 35:8
receiving 104:16	reflections 15:16	relies 30:2,5	reports 6:3 18:1 23:20 33:19	respects 29:6 respects 22:17
recipe 79:8	reflects 25:9	religious 25:11 25:15	request 21:8 51:3 89:5 95:16	respond 44:6 86:15
recipient 62:12 62:14	refreshed 82:19	remain 6:8 78:22	requests 119:5	responding 44:10 51:22
recognized 39:2	refuse 37:1	remarks 7:17 15:11,16 16:22 37:18 38:2 56:6 87:6	require 8:4 20:22 21:6,18 21:20 59:21 61:16 67:5 81:5,14 82:12 84:14,18 85:9 85:14	response 61:8 117:3
recognizes 44:21	regard 60:7 67:3 111:1	reliance 29:10	required 41:16 76:15,15 92:14 96:20 108:18	responses 6:20 54:16
recommendat... 119:14	regarding 1:5 7:20 38:5	religion 25:11	requirement 39:10 40:2	responsive 11:7 15:16
recommendat... 5:19 28:14 115:3 120:1	register 26:19 26:20	religious 25:11		rest 92:10
recommended 4:10	registers 83:2,6	religion 25:11		restraints 62:6
record 21:1 25:9	regulate 56:16	religion 25:11		restrictions 112:10
	regulation 4:19	religion 25:11		restrictive 22:7 72:12 73:13
	regulations 7:6 7:9 50:12,15 50:16	religion 25:11		

77:19	112:21 114:8	39:11 41:10,21	search 21:6,9	81:13 85:7
result 11:15	122:1	42:9,10 45:12	24:22 25:22	86:11 100:13
103:16 104:3	rightly 48:13	45:13 52:2,20	26:2 35:16,21	122:8
resulted 43:21	116:16	53:4 66:6	51:3 66:15	sections 81:18
resulting 31:11	rights 28:21	94:22 107:18	76:14,19	secure 42:5
resume 31:21	75:22	107:20 108:2	104:17,20	94:13
123:13	ripens 65:8	108:14,16	120:12,12,12	security 2:14,17
ret 2:15	rise 29:19 46:1	109:2,8 110:3	searched 57:3	2:18 16:9,15
retain 17:12	risk 117:22	110:6,7 115:15	76:11 105:3	16:16 33:4
69:15,17 112:3	road 28:3 79:7	116:14	searches 76:5,8	36:19,20 43:12
112:8	robertson 2:15	safeguard 32:3	searching 11:10	69:18 70:7
retained 10:10	16:10 33:1,2	safeguards 48:9	second 6:13	72:16,19 93:16
return 18:13	45:22 51:1	74:8,9 80:15	11:19 35:12	94:7 96:1,5,17
23:16 118:11	62:10 63:7	sales 3:20	44:4 53:19	105:9
118:15	77:18 86:22	sam 28:16	64:21 78:4,11	see 33:12 47:15
reveal 25:14	89:18,21 92:9	sanitized 107:2	87:1 120:11	48:3 65:5,16
revealed 60:19	93:5 94:15	satellite 108:11	secondly 30:22	71:6 79:12
76:10	99:7 102:1	satisfied 21:3	34:10 51:12	89:7,7 98:5
revealing 25:16	104:20 115:2	satisfies 74:7	62:8 122:7	105:7 106:10
49:21 61:11,13	121:18	save 68:6 72:9	secrecy 28:22	106:10 121:16
reveals 38:13	robertsons	saw 64:7	29:4 36:19	122:22 123:2
66:13	119:15	saying 7:15	46:1	seeing 43:7,8
revelation 31:10	robust 6:4	63:20 64:17	secret 29:14,15	seek 19:3
revelations 36:2	role 3:2 4:22	86:4	29:19,20,21	seeks 21:20
reverse 12:22	36:5 37:9 42:7	says 56:10 75:15	31:14,16 46:1	seen 64:8 77:8
115:18 117:5	46:2 87:13	107:11 115:17	49:18 50:12	107:1
reversed 90:12	97:19 100:11	121:6	53:22 76:3,5,8	segments 66:5
review 3:15 4:13	100:13 101:21	scale 38:11	88:15 89:3	segregate 70:11
36:13 38:12	120:22 121:12	47:10 58:17	98:19 102:7	segregated
39:3 41:14	rotenberg 3:5	scaling 80:12	103:10	19:11
46:15 87:8,18	round 72:9	scheduled	secrets 28:19	seize 67:4,5 75:8
90:12 92:14,18	roving 118:7	107:11	section 1:6,7	seizure 76:19
109:20 119:3,5	row 15:13	school 3:20	5:11,12 8:16	113:17,18
reviewable 36:1	rubber 33:17	science 3:4,9	11:20 12:1,6	seizures 75:14
reviewed 11:6	rule 53:8	scope 9:6 48:8	12:22 17:3	76:2
17:4 19:10	rules 5:20 36:10	58:10 77:13	20:2,8,21 22:6	senate 3:16
63:10 90:12	running 78:1	scrambling	24:7 25:13	senator 28:15
rico 64:11	79:19	93:12	26:6,13,16,17	66:21
right 14:20	<hr/>	screen 9:7	28:15 37:19	sense 66:12
34:21 56:20	S	scrupulous	38:3 40:17	105:7
62:17 74:3,8	s 11:17 12:14	33:14	47:12 54:21	sensibrenner
79:10 81:20	13:1,3,4,12,16	scrutinize	55:5,15 60:9	86:1
96:7 104:6	14:1 16:10,17	105:16	61:1 62:11	sensitive 27:18
106:7 109:12	18:8 19:1,4,16	seal 124:12	80:22 81:1,8	74:19 96:16,17

96:22 106:11	sifting 18:1	10:16 77:4	sphere 110:9	116:1,6 117:12
sensitivity 106:9	signature 93:8	sorry 38:1 90:2	spite 59:14	statute 38:16
sent 33:20	signed 33:7	sort 48:1 54:13	spoken 86:3	39:9 43:4,7
separate 19:3	significant	55:7 65:18	spring 40:8	47:20,21 57:22
20:22 69:18	39:18 42:12	70:19 81:22	staff 40:12	60:22 64:4,6
72:2,2	45:19 74:12	85:10 89:6	stamp 33:17	64:18 80:18
september 33:6	76:2 94:16	90:18 97:8	stand 28:20 33:8	82:8 83:1
sequence 65:17	signs 93:1	106:6 121:14	standard 20:20	84:12,13,21
series 15:18	similar 20:6	sotomayor 25:6	20:21 21:3	85:1,19 86:7
103:11	similarly 57:17	sought 39:8	54:21 58:3,17	87:10 91:3,22
serious 14:6	103:18	62:16 122:11	59:13,16 61:9	92:2 96:21
29:17 75:17	simply 18:13	122:16	62:21 81:21	100:2 103:6
113:16	27:11 45:15	sound 71:3	82:12	107:8 111:8,20
serve 28:2	sincere 102:11	sounds 34:21	standards 20:8	112:15,20
served 16:11,14	single 27:2	sources 36:21	74:21 106:4,4	122:10,11
62:4	sit 17:5 33:10	southern 101:9	standing 37:4	statutes 21:11
servers 69:20	situation 58:7	speak 37:16	101:11	59:14 64:9
service 11:22	64:2 78:19	speakers 6:5,9	start 7:11 16:19	84:9
62:4	92:16 94:8	speaks 67:11	47:3 51:22	statutorily
set 20:18 30:17	103:20	special 109:4	56:3 75:6	41:16
50:16,16 55:11	situations 56:14	110:22 113:12	started 39:17	statutory 20:7
59:10 114:18	75:12	specific 8:15	54:14 120:8,17	36:15 41:2
120:19	six 54:5 69:1	12:17 26:8,9	starts 98:11	109:7 118:16
setting 7:11	slight 70:16	28:13 56:9	state 33:3 50:3	stay 79:22
seven 26:15	small 11:5 18:11	61:18,18,19	124:4	stayed 80:5
sexual 25:11	93:4	115:17 117:8	stated 9:20 17:2	steel 51:11
shallower 26:5	smith 26:17,20	119:5 120:7	statement 32:20	stems 27:14
share 5:4	45:14	121:9,16	44:15	steps 41:5,16
sharon 3:17	sneaked 89:20	122:17	statements 7:2	steve 15:22
shift 117:2	snowden 8:14	specifically	63:18	16:19 22:19
shifting 122:16	51:14	39:22 67:3,13	states 12:16,20	40:10 44:8
shocking 31:10	society 51:17	88:21 110:10	12:21 13:5,13	46:18 52:5
show 62:17	solely 18:9	116:20	13:17 18:21	56:3 63:18
showing 17:13	soltani 3:7	specificity 59:22	23:19 39:21	65:21 68:16
20:22 61:16	solution 109:7	specified 10:22	41:7 42:1	87:2 104:14,18
105:16 115:1	somebody 12:14	speculative	48:14,18 49:20	107:15 113:3
side 34:22 35:10	12:19,21 52:22	47:12 48:2	52:17 53:2	116:7 120:14
37:10 104:10	53:1 85:8 88:5	49:2 79:6	75:9 77:12	steven 2:11 3:3
104:19 105:2,9	96:3 97:18	80:13	95:1,5 107:19	steves 49:10
105:11	104:22 109:16	spell 123:2	107:21 108:10	106:7
sidebar 54:13	114:3 115:21	spells 10:7	109:1,9,11,17	stop 78:16
sided 34:8	116:3 117:12	spending 94:21	109:21 110:4	stopped 31:19
sides 30:6 34:17	121:6 123:2	spent 40:11 52:4	112:12 113:18	60:19
34:20,20	sophisticated	79:18	113:21 114:3,9	story 90:1,3

95:7	succeeds 41:18	47:6 66:8,10	39:10,20,21	96:15 103:19
stove 51:11	successful 14:14	75:5 76:13	115:14	109:15 114:2
strategic 14:11	suddenly 108:14	99:15	surveilled	114:12 117:12
street 102:13	108:17,21	sure 46:20 58:13	104:11	118:5
strength 80:12	sue 5:6 123:9	78:22 80:4,14	suspect 27:3	talks 122:9
stress 22:6	sufficient 67:15	91:20 92:13	53:9 61:5,18	tangible 55:6
strict 22:13	99:10 108:4	95:14 102:4	109:16	81:9,15 82:8,9
54:18	sufficiently 54:3	105:17 106:2	suspicion 10:20	82:20
strong 79:3 80:9	suggest 18:22	116:21	18:5,9 95:20	target 12:13,18
strongly 61:22	suggested 66:10	surprise 38:10	100:17	13:4 31:2 41:1
structural 99:11	85:12 88:1	surprising	suspicious 18:14	41:7 46:11
99:17	91:2 93:5	59:12	45:9 108:21	48:1,13 107:18
studies 2:14	105:22	surprisingly	swath 64:16	115:20 116:3
16:9	suggesting	43:8	swept 26:14	117:10
study 115:9	79:11	surveil 39:12	switches 83:8	targeted 13:11
stunned 89:22	suggestion	surveillance 1:5	system 29:18,19	88:16 100:21
90:2	24:11 35:3	1:8 2:16 8:5	30:1,17,22	109:8 116:16
subject 8:14	51:22 119:15	9:1 11:17 12:2	32:1 102:17	targeting 12:19
13:20 19:19	suggestions	15:3,5 16:12	103:17 114:18	13:1,3 34:3
30:7,7 51:5	120:7 121:10	19:3,4 23:4,11		41:4,13,21,22
88:7 114:6	121:13	24:21 25:4,21	T	45:8,11 52:19
115:9	summarized	26:1,3,5 27:2	taft 16:14	88:16 101:3
subjected 10:15	17:2	27:14 29:9,14	tail 120:8	109:21 110:3
submit 7:7	summary 7:16	31:2 34:3,12	take 28:11 35:8	115:18 117:5
32:19,21 34:12	111:6	35:15,18 36:6	37:10 38:17	119:5
37:6 123:8	summer 40:15	36:18 38:21	48:15 54:4	targets 39:13
submits 41:12	supervision	39:4,5 40:6,19	73:18 79:9	40:19 41:3
submitted 7:9	12:1	40:20 41:3,7	84:16 89:17,21	42:4 43:12
subordinate	supplied 32:8	41:20 42:4	92:11,13	52:14 94:4,20
70:17	support 86:7	43:11 44:13	102:10 104:10	95:4,5 100:20
subpoena 21:16	105:18	46:6,10,14	121:15 123:13	tasking 88:17
57:12 58:15,22	supported 17:3	47:11 48:8	taken 41:16	tasks 42:11
62:1,3,5,11	19:5 92:17	50:4 53:16	takes 9:14 41:6	technical 6:14
65:1,7,21	110:12	58:17,20 66:11	58:18 97:20	technically
81:16,17 82:1	supporting	83:18,19,20	111:4	88:10
subpoenas	95:18	84:3,4,6 93:21	talk 33:9 45:21	technique 67:12
21:12,18 56:14	suppose 85:10	94:9,9 95:16	talked 45:1	technological
58:8 59:17	supposed 51:9	95:21 96:16	53:20 62:10	23:6 29:8
65:3,5,11,15	60:2 78:20	100:1,12,20	66:6 69:3	technologies
84:16,18	99:5	103:7 108:15	70:18 114:17	14:14
subquestions	suppression	109:4 110:11	talking 16:7	technology 3:2
55:8	65:12	111:3 117:7	52:21 58:11	3:19 23:8
subscriber	supreme 24:19	118:8	70:20 71:12	39:15 51:6
17:18	36:22 37:5	surveillances	79:20 82:8	83:3 108:8

tecum 81:16	text 38:12	theories 106:21	66:20 67:19	three 6:12 43:16
telephone 8:21	thank 5:2,6	theres 18:1 22:4	69:8,9 71:4,6	54:17 74:10
9:10,10,11,16	14:20,21 22:18	44:20 45:8	71:21 72:12,20	87:4 118:21,22
10:4,14,21	22:19 28:4,7,8	47:22 48:3	73:9,12 75:4	throw 55:1
11:17 17:1	32:16 33:2	58:15 63:14,14	75:15 76:1,20	time 7:1 9:12
20:11,18 44:16	37:12,13,15	65:10 67:18	77:9,10,11,18	17:14 35:18
60:11 61:12	44:3,9 46:21	81:13,19 86:6	78:6 79:5,8,9	42:6 43:3
67:21 69:6,12	47:2 51:21	89:11 95:21	79:11,14 82:4	54:14 57:15
70:5 71:17	54:10,11 80:17	105:17 108:6	82:7,8,11,22	58:9 61:2
83:12 105:4	92:7 104:7	113:15 115:16	84:5,12,17	66:13 74:1,22
telephony 31:15	107:9,10 119:9	120:22 122:2,7	85:5,18,19	77:6,6 78:19
98:2,9	123:4,4,5,10	theyre 23:12	86:6,15 89:4	81:22 82:17
tell 33:20 34:16	thankfully	50:15 75:19	89:19 90:11,21	83:8 93:6
70:5 77:22	51:18	82:17,21 83:22	91:19 92:3	94:21 108:13
79:17 103:13	thanks 16:20	88:6,17,18	93:10,16,19	111:11 115:7
105:19	22:20 56:4	91:22 93:12,16	95:6 97:16	117:14 123:5
term 81:10	65:21 68:17	107:6 110:13	98:11,12 99:10	times 31:7 52:13
83:20 121:15	84:4 123:12	thing 34:9 53:9	101:16,19,22	102:13
121:20	thats 7:13 9:9	54:2 59:12	102:16 103:4	tiny 19:9 27:9
terms 8:15	11:5 18:16	71:2 74:2	105:5 106:7,15	tireless 5:9
17:22 22:11,13	20:19 23:2	81:15,15 83:17	109:22 112:21	title 53:7,10
44:16 54:9	27:6 33:8 34:8	111:15 113:5	113:8,15 114:8	104:21 117:1
70:15 83:2	36:12 45:2	116:22 120:14	115:8,18 116:1	today 5:10 6:12
84:10 92:14	49:5 50:8,20	things 8:1,3,20	117:4 119:19	16:7,21 23:10
93:18 106:8	51:14 53:3,5	55:6,14 66:4	120:5,15,21	28:10 31:12
120:7,17	54:2 55:3,12	70:19 71:22	121:7,10,12	33:9 37:18
121:19 123:1	57:4,21 64:1,2	80:4 81:9 84:9	122:1,7,14	38:2 44:1,14
terrorism 77:7	64:18 65:6,14	85:14 97:5	thinking 118:6	80:1 88:2
terrible 121:6	65:18 67:21	101:6	122:14	today's 5:20
terrorism 4:14	68:13 70:6	think 22:15 23:2	third 4:3 6:14	tool 79:4
4:20 13:9	75:1 77:9,16	23:7 28:22	87:22	tools 80:5,10,13
110:18	78:20,21 79:8	30:15 31:22	thorough 40:13	topic 48:11
terrorismrelat...	79:11 82:13,22	32:4,12 34:21	thought 44:12	torture 84:8
9:8 11:8	83:3,3 87:10	35:12 44:14,17	64:12 85:21	total 27:21
terrorist 8:4	89:18 90:3	44:19,21 45:19	86:2	touch 6:2 56:5
10:22 14:9,10	92:2 94:14	46:4 48:11	thoughts 81:17	66:19
18:6 19:1	95:14 96:7	49:4,8,12 50:5	118:20	touched 54:2
20:14 74:12	97:1 101:4	50:8,17 51:4	thousands	107:16
109:1,15	105:5,12	51:16 54:2,14	108:22	tough 46:19
terrorists 8:3	111:15 112:12	56:5,11 57:18	threat 14:5	tower 9:22
tested 65:10,12	113:11 114:13	57:20 58:5,12	46:11	trace 35:17 83:2
testified 19:7	120:9,13	59:9,20 60:2,7	threats 14:15	track 118:3
testifying 40:11	theme 105:8	60:14,20 61:13	77:12,13,14	tracked 26:21
testimony 85:3	theoretical 31:6	63:5,7 64:17	96:16	tracking 25:6,12

26:7 45:2,4,6,8	two 5:10,18 6:16	unconstitutio...	117:12	verbatim 124:5
traditional	7:2,13,21 8:2	23:12 26:4	university 3:3	version 107:3
64:14 102:17	10:2 14:18	undeniable	unnecessary	versus 37:1
traffic 38:9	15:3,15 27:3	36:19	19:15	45:14 77:20
trained 23:3	30:6,16 32:3	underlying 50:9	unusual 94:14	120:11
transactional	44:5 51:1 62:2	underscore	unwise 23:12	vetted 53:17
17:11 21:21	63:17 81:18	23:10	upheld 26:18	view 25:4 36:8
transcript 7:4	103:21 106:5	understand	urge 114:16	62:22 70:19
124:6	120:20,20	14:3 17:7 20:3	urged 6:9,19	77:19 84:11
transcription	type 10:3,18	46:4 56:19	urgent 43:2	98:15,16
124:5	20:15 38:10	60:6 73:3 90:6	usa 1:6 5:12	103:14 111:8
transmitted	83:9 88:11	93:20 94:21	8:16	112:22
83:22	94:8	understandable	usage 84:10	viewed 122:20
transparency	types 15:3,5	23:2	use 20:12 21:3	views 5:4 6:21
106:19	54:5 94:9	understanding	35:9 49:14,18	15:8 54:22
transparent	typical 84:17	56:1 75:7	50:13,19 53:21	80:20
106:21	typically 93:2	76:18	60:7 62:6,6	violate 30:10
trap 35:17 81:19		understands	64:8 65:3 77:4	violated 103:11
83:2 86:20	U	81:11	81:10 84:4	visited 25:18
traps 81:21	u 11:17 13:1,3,4	understood	102:15 110:16	visits 23:22
trial 65:9,13	13:12,16 14:1	55:14,21 57:19	111:16 118:17	voices 32:13
tried 49:17	16:10,17 18:8	undertake 46:9	121:20	voicing 64:4
triggered 27:10	19:1,4,16	38:20	used 83:18	voluntarily 22:1
trouble 48:4	39:11 41:10,21	undertook	useful 57:1,4	voted 56:9 63:21
true 27:12 51:2	42:10 45:13	38:20	77:6,19	
51:14,16 62:9	52:2 53:4 66:6	undue 39:13	uses 50:11	W
65:6 74:3,6	107:20 108:2	unfortunately	usual 97:16	wainstein 2:17
78:22 80:5,6	108:14,16	123:5	usually 35:22	16:13 37:14
trust 105:15,15	109:2 110:6,7	unilateral 94:1	49:19 63:12,12	38:1 47:5,17
truth 75:4	115:15 116:14	unique 64:2	83:22 92:21	51:21 63:16
try 54:17 102:10	ultimately 40:14	united 12:16,20		73:19 78:10
116:11,13	65:5 101:11	12:21 13:5,13	V	87:1 103:18
trying 101:13	109:6	13:17 18:21	v 26:17 47:7	104:7 115:11
tthe 100:13	unable 40:5	23:19 39:20	49:2 66:7	wainsteins
turn 10:4 14:16	unanimous	41:7 42:1	100:9 111:3	51:12
41:4 55:2	24:20	48:14,18 49:20	valid 121:22	wald 2:5 4:6
turned 36:8	unauthorized	52:17 53:2	validity 6:10	14:19 15:1
65:11 73:5	31:13 104:4	75:9 77:12	100:2	44:3,9 46:18
82:17	uncertainty	95:1,5 107:18	valuable 116:8	46:22 49:6
turning 11:19	118:8	107:20 108:10	value 54:3 79:16	50:22 51:20
turns 73:5	unclassified	109:1,9,11,17	various 42:11	65:22 68:19,22
tweaking 91:3	5:22 7:17	109:21 110:4	68:2 79:20	69:4 70:16
twelve 29:16	uncommon	112:11 113:18	vast 11:6 27:17	72:6,10 87:3
twice 79:5	73:21	113:20 114:3,9	vendors 77:21	89:20 92:7,10
		115:22 116:6		

96:1 97:14 104:5 107:9 walking 79:10 wall 102:13 want 4:5 7:11 11:13 28:11 29:13 32:10 33:9 45:21 49:7 55:3,3 56:3 64:22 66:19 78:13 80:19 97:15 102:21 109:14 113:3 117:4 wanted 5:2,6 32:17 98:10 wants 88:12 92:11 warrant 12:17 21:6,20 35:21 76:7 90:9 92:17,20 93:1 94:8 104:20,22 105:17,18 110:1 113:9,17 114:2,6,11,12 115:1 116:11 116:13 warrantless 60:18 warrants 24:4,8 33:19 35:15,16 35:18 102:1,2 105:12 110:12 110:14 washington 1:16 16:18 wasnt 62:19 91:2 100:19 101:10 way 52:1 55:20 62:9 63:22 64:4,18 76:6 78:20 80:2	84:7,19 85:5 85:19,22 86:5 86:12 89:1 92:7,9 95:22 99:4 102:1 103:2,16 120:19 121:20 124:10 ways 29:5 77:14 wealth 25:10 weapons 14:13 website 7:5 23:22 websites 25:17 wed 69:19 weeks 49:4 86:4 98:18 115:10 weitzner 3:9 welcome 4:2 7:8 32:21 123:8 weve 49:16 63:19 77:8 118:4 whack 92:11,13 whats 49:5 57:18 95:16 96:9 102:20 122:4 white 2:18 93:14 whos 104:10 115:21 116:3 116:16 wickersham 16:14 wide 51:16 wilson 60:22 wire 84:1 108:15 wiretap 35:16 35:21 53:10 104:21 wiretapped 114:6 wiretaps 53:8	wish 7:7 33:22 102:11 witness 124:12 witnesses 119:10,16 witnessing 29:17 witting 95:17 wondered 97:12 woodward 51:9 wool 51:11 word 35:5,9 56:11,13 60:7 63:1 83:18 84:4 104:6 words 11:3 12:22 28:21 67:2 111:17 work 29:4 33:14 33:20 57:2 60:3 79:22 88:8 91:1 102:12 103:17 107:5 116:20 workable 95:6 108:19 worked 32:11 76:4 works 35:14 workshop 1:5 1:15 5:4,14,20 7:3 world 79:13 116:18 worrisome 96:14 worrying 94:22 worse 40:3 worth 27:20 122:14 wouldnt 110:13 113:10 written 7:7 12:9 32:19 60:22	123:9 wrong 24:13 52:3 115:13 wrote 33:5 <hr/> X <hr/> Y <hr/> yall 118:22 yalls 118:17 yeah 107:14 year 42:16 47:7 48:2 years 18:18 26:15 29:16 32:5 33:11 39:16 65:16 74:10,10 90:7 98:19 100:5 112:6 yellow 15:13 york 101:10 102:13 youd 32:21 69:11 96:22 youll 52:20,22 78:5 youre 32:21 52:19 70:4,6 83:4,15 91:5 108:14 109:15 110:3,6,7 112:21 114:8 114:12 116:4 118:13 121:5 youve 46:19 121:7 <hr/> Z <hr/> zazi 73:4,4 122:21 <hr/> 0 <hr/>	<hr/> 1 <hr/> 10th 124:19 11 4:10 40:4 79:10 107:11 107:11 108:20 109:12 1127 1:16 12 123:14 12333 67:9 116:18 15 15:19 17 107:11 1902 90:13 1974 28:16 1978 38:20 40:2 46:6 93:21 103:2 108:8 1994 76:4,12 1st 7:10 <hr/> 2 <hr/> 2001 31:11 61:16 64:8 122:10 20036 1:17 2004 85:5,6 2005 16:3 36:3 122:10,13 2006 17:9 118:7 2007 40:8 2008 36:5 38:16 40:16 42:16 2009 16:3 2011 8:17 20:2 2012 11:9 12:7 19:7 33:6 2013 1:10 124:13 2014 124:19 215 1:6 5:11 8:16,18,21 17:3 19:18 20:2,8,21 22:6
--	--	--	---	--

22:10 23:15,17 24:7 25:13 26:6,13,16,17 28:15 44:16 54:21 55:5,15 60:9 61:1,6,10 61:14 62:11,13 62:14 63:1,21 65:21 67:3,14 67:21,22 71:11 71:17 81:1,5,8 82:4,5 83:19 85:7 86:11 89:15,15 118:18 120:4,6 122:9	117:7,13 118:16 119:3,7 120:5			
	8			
	9			
	9 1:10,17 4:10 40:4 79:10 108:20 109:12			
	90 10:11 17:5			
3				
30 1:17 107:11 123:14				
300 11:9 19:8 74:5				
4				
5				
6				
7				
702 1:7 5:12 11:20 12:1,6 12:22 23:16 28:15 37:20 38:3 40:17 45:11 47:12 48:13 94:17,18 95:2 100:13 107:15 109:7 109:19 110:18 110:19 111:4 114:1,13 115:14,17 116:1,12 117:6				