

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Public Hearing Regarding the  
Surveillance Program Operated Pursuant to  
Section 702 of the Foreign Intelligence  
Surveillance Act

March 19, 2014

The public hearing was held at the Renaissance  
Mayflower Hotel, 1127 Connecticut Avenue NW,  
Washington, D.C. 20036 commencing at 9:00 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

Government Perspective on Section 702 Foreign  
Intelligence Surveillance Act

- James A. Baker, General Counsel, Federal Bureau of  
Investigations
- Rajesh De, General Counsel, National Security  
Agency
- Robert Litt, General Counsel, Office of the  
Director of National Intelligence
- Brad Wiegmann, Deputy Assistant Attorney General,  
National Security Division, Department of Justice

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

PANEL II

Legal Issues with 702

Foreign Intelligence Surveillance Act

Laura Donohue, Professor of Law, Georgetown

University Law School

Jameel Jaffer, Deputy Legal Director, American

Civil Liberties Union

Julian Ku, Professor of Law, Hofstra University

Rachel Levinson-Waldman, Counsel, Liberty and

National Security Program, Brennan Center for

Justice

PANEL III

Transnational and Policy Issues

John Bellinger, Partner, Arnold and Porter

Dean C. Garfield, President and CEO, Information

Technology Industry Council

Laura Pitter, Senior National Security Researcher,

Human Rights Watch

Ulrich Sieber, Director, Max Planck Institute for

Foreign and International Criminal Law, Germany

Christopher Wolf, Partner, Hogan Lovells

1 PROCEEDINGS

2 MR. MEDINE: Good morning. Welcome to  
3 the Privacy and Civil Liberties Oversight Board's  
4 hearing on the 702 Program.

5 I'm David Medine, PCLOB's chairman.  
6 It's 9:05 a.m. on March 19th, 2014 and we are in  
7 the grand ballroom of the Mayflower Hotel located  
8 at 1127 Connecticut Avenue, NW, Washington, D.C.

9 This hearing was announced in the  
10 Federal Register on March 10th, 2014. As  
11 chairman, I will be the presiding officer.

12 All five Board members are present and  
13 there is a quorum. The Board members are Rachel  
14 Brand, Elisebeth Collins Cook, James Dempsey, and  
15 Patricia Wald.

16 I will now call the hearing to order.  
17 All in favor of opening the hearing please say  
18 aye.

19 (Aye)

20 MR. MEDINE: Upon receiving unanimous  
21 consent to proceed, we will now proceed.

22 I want to thank the many panelists who

1 will be participating in today's hearing for  
2 agreeing to share their views with the Board.

3 I also wanted to thank the Board's  
4 staff, Sharon Bradford Franklin, Sue Reingold,  
5 Peter Winn, Diane Janosek, Brian Frazelle, and  
6 Simone Awang for their efforts in making this  
7 event possible.

8 Last year PCLOB agreed to provide the  
9 President and Congress a public report on two  
10 federal counterterrorism programs, the Section 215  
11 program under the USA PATRIOT Act and the 702  
12 program under the FISA Amendments Act. The report  
13 on the 215 program was issued on January 23rd,  
14 2014.

15 Our focus today will be on the Section  
16 702 program under the FISA Amendments Act. The  
17 purpose of this hearing is to foster a public  
18 discussion of legal, constitutional, and policy  
19 issues relating to this program.

20 A few ground rules for today, we expect  
21 that the discussion will be based on unclassified  
22 or declassified information, however some of the

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

4           In order to promote a robust discussion  
5 speakers may choose to reference these documents  
6 or information, but they should keep in mind that  
7 in some cases they remain classified. Therefore,  
8 while discussing them, neither the Board members  
9 nor speakers in a position to do so will confirm  
10 the validity of the documents or information.

11           There will be three panels today. The  
12 first will consist of government officials whose  
13 agencies have varying degrees of responsibility  
14 for the surveillance programs that will be the  
15 subject of our report.

16           The second panel will consist of  
17 academics and advocates who will focus on legal  
18 issues, including statutory and constitutional  
19 issues. After the first two panels we will be  
20 taking a lunch break.

21           The final panel will consist of a mix  
22 of academics, advocates, and private sector

1 representatives and will focus on transnational  
2 and policy issues.

3 Board members will each pose questions  
4 during each panel with questions in rounds for  
5 each Board member. Panelists are urged to keep  
6 their responses brief and to permit the greatest  
7 exchange of views.

8 The program is being recorded and a  
9 transcript will be posted on PCLOB.gov. Written  
10 comments from members of the public are welcome  
11 and may be submitted online at regulations.gov or  
12 by mail until March 28th.

13 Today's hearing will focus on the  
14 government's collection of foreign intelligence  
15 information from electronic communication service  
16 providers under court supervision pursuant to  
17 Section 702 of the Foreign Intelligence  
18 Surveillance Act.

19 Information is obtained with FISA court  
20 approval based on written directives from the  
21 Attorney General and the Director of National  
22 Intelligence to acquire foreign intelligence

1 information. This law permits the government to  
2 target non-U.S. persons, someone who is not a  
3 citizen or a permanent resident alien, located  
4 outside the United States for foreign intelligence  
5 purposes without obtaining a specific warrant for  
6 each target.

7 We will now turn to our first panel,  
8 and I understand that Bob Litt will be making an  
9 opening statement for the panel.

10 MR. LITT: Thank you, and thank you for  
11 the opportunity to appear on behalf of the whole  
12 group here and talk about Section 702.

13 I would like to give a brief overview  
14 of Section 702 to set the stage, and we'll be glad  
15 to fill out some of the points I make here in  
16 response to questions.

17 Section 702, as you noted, enables us  
18 to collect intelligence against foreign targets  
19 who are outside of the United States while  
20 robustly protecting privacy rights.

21 Under Section 702 the FISA court  
22 approves annual certifications submitted by the

1 Attorney General and the Director of National  
2 Intelligence that identify categories of foreign  
3 intelligence that may be collected. We then  
4 target selectors such as telephone numbers or  
5 email addresses that will produce foreign  
6 intelligence falling within the scope of the  
7 certifications.

8           The FISA court also has to review and  
9 approve targeting and minimization procedures.  
10 The targeting procedures ensure that we target  
11 only non-U.S. persons who are reasonably believed  
12 to be outside of the United States, that we do not  
13 intentionally intercept totally domestic  
14 communications, and that we do not target any  
15 person outside of the United States as a  
16 subterfuge to actually target someone inside the  
17 U.S.

18           The minimization procedures ensure that  
19 consistent with foreign intelligence needs, we  
20 minimize the acquisition and retention of  
21 non-public information available about U.S.  
22 persons and that we prohibit the dissemination of

1 such information.

2 I want to make a couple of important  
3 overview points about Section 702. First, there  
4 is either a misconception or a mischaracterization  
5 commonly repeated that Section 702 is a form of  
6 bulk collection. It is not bulk collection. It  
7 is targeted collection based on selectors such as  
8 telephone numbers or email addresses where there's  
9 reason to believe that the selector is relevant to  
10 a foreign intelligence purpose.

11 I just want to repeat that Section 702  
12 is not a bulk collection program.

13 Second, from a legal point of view  
14 persons who are not U.S. persons and who are  
15 outside of the United States do not have rights  
16 under the Fourth Amendment and so the Constitution  
17 doesn't require individualized warrants to target  
18 them.

19 In fact, the type of intelligence that  
20 is covered by Section 702 targeting foreigners  
21 outside of the United States has historically been  
22 viewed as part of the President's inherent

1 constitutional authority and I'm not aware of any  
2 other country that brings this kind of collection  
3 under this sort of judicial process.

4 Third, collection under 702 is subject  
5 to extensive oversight by all three branches of  
6 government. We can explain the oversight in more  
7 detail later, but it includes extensive review of  
8 collection activities under Section 702 by  
9 inspectors general, by the Department of Justice,  
10 and the Office of the Director of National  
11 Intelligence. It includes reporting of all  
12 compliance incidents to the Foreign Intelligence  
13 Surveillance Court, and it includes periodic  
14 reports both to Congress and to the court.

15 As the documents that we've  
16 declassified and released make clear, the Foreign  
17 Intelligence Surveillance Court carefully  
18 scrutinizes our activities under this section.  
19 And while there have been a number of compliance  
20 incidents over the years, the court has never  
21 found any intentional efforts to violate the  
22 requirements of Section 702.

1           Fourth, the fact that the  
2           communications of U.S. persons may be incidentally  
3           intercepted when we target valid foreign  
4           intelligence targets is neither unexpected nor  
5           unique to Section 702 collection.

6           Both the statute itself with its  
7           required minimization procedures and the  
8           legislative history make completely clear that  
9           Congress knew full well when it passed Section 702  
10          that incidental collection of communications of  
11          U.S. persons would occur when they're in  
12          communication with valid foreign targets.

13          And it's important to note that this  
14          kind of incidental collection occurs all the time  
15          in other contexts. When we conduct a criminal  
16          wiretap or a wiretap pursuant to Title I of FISA  
17          we will likely intercept communications of persons  
18          who are not targets. When we seize someone's  
19          computer we may find communications with persons  
20          who are not targets.

21          The minimization rules under Section  
22          702 which the FISA court approves is consistent

1 with both the statute and the Fourth Amendment are  
2 designed to protect the privacy of persons whose  
3 communications are incidentally collected, while  
4 still allowing the use of information that is  
5 lawfully collected for valid foreign intelligence  
6 and law enforcement purposes.

7           Finally, I want to close by just  
8 emphasizing that Section 702 is one of the most  
9 valuable collection tools that we have. Many of  
10 the specific achievements of Section 702 have to  
11 remain classified so that we aren't revealing  
12 exactly who we're targeting and what we're  
13 collecting. But it is one of our most important  
14 sources of information, not only about terrorism  
15 but about a wide variety of other threats to our  
16 nation.

17           And unless one of my colleagues has  
18 something to add, I think we're ready to address  
19 your questions.

20           MR. MEDINE: Great, thank you very much  
21 for that statement.

22           I wanted to start off and pick up with

1 your discussion of incidental collection, and  
2 again just to make clear that under this program,  
3 even though the target may be a non-U.S. person  
4 there will be times when the conversations, either  
5 by email or telephone, the person on the other end  
6 will be a U.S. person.

7           And so my question to the panel is  
8 whether because you're gathering communications of  
9 U.S. persons if that implicates Fourth Amendment  
10 concerns? And if so, do you believe there's a  
11 foreign intelligence exception to the Fourth  
12 Amendment? And if not, how is warrantless  
13 collection of information of U.S. persons  
14 permissible?

15           And then to follow up on Mr. Litt's  
16 comment analogizing this to a traditional wiretap,  
17 is there a distinction here where on a traditional  
18 wiretap the court has, there's been a judicial  
19 determination with particularity of a particular  
20 collection, whereas here there's only broad  
21 programmatic court approval and not approval of  
22 the specific collection?

1           So I guess broadly speaking, can you  
2 address the Fourth Amendment concerns regarding  
3 incidental collection?

4           MR. WIEGMANN: Sure, I'll take that.  
5 So this is, as Bob said, collection that is  
6 targeting non-U.S. persons overseas who don't  
7 enjoy Fourth Amendment rights under controlling  
8 Supreme Court precedent. So that affects the  
9 Fourth Amendment analysis.

10           That's not to say that U.S. persons  
11 whose information is or whose communications are  
12 collected incidentally doesn't trigger a Fourth  
13 Amendment review. It does. Those people still  
14 have Fourth Amendment rights, but what the courts  
15 have said is that, what the FISA court has said is  
16 that the minimization procedures that are in place  
17 render that collection reasonable from a Fourth  
18 Amendment perspective.

19           We think there's an exception to the  
20 warrant requirement. Before FISA was enacted in  
21 the 1970s a number of courts held in a number of  
22 different circuits that there is a foreign

1 intelligence exception to the warrant requirement  
2 under the Fourth Amendment, in light of the  
3 special needs of the government to collect foreign  
4 intelligence, weighed against the privacy  
5 interests of U.S. persons concluded that you don't  
6 need a warrant when you're engaged in foreign  
7 intelligence collection.

8           So then the only remaining question is,  
9 is it reasonable under the Fourth Amendment to  
10 collect information on U.S. persons incidentally  
11 when you're targeting non-U.S. persons. And what  
12 the FISA court has held is that it is reasonable  
13 in light of the minimization targeting procedures  
14 that we have in place. So I don't know if that  
15 answers your question, but.

16           So the way you look at it is the  
17 warrant requirements not applicable to foreign  
18 intelligence collection still have a  
19 reasonableness requirement with respect to  
20 incidentally collected U.S. persons, and that in  
21 fact, it is reasonable in light of the procedures  
22 that we have that are designed to ensure that we

1 are targeting only non-U.S. persons.

2 MR. MEDINE: And could you address why  
3 the minimization procedures make it a reasonable  
4 form of collection under the Fourth Amendment?

5 MR. WIEGMANN: Yes, so the minimization  
6 procedures address, and the targeting procedures  
7 address the acquisition, retention, and  
8 dissemination of U.S. person information.

9 And so those procedures all are  
10 designed to protect those U.S. persons whose  
11 information might be incidentally collected.

12 So for example, you can only  
13 disseminate information about a U.S. person if it  
14 is foreign intelligence, or necessary to  
15 understand foreign intelligence, or is evidence of  
16 a crime.

17 You have retention rules. I believe in  
18 some cases, for NSA for example, you have a five  
19 year retention limit on how long the information  
20 can be retained. And so these are procedures that  
21 the courts have found protect U.S. privacy and  
22 make the collection reasonable for Fourth

1 Amendment purposes.

2 MR. MEDINE: And under the minimization  
3 procedures I understand that the agency, the NSA,  
4 FBI, the CIA have their own minimization  
5 procedures and they're not the same with each  
6 other?

7 MR. WIEGMANN: That's right.

8 MR. MEDINE: Can you address why that  
9 shouldn't be a concern that this information is  
10 not being subjected to the same minimization  
11 standards?

12 MR. WIEGMANN: So each of them have  
13 their own minimization procedures based on their  
14 unique mission, and the court reviews each of  
15 those for CIA, FBI, NSA, and it's found them all  
16 reasonable for each different agency. They're  
17 slightly different based on the operational needs,  
18 but they're similar.

19 MR. MEDINE: Would it make more sense  
20 then if the same set of minimization procedures  
21 apply across the board for this kind of  
22 information?

1           MR. WIEGMANN: I don't think. Again,  
2 just to contrast, for example, FBI and NSA that  
3 are using information in different ways. The FBI  
4 has a little more latitude with respect to U.S.  
5 person information in terms of criminal activity  
6 and evidence of a crime than NSA, which doesn't  
7 have that law enforcement mission. So I think it  
8 is important to have some differences between the  
9 agencies in terms of how they handle the  
10 information.

11           MR. MEDINE: And is it the practice  
12 that all information that's collected under 702 is  
13 subject to the minimization procedures?

14           Some questions I think have been raised  
15 in some of the comments that were submitted as to  
16 whether address books or other information would  
17 be considered communications that would be subject  
18 to minimization, or is it the approach that all  
19 information collected under 702 is subject to  
20 minimization?

21           MR. WIEGMANN: All U.S. person  
22 information is subject to minimization procedures.

1 MR. MEDINE: I think my time is up.

2 MS. BRAND: First of all, thanks to all  
3 of you for being here this morning. We appreciate  
4 your taking the time and making yourselves  
5 available.

6 I want to continue on the Fourth  
7 Amendment discussion. Could one of you explain  
8 the process both inside the executive branch and  
9 then with the court of conducting the Fourth  
10 Amendment analysis and seeking the court's  
11 approval of the Fourth Amendment analysis and what  
12 kinds of opinions on the Fourth Amendment you've  
13 had from the court, to the extent that you can  
14 talk about it. Help us to understand how that  
15 works.

16 MR. WIEGMANN: So, you know, the FISA  
17 court operates a little bit differently than a  
18 regular court in the sense that it's ex parte,  
19 but. So that means only the government is there.  
20 There's not a party on the other side.

21 But other than that, we are briefing  
22 the legal issues in much the same way as we would

1 in a regular proceeding where there is a party on  
2 the other side. So we have an obligation to  
3 persuade the court that the collection under 702  
4 is lawful, that it complies with the Fourth  
5 Amendment, and as I just explained to the chair,  
6 that minimization procedures comply with the  
7 Fourth Amendment.

8 So we would brief that issue explaining  
9 the Fourth Amendment procedures, and the court  
10 issues opinions and has issued opinions going  
11 through the Fourth Amendment analysis and finding  
12 that 702 collection, including the minimization  
13 targeting procedures meets the Fourth Amendment  
14 standards. So it's a full-up kind of regular  
15 legal briefing on that.

16 MR. LITT: And if I could just add  
17 something to that, it is typical in matters that  
18 involve the collection of evidence for these  
19 proceedings to be conducted ex parte. Wiretap or  
20 search warrant applications are also all done ex  
21 parte, even if they happen to present significant  
22 legal issues. So this is nothing novel in terms

1 of the approach that's taken there.

2 MR. DE: And if I could have one point.  
3 So in addition to what Brad was articulating, the  
4 court reviews this at least annually, the Fourth  
5 Amendment analysis.

6 As you all know, the 702 process  
7 requires annual certification. As part of that  
8 certification process every year the minimization  
9 and targeting procedures for the various agencies  
10 are submitted to the FISC, which by statute has to  
11 conduct a Fourth Amendment analysis on those  
12 procedures as part of that annual review process.

13 MS. BRAND: So the Fourth Amendment  
14 analysis is once a year of the program overall?

15 MR. DE: Well, the court has consistent  
16 jurisdiction over the program all year. The point  
17 I was making is that as part of the annual  
18 certification process, by statute the court is  
19 required to do a Fourth Amendment analysis of the  
20 annual, of the procedures that are submitted  
21 annually.

22 MR. BAKER: It gets evaluated at least

1 once a year.

2 MS. BRAND: Can you elaborate on that?  
3 What would there be in addition to that once a  
4 year analysis?

5 MR. DE: There could be a variety of  
6 factors. There could be a need to change  
7 procedures in the year, so that would prompt  
8 another analysis. I don't believe we've done that  
9 but that could be one circumstance.

10 There could be a variety of compliance  
11 matters that raise particular concerns to the  
12 court, in which case the court may want to do a  
13 review off-cycle.

14 So I think we wouldn't presume and say  
15 it only had to be once a year, but at a minimum by  
16 statute it needs to be once a year.

17 MS. BRAND: Okay. Bob, you talked  
18 about 702 not being bulk collection. I'd like to  
19 delve into that a little bit more, it's not bulk  
20 collection. You talked about selectors. We need  
21 to elaborate on that a little bit, I think. What  
22 is it? It's not bulk you say, but what is it?

1           MR. LITT: Sure. Well, I think it's  
2 probably helpful to talk about what bulk  
3 collection is first of all.

4           And if you look at the President's  
5 policy directive there's a definition. I don't  
6 have it in front of me, but it's essentially bulk  
7 collection is collection of communications without  
8 relying on some sort of discriminant to ensure  
9 that you're targeting particular collection.

10           It's sort of viewed sort of more  
11 informally, it's getting a whole bunch of  
12 communications, hanging onto them and then  
13 figuring out later what you want.

14           This is not that. This is a situation  
15 where we figure out what we want and we get that  
16 specifically. And so that's why it is targeted  
17 collection rather than bulk collection. Is that  
18 helpful?

19           MS. BRAND: But I'd like to get a  
20 little bit more into what is it that you're  
21 getting. So you have a selector, I mean.

22           MR. LITT: Sure. So Raj probably can

1 talk to this a little better than I can.

2 MR. DE: So if I could, I'd step back  
3 and just talk about the different types of  
4 collection under Section 702, which I think is a  
5 necessary predicate to understand how collection  
6 occurs.

7 So there's two types of collection  
8 under Section 702. Both are targeted, as Bob was  
9 saying, which means they are both selector-based,  
10 and I'll get into some more detail about what that  
11 means. Selectors are things like phone numbers  
12 and email addresses.

13 Both are affected by compulsory legal  
14 process, both types are conducted with the  
15 assistance of electronic communication service  
16 providers, and both types of collection under 702  
17 are subject to the same statutory standards, so  
18 just as a predicate.

19 The first type is what's now been come  
20 to be known as PRISM collection, so just using  
21 that shorthand for a moment. And under this type  
22 of collection, communications to or from specific

1 selectors, again, things like phone numbers or  
2 emails, are provided with the assistance of ISPs  
3 pursuant to directives.

4           The second type of collection is the  
5 shorthand referred to as upstream collection.  
6 Upstream collection refers to collection from the,  
7 for lack of a better phrase, Internet backbone  
8 rather than Internet service providers.

9           It is also however selector-based, i.e.  
10 based on particular phone numbers or emails,  
11 things like phone numbers or emails. This is  
12 collection to, from, or about selectors, the same  
13 selectors that are used in PRISM selection. This  
14 is not collection based on key words, for example.

15           This type of collection upstream fills  
16 a particular gap of allowing us to collect  
17 communications that are not available under PRISM  
18 collection.

19           But given the unique nature of upstream  
20 collection there are different minimization  
21 procedures that apply, to get to the chair's  
22 question earlier.

1           The reason procedures aren't always the  
2 same for different types of collection, as Brad  
3 articulated, is that there are both different  
4 mission interests and different privacy interests  
5 at stake.

6           MS. BRAND: I see my time is up, so.

7           MS. COLLINS COOK: Thank you for coming  
8 here this morning. We really appreciate your time  
9 on this and happy to be a part of this dialogue  
10 here.

11           I wanted to follow up on a couple of  
12 points that have already been raised, but first,  
13 we've talked about the Fourth Amendment  
14 implications of the collection. We've also talked  
15 about the fact that, or it is known that the  
16 information that's collected can subsequently be  
17 queried.

18           Do you consider that subsequent query a  
19 search for the purposes of the Fourth Amendment?  
20 And if not, why not?

21           MR. WIEGMANN: No, I would say that the  
22 search occurs at the time that the collection

1 occurs. So when the information, as Raj just  
2 explained, from a particular selector is acquired  
3 by NSA, then that's the time at which the search  
4 occurs.

5           Once you've lawfully collected that  
6 information, subsequently querying that  
7 information isn't a search under the Fourth  
8 Amendment, it's information already in the  
9 government's custody. And so I don't think there  
10 are any other contexts really in general in which  
11 a warrant is required to search information  
12 already in your custody.

13           MS. COLLINS COOK: Following up on  
14 that, I think some have suggested that whether as  
15 a matter of Fourth Amendment necessity or as a  
16 policy, as a matter of policy that you should seek  
17 court approval before doing a query of a U.S.  
18 person identifier.

19           Can you talk a little bit about what  
20 the operational impact of such a requirement might  
21 be?

22           MR. WIEGMANN: Sure, and this is

1 something I guess some of my colleagues could talk  
2 about the operational impact. But as I said, in  
3 general with other types of collection, whether  
4 it's collection under Title I of FISA, which is  
5 your regular collection under which you've gone to  
6 the FISA court and already gotten approval to  
7 target a particular agent of a foreign power in  
8 the United States, or moving over to the criminal  
9 side if it's information collected under the  
10 Wiretap Act, commonly known as Title III, under  
11 which you're conducting surveillance, let's say of  
12 an organized crime figure or in a drug case of an  
13 individual, in all of these contexts we collect  
14 information.

15           We don't, once we've collected it,  
16 we've gotten the necessary court approvals to  
17 obtain the information, we don't then have to go  
18 back to court to query the same information that  
19 we've already collected lawfully a second time to  
20 say is it okay to look at it. We've already  
21 gotten the conclusion that it's legal to collect  
22 it.

1           And if you have to go back to court  
2 every time you look at the information in your  
3 custody you can imagine that that would be quite  
4 burdensome and difficult, to have to go back every  
5 time to look at information that's already in your  
6 custody. But I can let the FBI and NSA address it  
7 a little bit.

8           MR. DE: If I could add a couple of  
9 points and then I'll turn it to my colleague from  
10 the bureau.

11           Just one basic point, we've been  
12 talking about U.S. person queries and I just  
13 articulated two types of collection. Just to  
14 clarify, U.S. person queries are not allowed under  
15 what I described as upstream collection. So as I  
16 articulated, there may be different reasons to  
17 have tailored procedures, minimization procedures  
18 for different types of collections. So such  
19 queries are not allowed for upstream.

20           Adding to Brad's point about lawfully  
21 collected information, so once information is  
22 collected pursuant to 702, the government can and

1 often will review what it needs to in that  
2 information.

3           Querying that lawfully collected  
4 information, one way to think about that is a way  
5 to more efficiently review that which the  
6 government already has in its possession and can  
7 review all of.

8           And so to get to your question about  
9 policy limits on querying that data, one also  
10 needs to understand that that information is at  
11 the government's disposal to review in the first  
12 instance, and querying it is just a way to  
13 organize it.

14           Secondly -- thirdly, if I could add  
15 there are standards in place for querying that  
16 information, at least for NSA. Such a query, and  
17 we're talking about PRISM collection, must be  
18 reasonably likely to return foreign intelligence  
19 information.

20           And then finally, in order to  
21 disseminate any U.S. person information that may  
22 result from such a query it has to be necessary to

1 understand the foreign intelligence or evidence of  
2 a crime is apparent from our publicly available  
3 procedures.

4 But on the operational element, let me  
5 turn that to Jim.

6 MR. BAKER: So just at a high level I  
7 think let me make a couple of comments. So first  
8 I think you have to think about the fact that  
9 you're creating a new and special category of  
10 information, as Brad was saying, right. So this  
11 would be information that had already been  
12 acquired pursuant to lawful process.

13 We normally will query that. We'll  
14 look through that. When something comes in, we'll  
15 look through our collected materials to try to  
16 find -- a threat comes in, let's say for example.  
17 We look at our collected materials, we try to  
18 figure out what we have, and then, you know, move  
19 forward as expeditiously as possible.

20 So you would be creating a new category  
21 of information that sort of would be off-limits  
22 from the normal type of collection that we do.

1 And I don't pretend to fully understand all the  
2 implications that that would have.

3 But a couple that come to mind, first  
4 of all, obviously would be delay. So you would  
5 have some additional process that you would have  
6 to go through, and I'm sure there would be some  
7 kind of emergency carve out and so on, but you'd  
8 have to think about and factor in the reality that  
9 you would be introducing delay into the system.

10 You would also then as a result  
11 potentially create a gap. There are several types  
12 of gaps, I guess. But you would have, there would  
13 be a disinclination for people, because either  
14 they don't have the facts, or it's just too hard  
15 or whatever, to actually go and pursue that extra  
16 pot of information.

17 So there might be some type of  
18 connection between what we can look at normally,  
19 this material, and then other types of material.  
20 And having that type of gap might, you know,  
21 actually create a blind spot for us in terms of  
22 intelligence collection.

1                   You'd also have to think about, I  
2 think, the technical complexity of what it is that  
3 you're suggesting. So this is going to have to be  
4 segregated in some way, treated differently. And  
5 we'd just have to think about that. That could  
6 lead to, you know, training issues, technical  
7 costs, things like that.

8                   So it's, you just have to actually do  
9 it in a way that would be different than from  
10 other types of data that we handle, so that's sort  
11 of at a high level some of the things that come to  
12 mind.

13                   MR. LITT: Beth, can I add one brief  
14 point to this which is that over the last decade,  
15 decade and a half, there have been a number of  
16 commissions that have been set up to investigate  
17 after a variety of terrorism incidents, 9/11, Fort  
18 Hood, the underwear bomber and so on.  
19 Consistently every one of those commissions has  
20 found that we need to eliminate barriers to making  
21 use of the information that's lawfully in our  
22 possession in order to better protect the nation.

1                   And this, requiring some kind of  
2 additional process before we can query this  
3 information runs directly contrary to the  
4 recommendations of all those commissions.

5                   MS. COLLINS COOK: Thank you. I see  
6 that my time is up.

7                   MR. MEDINE: By the way, I should say  
8 in the excitement of getting into the questioning  
9 I never had actually a chance to introduce the  
10 panelists. And so I just wanted for the benefit  
11 of the audience, you're familiar to us, but for  
12 the benefit of the audience we have Jim Baker,  
13 who's the General Counsel of the FBI, Raj De,  
14 who's the General Counsel at NSA, Bob Litt is the  
15 General Counsel at the Director of National  
16 Intelligence, and Brad Wiegmann, who is the Deputy  
17 Assistant Attorney General at the National  
18 Security Division of the Justice Department.

19                   Again, thank you all for being here.

20                   MR. DEMPSEY: Thanks, and thanks to the  
21 witnesses for being here. They are very  
22 well-known to us. I think everybody should

1 realize that we've now spent many, many days with  
2 these gentlemen and with many, many of their  
3 colleagues at all their agencies going through  
4 this information, and delving deeply into this.

5           And there's been a huge amount of  
6 dedication of time on the part of the agencies to  
7 make sure that we have everything that we ask for  
8 and to make sure that all of our questions are  
9 answered. And so, you know, all the Board members  
10 really appreciate the amount of time that you've  
11 dedicated to talking with us.

12           And I think it is very important here  
13 to be one hundred percent clear, and I think there  
14 has been a lot of misunderstanding about the 702  
15 program, and I think I do see issues with the  
16 program and things we're talking about, but I  
17 think it's very important to narrow the subjects  
18 of controversy, or discussion, or concern.

19           And I'm afraid that Raj may have partly  
20 reinserted a problem here when you said that U.S.  
21 person selectors were not used for upstream  
22 collection, or for upstream searches they're not

1 used at all, period, at the collection stage.

2           You were saying that U.S. person  
3 identifiers or selectors are not used to search  
4 the acquired database of communications that were  
5 otherwise acquired on a particularized basis under  
6 the upstream program, correct?

7           MR. DE: Correct. I definitely would  
8 prefer not to introduce more ambiguities. Let me  
9 be absolutely clear, Section 702 collection of any  
10 flavor, upstream or PRISM, is only targeting  
11 non-U.S. persons reasonably believed to be located  
12 abroad.

13           The topic I was discussing was, is in  
14 the realm of that lawfully collected targets  
15 information, once it's in the government's  
16 possession a secondary issue arises as to how one  
17 can search through that data. And the issue that  
18 we were discussing was whether those searches can  
19 be conducted using U.S. person identifiers within  
20 that lawfully data. And the answer to that  
21 question is no with respect to upstream  
22 collection.

1           MR. DEMPSEY:  And here when you're  
2 talking about search and collect and acquire, all  
3 of those terms you're using to mean in a  
4 colloquial sense when the government collects,  
5 obtains, puts into its database, acquires, you're  
6 not parsing those words for 702 purposes.  There's  
7 not a distinction between the search, the  
8 collection, the acquisition, right?  It's all,  
9 you're using those things all that refer to the  
10 same activity.

11           MR. DE:  There's no parsing between  
12 acquisition or collection.

13           So there are some theories out there  
14 that when the government receives the data it  
15 doesn't count as collection or acquisition.  That  
16 is incorrect.  Acquisition and collection for  
17 these purposes are the same thing.

18           But the term search is a different  
19 term.  Search, as we were just discussing, means  
20 searching information that has already been  
21 lawfully acquired or collected.

22           MR. DEMPSEY:  Although the first --

1    okay, so now we have two meanings of search.  It's  
2    so hard to be clear on this.  Brad was explaining  
3    a search occurs when you first collect or acquire.  
4    That is the Fourth Amendment search.

5               MR. DE:  I think he was speaking to the  
6    use of the term in the Fourth Amendment, not the  
7    use of the term for purposes of this.

8               MR. DEMPSEY:  And then querying, then  
9    there's a second use of search meaning query.  So  
10   you query your database?

11              MR. DE:  Correct.

12              MR. LITT:  That's the term that we  
13   typically use rather than search in that context.

14              MR. DEMPSEY:  Right.  In that case a  
15   query is not a search for Fourth Amendment  
16   purposes.

17              MR. LITT:  Right.

18              MR. DEMPSEY:  Briefly talk a little bit  
19   about this 51 percent theory.  So persons  
20   reasonably believed to be outside the United  
21   States, and there's been some talk about, well, so  
22   there may have been some slide somewhere, I don't

1 know where this came from, but some notion that,  
2 oh, if it's a 51 percent likelihood, therefore 49  
3 percent of the time we might be wrong, that the  
4 person's not outside the United States and that's  
5 permitted under 702. Can you comment on that.

6 MR. DE: Sure. So I think the bigger  
7 picture question that that gets to how a  
8 determination is made for purposes of the statute  
9 that you are in fact targeting a non-U.S. person  
10 reasonably believed to be located abroad.

11 So as Bob articulated, and I'm sorry  
12 for repeating this but just for clarity, the  
13 statute does not allow us to target U.S. persons,  
14 it does not allow the government to target anybody  
15 within the U.S., it does not allow for reverse  
16 targeting, it does not allow for the intentional  
17 collection of wholly domestic communications.

18 So as to how we establish a reasonable  
19 belief that the target is in fact a non-U.S.  
20 person reasonably believed to be located abroad,  
21 there is no 51 percent rule that if you are 51  
22 percent sure it is a non-U.S. person located

1     abroad that is sufficient. That is not the rule,  
2     and I don't honestly know where that misconception  
3     has come from.

4             The foreignness determination, which is  
5     shorthand for referring to the determination that  
6     it is a non-U.S. person reasonably located to be  
7     abroad, is based on a totality of the  
8     circumstances.

9             So what does that mean? That means  
10    that an analyst must take into account all  
11    available information. It means that an analyst  
12    cannot ignore any contrary information to suggest  
13    that that is not the correct status of the person.  
14    And it also means naturally that any such  
15    determination is very fact-specific to the  
16    particular facts at hand.

17            I did a little checking and it turns  
18    out in our internal training materials, at least  
19    at NSA, we actually ask our analysts a question  
20    along the lines of, if you have four pieces of  
21    information that suggests a person is abroad and  
22    two pieces of information that suggests a person

1 is domestic, given that the score is four to two  
2 is that sufficient to establish foreignness?

3 And the correct answer to that is, no,  
4 it is not sufficient because it is not a majority  
5 test. It is a totality of the circumstances test.  
6 One must take into account the strength,  
7 credibility, and import of all relevant  
8 information.

9 But just to add on to that, to your  
10 bigger point about confidence in that  
11 determination, analysts have an affirmative  
12 obligation to periodically revisit the foreignness  
13 determination. So it is not a once and done  
14 system.

15 Moreover, targeting determinations must  
16 be documented ex ante before any collection  
17 occurs. That documentation is reviewed, every  
18 determination is reviewed in 60 day increments by  
19 the Department of Justice and the Office of the  
20 Director of National Intelligence to determine if  
21 they agree with that determination.

22 And then finally, the targeting

1 procedures, as we mentioned, which account for a  
2 lot of this are reviewed annually by the Foreign  
3 Intelligence Surveillance Court and approved to be  
4 consistent with the Fourth Amendment and the  
5 statute obviously.

6 MR. WIEGMANN: And if I could just add  
7 from the DOJ perspective, as Raj said, we reviewed  
8 all of those foreignness determinations and we  
9 found an error rate of less than .1 percent  
10 basically. So that equates to essentially less  
11 than one in a thousand cases in which we're  
12 finding that NSA is making erroneous foreignness  
13 determinations.

14 MR. MEDINE: Judge Wald.

15 MS. WALD: Thank you again. I think  
16 that the NSA has said that in some of its  
17 information that if information about U.S. persons  
18 is collected incidentally to a 702 search that was  
19 targeted on a non-U.S. person and the incidental  
20 information about U.S. persons is found not to  
21 have any foreign intelligence value it will be,  
22 quote, purged.

1           Can you explain exactly what purging  
2 means? Does that mean that it can subsequently  
3 not be used at all, or it can be subsequently used  
4 or retained for some purposes? And finally, at  
5 what point and by whom would this decision of  
6 non-intelligence value be made? There's a lot of  
7 sub-questions.

8           MR. DE: Sure. Well, let me step back  
9 for a moment. If the information is determined to  
10 not have --

11           MS. WALD: Could you just speak a tiny  
12 bit louder because I'm at the tail-end of this  
13 table.

14           MR. DE: Certainly. If information is  
15 determined to not have foreign intelligence value  
16 then it is required to be purged.

17           What purging means is removed from NSA  
18 systems in a way that it cannot be used, period.

19           MS. WALD: For any reason at all?

20           MR. DE: Correct. There are extensive  
21 requirements we have gone through with the Foreign  
22 Intelligence Surveillance Court to ensure to the

1 best extent humanly possible that NSA's technical  
2 systems can, in fact, purge data as required by  
3 both our minimization procedures and the Foreign  
4 Intelligence Surveillance Court.

5 MS. WALD: But just to pursue that a  
6 little bit, in your experience is that to purge or  
7 not to purge decision made early in the process or  
8 is it kept in there until the analyst or whoever  
9 has a chance to do some more hunting around and  
10 see whether or not maybe other things would  
11 suggest that that does have intelligence value?

12 In other words, if there's such a  
13 concern about U.S., as there is in outside groups,  
14 about U.S. incidental information that's in the  
15 files and later there's a possibility of it being  
16 queried, I wonder how extensive this purging  
17 operation really is?

18 MR. DE: To purge or not to purge, that  
19 is the question.

20 MS. WALD: Yes.

21 MR. DE: So our procedures require that  
22 the determination about foreign intelligence value

1 be made as early as possible in the, what one in  
2 the technical sense calls the processing cycle.  
3 So it is not something that by default can be  
4 ignored.

5 That being said --

6 MS. WALD: And who makes that?

7 MR. DE: An assessment as to foreign  
8 intelligence value is made by foreign intelligence  
9 analysts.

10 MS. WALD: By the analysts who are  
11 working on it?

12 MR. DE: Correct, as they would be the  
13 ones who have the most relevant information.

14 But that also goes to a bigger point as  
15 to the nature of intelligence analysis. I think  
16 you all would appreciate that it's difficult to  
17 determine without context the foreign intelligence  
18 value of any particular piece of information. In  
19 fact, that's why the intelligence community is  
20 often encouraged to connect the dots of various  
21 pieces of disparate information.

22 And so I think we would hope and expect

1 that analysts make that determination about  
2 foreign intelligence value within the context of  
3 all available information.

4 But to your point as to if information  
5 is not reviewed, what is the default? This is a  
6 large reason why we in fact have default retention  
7 periods for data. And for example, for NSA the  
8 default for PRISM collection is a five year  
9 retention period.

10 But that's also a reason why that  
11 retention period is adjustable, or at least is  
12 tailored to the specific nature of the collection.

13 So for example, for upstream collection  
14 the retention period is two years, recognizing the  
15 nature of, the unique nature of upstream  
16 collection and that it may have a greater  
17 implication for privacy interests.

18 MS. WALD: Okay. The President  
19 required, I think he required in his January  
20 directive that went to 215 that at least  
21 temporarily the selectors in 215 for querying the  
22 databank of U.S. telephone calls metadata had to

1 be approved by the FISA court.

2           Why wouldn't a similar requirement for  
3 702 be appropriate in the case where U.S. person  
4 indicators are used to search the PRISM database?  
5 I mean what big difference do you see there?

6           MR. LITT: Well, I think from a  
7 theoretical perspective it's the difference  
8 between a bulk collection and a targeted  
9 collection, which is that the --

10           MS. WALD: But I would think that, I'm  
11 sorry for interrupting, Bob. I would think that  
12 message, since 702 has actually got the content.

13           MR. LITT: Well, and the second point I  
14 was going to make is that I think the operational  
15 burden in the context of 702 would be far greater  
16 than in the context of 215.

17           If you recall the number of actual  
18 telephone numbers as to which a RAS, reasonable  
19 articulable suspicion determination was made under  
20 Section 215 was very small.

21           The number of times that we query the  
22 702 database for information is considerably

1 larger. I suspect that the Foreign Intelligence  
2 Surveillance Court would be extremely unhappy if  
3 they were required to approve every such query.

4 MS. WALD: I suppose the ultimate  
5 question for us is whether or not the  
6 inconvenience to the agencies, or even the  
7 unhappiness of the FISA court would be the  
8 ultimate criteria.

9 MR. LITT: Well, I mean I think it's  
10 more than a question of inconvenience. I think  
11 it's a question of practicability.

12 MR. DE: And if I could add one point  
13 to that. I think one must also look at the  
14 underlying nature of the collection program at  
15 issue. And so I think we should be clear not to  
16 conflate the 215 program with the 702 program, and  
17 as you mentioned, one deals with metadata and one  
18 deals with content.

19 But the important point being the  
20 latter is directed at content collection targeting  
21 non-U.S. persons located abroad, whereas the 215  
22 program, although it deals with metadata, did not

1 have such a necessary distinction.

2 MS. WALD: It did have a selective, I  
3 mean the 215 program and the original --

4 MR. MEDINE: I'm going to, your time,  
5 the Judge's time has expired, but we'll have an  
6 opportunity in another round to continue that  
7 discussion.

8 I want to shift to a different topic,  
9 which is about communication, about searches or  
10 about queries, which is, and I'm happy to have you  
11 explain it, but my understanding basically is that  
12 you are looking for other peoples' discussion of a  
13 particular selector or email term.

14 But I'd like to get back to some of the  
15 definitions here, which are there are some terms  
16 here that would be helpful to understand your view  
17 of, which is what is a target? What is a tasking?  
18 What is a selector? What's a directive?

19 If you could explain those terms,  
20 because I did want to shift to how those terms  
21 might apply in the about context.

22 MR. WIEGMANN: Okay, I can take a stab

1 at that. So a target is the -- maybe I should  
2 start with selector since that's the operative  
3 term that the others build on.

4 A selector would typically be an email  
5 account or a phone number that you are targeting.  
6 So this is the, you get, you know, terrorists at  
7 Google.com, you know, whatever. That's the  
8 address that you have information about that if  
9 you have reason to believe that that person is a  
10 terrorist and you would like to collect foreign  
11 intelligence information, I might be focusing on  
12 that person's account.

13 So when you go up on that selector, we  
14 say go up on or target that selector, that means  
15 we're collecting information, we're going to the  
16 provider and getting information related to that  
17 person's account.

18 So we're intercepting in real time and  
19 then collecting the historic communications of  
20 that particular account.

21 Okay, so that's what we mean by  
22 targeting a selector. You're using that selector,

1 you're providing that to the company, the  
2 provider, to get information on that account, or  
3 if it's a phone number on that phone number.

4 So that's when we say selector it's  
5 really an arcane term that people wouldn't  
6 understand, but it's really phone numbers, email  
7 addresses, things like that.

8 And targeting, it means that's the one  
9 you're trying to get. They may be in  
10 communication with other email addresses or other  
11 phone numbers and so forth. Those are not the  
12 targeted numbers or accounts, those are others  
13 that are incidentally acquired because they're on  
14 the other end of these communications. So target  
15 is the one you're going after.

16 And the statute requires that that  
17 target be a non-U.S. person located overseas. And  
18 so that's the foreignness determinations that  
19 we're talking about as we go through at great  
20 lengths to make sure that that target is in fact  
21 belongs to a non-U.S. person that is located  
22 overseas.

1           The other two questions?

2           MR. MEDINE:   Tasking or task.

3           MR. WIEGMANN:   Tasking is when you're  
4 going and saying, okay, I want to task this  
5 account means I want to collect information from  
6 that account.   So that's the collection.

7           MR. LITT:   You task a selector.

8           MR. WIEGMANN:   You task a selector.   So  
9 you're identifying, that's when you take that  
10 selector to the company and say this one's been  
11 approved.   You've concluded that it is, does  
12 belong to a non-U.S. person overseas, a terrorist,  
13 or a proliferator, or a cyber person, right,  
14 whoever it is, and then we go to the company and  
15 get the information.

16           MR. MEDINE:   And directives.

17           MR. WIEGMANN:   So directives are the  
18 orders that go to the companies that say they have  
19 to comply with the lawful tasking.   So that's the  
20 kind of more overarching order that goes to a  
21 company provider and says, okay, you have a legal  
22 obligation to comply with the taskings that are

1 given to you and here are the rules and  
2 everything. And that's all provided to them.

3 Is that a fair summary? I'll ask my  
4 colleagues to see if that is --

5 MR. DE: Keeping target as the  
6 statutory term. A term like selector is just an  
7 operational term to refer to something like an  
8 email or phone number, directive being the legal  
9 process by which that's effectuated, and tasking  
10 being the sort of internal government term for how  
11 you start the collection on a particular selector.

12 MR. MEDINE: Okay. So I guess building  
13 on that, what's the statutory rationale for about  
14 collections, because if the target is the email  
15 account or phone number, what is the justification  
16 for gathering communications between two persons,  
17 it may even be two U.S. persons who are discussing  
18 that phone number or that email address, but they  
19 are not themselves, there's no to or from that  
20 particular email address or particular phone  
21 number, why is that targeting that is permissible  
22 under the statute?

1           MR. WIEGMANN: Right. So the  
2 conclusion there again in a typical case, you're  
3 right, if you're targeting, you know, bad guy at  
4 Google.com you're targeting that person's  
5 accounts, their communications.

6           Why abouts collection is different is  
7 it's not necessarily communications to or from  
8 that bad guy but instead about that selector.

9           And so what the court has concluded is  
10 that when the statute uses the term targeting of a  
11 non-U.S. person overseas, targeting that selector  
12 qualifies under the statute for targeting that  
13 non-U.S. person overseas.

14           So it doesn't have to be targeting  
15 necessarily to or from, but can also target the  
16 communications that are about that particular  
17 selector.

18           MR. MEDINE: So that's a different  
19 meaning of target than earlier, which is where  
20 you're focusing on an account, now you're  
21 discussing targeting means discussions about that  
22 account.

1           MR. WIEGMANN: About that selector,  
2 correct.

3           MR. DE: It is always focused on that  
4 account, so I think the key is, the misperception  
5 that some may have that about collection is  
6 somehow about a key word or about the person that  
7 may be behind that account.

8           But all collections under Section 702,  
9 whether it's upstream abouts, which is a subset of  
10 upstream, or PRISM is all based on the selectors  
11 at issue.

12          MR. MEDINE: But does it raise -- oh, I  
13 see my time has expired so I'll --

14          MS. BRAND: I'm glad to see you're  
15 following your own rules.

16          Just to follow-up on that because  
17 that's a good line of inquiry, just to make sure  
18 that everyone understands. So you're saying that  
19 if someone is emailing about Rachel Brand or about  
20 explosives that would not be a permissible about  
21 query under your explanation?

22          MR. DE: So I would like to --

1 MS. BRAND: But you could, you could  
2 perhaps get it about Rachel Brand at --

3 MR. DE: Just so that, because I think  
4 this is an issue that all of us slip into,  
5 clarifying querying for collection.

6 So we are discussing now the collection  
7 of information. Abouts is a type of collection of  
8 information.

9 MS. BRAND: I'm sorry, right. Yes,  
10 that's right.

11 MR. DE: And so all collection of  
12 information is based, focused on selectors, not  
13 key words, as you just mentioned like terrorist,  
14 or like a generic name or things along those  
15 lines.

16 MS. BRAND: Okay.

17 MR. DE: And it's the same selectors  
18 that are used for the PRISM program that are also  
19 used for upstream collection. It's just a  
20 different way to effectuate the collection.

21 MS. BRAND: Okay. I think a large part  
22 of the function of these hearings is a public

1 education function and so I thought David's  
2 questions were great to explain the meaning of  
3 different terms, and I'm glad that you're willing  
4 to bear with us asking you some questions that  
5 we've already discussed with you in private. But  
6 I think it's helpful for everyone to understand  
7 what we're talking about.

8           And along those lines there was some  
9 discussion in Pat's questions about purging data  
10 that doesn't turn out to be foreign intelligence  
11 information.

12           But can you explain how on the front-  
13 end you implement the requirement that, not only  
14 that the target be a non-U.S. person reasonably  
15 believed to be abroad but that you expect to get  
16 foreign intelligence information through the  
17 collection, that's a separate statutory  
18 requirement. How do you go about ensuring that  
19 you're collecting that type of information?

20           MR. DE: Sure. So in our earlier  
21 discussion we skipped right to the foreignness  
22 determination, but that's actually a second step.

1 There has to be a reason one actually wants to  
2 collect intelligence from the particular selector  
3 in the first place.

4 And then one has to get to the fact, is  
5 this a type of collection permitted under the  
6 statute? So there has to be a valid foreign  
7 intelligence reason to do that collection.

8 But beyond that there has to be a valid  
9 foreign intelligence reason within the ambit of  
10 one of those certifications that the FISC approves  
11 annually. Those are certifications on things like  
12 counterterrorism, encountering WMDs, for example,  
13 weapons of mass destruction.

14 And so when an analyst needs to make a  
15 determination as to the valid foreign intelligence  
16 purpose for which they want to effectuate  
17 collections, they must also document that.

18 That is documented in a targeting  
19 rationale document in advance, ex ante, and those  
20 are always reviewed by the Justice Department and  
21 the Director of National Intelligence every 60  
22 days.

1                   MR. WIEGMANN: This is an important  
2 point for non-U.S. persons because people think  
3 about, okay, well once you've concluded that it's  
4 a non-U.S. person overseas then you can collect  
5 whatever you want. As Raj said, that's really not  
6 the case.

7                   It really is targeted, not only based  
8 on the identity of the person and the location of  
9 the person, but also that you're trying to get  
10 foreign intelligence. And so it's an important  
11 protection really in the statute that is designed  
12 for non-U.S. persons. It's not blanket collection  
13 of any non-U.S. person overseas. It's aimed at  
14 only those people who are foreign intelligence  
15 targets and you have reason to believe that going  
16 up on that account that I mentioned, bad guy at  
17 Google.com is going to give you back information,  
18 information that is foreign intelligence, like on  
19 cyber threats, on terrorists, on proliferation,  
20 whatever it might be.

21                   MS. BRAND: What can you tell us in an  
22 unclassified setting about the documentation of

1 foreign intelligence purpose or the oversight to  
2 ensure? I mean we've talked a little bit about  
3 that in past questions, but can you give us  
4 anything more specific?

5 MR. WIEGMANN: They do have to document  
6 that at NSA and every -- it's essentially called a  
7 tasking sheet, I think. And on that sheet they  
8 are documenting the foreign intelligence purpose  
9 that they are trying to pursue in going after a  
10 particular target.

11 And those are all reviewed together  
12 with the foreignness determination by the  
13 Department of Justice on a regular basis.

14 MS. BRAND: That's a separate sheet for  
15 every selector?

16 MR. WIEGMANN: For every single one,  
17 that's right.

18 MR. BAKER: And I think, at least with  
19 respect to FBI, I think the review that Raj  
20 mentioned earlier is done every 30 days on these  
21 tasking decisions, I guess you'd say, the foreign  
22 intelligence and the foreignness determination.

1           MR. DE: And if I could put that into  
2 the broader context of if the question really is  
3 getting at what is the process within which that  
4 happens, even before that happens we have training  
5 for analysts as to how they should document this  
6 material, we have audits of our databases, we have  
7 a comprehensive compliance program, we have spot  
8 checks, even within NSA prior to the 60 day  
9 reviews that are done by the Department of Justice  
10 and DNI, for us anyway.

11           There are also quarterly reports to the  
12 FISC on compliance with the program, semiannual  
13 reports to the FISC and to Congress, and annual  
14 inspectors general assessments, and as I  
15 mentioned, the annual certification process by the  
16 FISC.

17           So I think those decisions are, while  
18 they're one very granular aspect of the program,  
19 are conducted within the context of this broader  
20 regime.

21           MS. BRAND: Okay. And I see that my  
22 time just ran out.

1 MS. COLLINS COOK: I wanted to ask one  
2 additional question about abouts. Can you do  
3 about collection through PRISM?

4 MR. DE: No.

5 MS. COLLINS COOK: So it is limited to  
6 upstream collection?

7 MR. DE: Correct. PRISM is only  
8 collection to or from selectors.

9 MS. COLLINS COOK: I wanted to shift to  
10 a separate topic. One of the things that I have  
11 found both concerning and frustrating through the  
12 process of our evaluation of programs is how to  
13 both assess and articulate the efficacy of these  
14 programs.

15 And Mr. Litt, you had begun speaking  
16 about this in your prepared remarks. And I'd like  
17 to ask a couple of questions. One, how do you  
18 assess the efficacy of a particular program? How  
19 do you think we should be assessing the efficacy  
20 of a particular program?

21 And three, it's not really a question,  
22 it's more of a comment which is, please don't give

1 me a series of success stories and then say that's  
2 how you evaluate the efficacy of the program.

3 Because I think that's an initial response from  
4 the government often in response to a question,  
5 either from a body like ours or from the media.

6 But how do you assess the efficacy of  
7 the program, how periodically do you do so, and  
8 how would you encourage us to assess the efficacy?

9 MR. LITT: Well, let me start on that,  
10 and I want to start by saying that I completely  
11 agree with you that sort of individual success  
12 stories are not the way to evaluate a collection  
13 program and its utility.

14 The way you evaluate collection  
15 programs is going to depend in part on what the  
16 particular program is for.

17 In this case, we have in fact the  
18 Office of the Director of National Intelligence  
19 has attempted, part of our job is to try to  
20 determine that resources are effectively allocated  
21 within the intelligence community budget.

22 And so we have done studies to try to

1 look at, okay, what are our collection priorities,  
2 how much reporting is generated on these  
3 priorities, and where do those reports come from,  
4 what kind of collection source, to the extent we  
5 can identify that. And that's one of the ways  
6 that we've determined that Section 702 is  
7 relevant.

8 Another thing is just by looking at the  
9 sheer nature of the information that we get and  
10 its utility towards a whole variety of national  
11 priorities. That's a more impressionistic  
12 approach, and yet you can see time and again in  
13 important intelligence reports that are provided  
14 to policy makers that it's derived from Section  
15 702 collection.

16 So those are two ways that I would look  
17 at estimating the value of a particular  
18 collection.

19 MR. DE: If I could just add on to  
20 that. With respect to this program or any program  
21 I think intelligence professionals will tell you  
22 that any tool must be evaluated in the context of

1 the other tools in which it is utilized.

2 All intelligence tools are used in  
3 complementary fashion with one another and to  
4 isolate one particular tool and evaluate its  
5 effectiveness in isolation probably doesn't do us  
6 justice as to what's valuable and what's not.

7 It also depends on the type of tool.  
8 Different types of intelligence programs are used  
9 for different purposes. A program like Section  
10 702 is used for different purposes, for example,  
11 than a program, a metadata program with telephony  
12 metadata.

13 One may be a discovery tool to help  
14 pursue more specific collection and others may be  
15 used as in fact the specific collection that  
16 follows from that.

17 Third, there may be uses in which the  
18 PCLOB has recognized in terms of either directing  
19 the government in certain directions or at least  
20 helping to shape the focus of the government.

21 And so I think the absolute wrong  
22 question is how many plots did this tool stop.

1 And you can fill in the blank for what this tool  
2 refers to. But that is absolutely the wrong  
3 question, and I think it won't do us justice to  
4 figure out what we need as a government.

5 MS. COLLINS COOK: I have time I think  
6 for one last question. What is the view of the  
7 various agencies as to whether or not 702 is an  
8 effective and valuable program for the United  
9 States?

10 MR. BAKER: I think it is an effective  
11 and valuable program for the United States.

12 And if I could just address your last  
13 question as well. I mean I think you really, in  
14 order to understand whether it's effective and  
15 useful you have to think about what your goals are  
16 with respect to this particular program.

17 And the goals for this program, like  
18 many other collection programs are to obtain I  
19 think timely, accurate, informative foreign  
20 intelligence information about the capabilities,  
21 plans, intentions of foreign powers, agents,  
22 actors, and so on and so forth.

1                   And so I think really what you're  
2 talking really is, I think, developing a good  
3 metric to understand whether this program is worth  
4 all of the costs associated with it. And so I  
5 think you'd want to look at the amount of  
6 information that you, that we acquire, but also  
7 then obviously the quality of it. How good is it?  
8 And I think you can slice that a lot of different  
9 ways, as my colleagues have suggested.

10                   So I think that's really what I would  
11 recommend you be focused on. But you have to,  
12 because this is a broad-based foreign intelligence  
13 collection program you have to look at not only, I  
14 mean you have to look at counterterrorism but you  
15 have to look more broadly than that because this  
16 program is not limited just to counterterrorism.

17                   MR. DE: I agree it's definitely an  
18 effective program. I think the one point I should  
19 have added is that the review that Bob mentioned  
20 happening within the executive branch is not  
21 limited to the executive branch.

22                   Congress also reviews the effectiveness

1 of this program, as well as the 215 program. And  
2 I think that's part of the rationale behind having  
3 sunset clauses for various programs is that when  
4 those statutory provisions expire, as did the 215  
5 program twice in the last five years and as did  
6 702 in 2012, Congress undertakes, as it should, an  
7 evaluation of the effectiveness of the programs.

8 MR. LITT: So I completely agree that  
9 it is an effective and important program and I  
10 really want to emphasize the last point that Jim  
11 made, which is that this program should not be  
12 considered solely as a counterterrorism program.  
13 This program has utility, has significant and  
14 exceedingly important utility in areas outside of  
15 counterterrorism.

16 MR. DEMPSEY: Trying to clear up  
17 another issue in terms of the participation of  
18 service providers and the awareness of service  
19 providers in the 702 implementation, is 702  
20 implemented, all 702 implementation is done with  
21 the full knowledge and assistance of any company  
22 that, from which information is obtained, is that

1 correct?

2 MR. BAKER: Yes. The answer to that is  
3 yes.

4 MR. DEMPSEY: So early on in the debate  
5 there were some statements by companies who may or  
6 may not have been involved in the program saying,  
7 well, we've never heard of PRISM. But whether  
8 they ever heard of PRISM, any company that was,  
9 from whom information was being obtained under 702  
10 knew that it was being obtained?

11 MR. LITT: Correct.

12 MR. DE: PRISM is just an internal  
13 government term that as a result of the leaks  
14 became a public term. But collection under this  
15 program is done pursuant to compulsory legal  
16 process that any recipient company would have  
17 received.

18 MR. DEMPSEY: So they know that their  
19 data is being obtained because --

20 MR. DE: They would have received  
21 legal process in order to assist the government,  
22 yes.

1           MR. DEMPSEY: One thing I read in one  
2 of the statements is under 702 you could target  
3 entire countries or regions, is that correct?

4           MR. DE: So all collection under 702 is  
5 based on specific selectors, things like phone  
6 numbers or email addresses. It is not a bulk  
7 collection program.

8           MR. DEMPSEY: And a selector would not  
9 be an entire area code, for example?

10          MR. DE: Correct, correct.

11          MR. DEMPSEY: Going back to the  
12 constitutional -- oh, one other set of questions.

13                Even I've lost track now of what you've  
14 already said here versus what you've said  
15 elsewhere. But in terms of where you make a  
16 determination that a person is a non-U.S. person  
17 outside, reasonably believed to be outside the  
18 United States and then you later discover that  
19 that was good faith but wrong, the person was in  
20 United States, or the person was a U.S. person, do  
21 you track that, and what do you do when you  
22 discover that, and how often do you discover?

1 I'm not talking about the roamings, I'm  
2 talking just about you thought he was outside the  
3 United States and that was just wrong, or you  
4 thought he was a non-U.S. person and that was just  
5 wrong, how often does that occur?

6 MR. DE: So I'll defer to Brad on the  
7 sort of overarching review, but if I could just  
8 make a point about what happens. So yes, we keep  
9 track of every time new information comes to our  
10 attention to suggest that a prior intelligence  
11 evaluation was incorrect, even if it had met the  
12 legal standard.

13 Every such incident is a compliance  
14 matter that has to be reported to the FISC and  
15 ultimately in semiannual reports reported to the  
16 Congress.

17 And third, that sets in process a  
18 purging process by which information that should  
19 not have been collected if it had not met the  
20 legal standard needs to be purged from NSA  
21 systems.

22 I think Brad can speak to the level of

1 accuracy of those.

2 MR. BAKER: Just real quick, it's the  
3 same. The item is de-tasked and the information  
4 is purged.

5 MR. WIEGMANN: Right. So just to  
6 distinguish again between two different types of  
7 compliance issues. One is the roamer example that  
8 you mentioned.

9 So this is, let's say we're up on a  
10 cell phone that we believe belongs to a bad guy  
11 who's outside the United States, a foreign person,  
12 and then that person shows up in Chicago, when  
13 that happens we de-task that cell phone. That  
14 means we're no longer collecting the  
15 communications.

16 That's a compliance incident that's  
17 reported but it's not an erroneous determination.  
18 It's based on the movement of the individual.

19 So putting those cases aside, in cases  
20 where we just kind of get it wrong, we think the  
21 email account or the phone is located overseas but  
22 it turns out that that's wrong, or it turns out

1 that we think it's a non-U.S. person but it is a  
2 U.S. person, we do review every single one to see  
3 if that's the case.

4 And our review at Justice we decided to  
5 review, and as I mentioned earlier, we think it's  
6 less than one in a thousand cases where they make  
7 that determination erroneously.

8 MR. DE: And this probably bears worth  
9 repeating that the initial determination is not a  
10 once and done, so there is an affirmative  
11 obligation for analysts to reaffirm the  
12 foreignness determination on a periodic basis,  
13 which contributes to the ability to make sure that  
14 determination is in fact fresh and current, which  
15 of course contributes to the accuracy of that  
16 determination.

17 MR. DEMPSEY: Going to the  
18 constitutional issues, back to those for a second,  
19 the FISA court has determined, I mean they must  
20 they must determine every year that the program is  
21 being implemented consistent with the Fourth  
22 Amendment.

1           The very first time they determined  
2           that, there was an opinion that they issued. That  
3           one is, am I right, not yet public?

4           MR. WIEGMANN: I think that's correct.

5           MR. DEMPSEY: Isn't that a good  
6           candidate for declassification?

7           MR. LITT: We have a lot of good  
8           candidates for declassification.

9           MR. DEMPSEY: Yeah.

10          MR. LITT: In all seriousness there, we  
11          are, there are a lot of documents that we have  
12          that we are reviewing for declassification that  
13          include not only FISA court opinions but a whole  
14          variety of other documents.

15          MR. DEMPSEY: The FISA court in 2008  
16          when they last considered the constitutionality of  
17          a program, the predecessor to 702, the court  
18          issued a redacted but largely unclassified opinion  
19          conducting a relatively full Fourth Amendment  
20          analysis.

21          And there's been some Fourth Amendment  
22          analysis conducted in this situation, and if

1 you're sort of talking about, you know, the  
2 Rosetta Stone kind of Ur document, then the very  
3 first court opinion should have been the most  
4 fulsome explanation of the constitutionality of  
5 the program.

6 I think that -- I mean I hear Bob  
7 saying there's a lot of opinions out there, but to  
8 me this one seems to be one that would explicate  
9 at least one court's judgement on this because  
10 it's been the basis of -- I assume all the rest  
11 just said nothing has changed that would merit us  
12 to reconsider our very first judgement.

13 MR. WIEGMANN: So I mean I think it's  
14 among the opinions. We're committed to reviewing  
15 all the opinions of the FISA court to determine  
16 which ones can be declassified in redacted form.  
17 So I imagine this will be among those that are  
18 reviewed. So absolutely, I don't disagree. It'll  
19 be among the opinions that will be reviewed.

20 MR. DE: I just don't want to leave  
21 folks with any mysterious misimpression. I think  
22 the Board has access to everything and so one

1 shouldn't have to assume anything about subsequent  
2 opinions. The Board has in fact reviewed  
3 everything.

4           And so I just don't want -- what I  
5 think would be an unfortunate consequence would be  
6 for folks to take away the impression that there  
7 is a mysterious opinion that has some secret  
8 analysis, and I don't think that's the case. I  
9 don't think you intended to suggest that.

10           MR. MEDINE: The Board does have access  
11 to it but I think the question is whether the  
12 public should have access to it as part of the  
13 debate. But it's Judge Wald's --

14           MR. DEMPSEY: The public had access to  
15 the 2008 --

16           MR. MEDINE: It's Judge Wald's turn.

17           MR. WIEGMANN: So just one other thing  
18 I would add on that is that 702 collection has now  
19 been challenged by a number of criminal defendants  
20 when 702 information is being used against them in  
21 their cases. And so we'll be filing public briefs  
22 and we can expect some more decisions in that area

1 as well.

2 So that's another way that the  
3 constitutionality of 702 will now be on the public  
4 record, or I mean the opinions on it, and the  
5 briefs and everything will now be a matter of  
6 public record.

7 MR. MEDINE: Judge Wald.

8 MS. WALD: Okay. By whom and under  
9 what substantive criteria is the initial decision  
10 to use a U.S. person selector for searching the  
11 PRISM base made? I mean who decides let's do  
12 that? What's the substantive criteria on which  
13 they make it?

14 You don't have to go into the review  
15 process. I know the decision will be reviewed up  
16 and down. But how does that get made? What's the  
17 substantive basis?

18 MR. DE: So I can speak for NSA in  
19 particular.

20 MS. WALD: So just to clarify, that  
21 means if it goes to one of the other agencies, not  
22 NSA, CIA or FBI or something, they make their own

1 substantive decisions for querying?

2 MR. DE: Yes. The 702 program perhaps  
3 as a necessary predicate is one that all agencies  
4 operate on their own and have their own  
5 minimization procedures which would address topics  
6 like searches.

7 NSA's procedures in this regard, in  
8 this element have been made public and so the  
9 standard is that such a query needs to be  
10 reasonably likely to return foreign intelligence  
11 information.

12 MS. WALD: Be reasonably likely. And  
13 who is it made by initially?

14 MR. DE: It's made by the analyst.

15 MS. WALD: By the analyst who's working  
16 on that particular case, okay.

17 My other question is that the President  
18 did, if I understand his directive correctly,  
19 direct that there be some changes in the treatment  
20 of non-U.S. persons as to the limits on and  
21 retention of the data acquired incidentally to  
22 bring them more in line with those of U.S. persons

1 incidentally where there is no foreign  
2 intelligence value apparently.

3 Can you tell us a little bit more  
4 specifically if anything has been done in that  
5 regard or is being contemplated vis-a-vis 702?

6 MR. LITT: So I think first of all it's  
7 important to understand the point that somebody  
8 made, it may have been Brad made earlier, which is  
9 that there are already protections to some degree  
10 built into the system there. The protections for  
11 non-U.S. persons are not as great as those for  
12 U.S. persons because U.S. persons are protected by  
13 the Fourth Amendment.

14 But there is a requirement that we  
15 can't target a selector unless we have reason to  
16 believe it's of foreign intelligence value. And  
17 there's sort of a general principle that the  
18 intelligence agencies, their job is to collect,  
19 analyze, and disseminate foreign intelligence  
20 information, not random information.

21 I think what the President has directed  
22 is that we go back and look at our procedures and

1 not only with respect to 702, but with respect to  
2 signals intelligence in general, assess whether,  
3 the extent to which it's possible to provide  
4 limitations on collection, retention, and  
5 dissemination that more closely track those for  
6 U.S. persons.

7 For example, Executive Order 12333  
8 provides specific categories of personal  
9 information about U.S. persons that can  
10 appropriately be retained and disseminated.

11 There's a list of them in Executive  
12 Order 12333 and the President has asked that we  
13 assess whether we can apply those same sorts of  
14 rules to personal identifiable information of  
15 non-U.S. persons.

16 MS. WALD: Right now, just to follow-  
17 up, right now if you get incidental information  
18 about a foreign person in the course of targeting  
19 another foreign person and you look at it, do you  
20 use the same criteria and look at the same review  
21 and say, well, you know, he was just talking to  
22 his grandmother or something, there isn't any

1 foreign intelligence there, and you purge it?

2 MR. DE: Any time there is not foreign  
3 intelligence value to collection, by definition it  
4 would be purged.

5 But I think an important point to be  
6 made as you are articulating, Judge, is incidental  
7 collection, just to explain that term a little  
8 bit, all communications obviously have two ends.  
9 One end is the target and the other is presumably  
10 not a target. We don't know. One doesn't know ex  
11 ante.

12 And so by definition there will be  
13 incidental collection of non-U.S. persons, as well  
14 as U.S. persons. Historically, constitutional  
15 protections obviously have only applied to the  
16 U.S. person subset.

17 MS. WALD: I understand.

18 MR. BAKER: Can I just make a comment  
19 about that?

20 MS. WALD: We don't have time. Okay,  
21 quickly on the last time, I found it very  
22 provocative when you were answering Beth Cook's

1 question about if you're going to assess the  
2 efficacy of a program you have to look at it in  
3 terms of its efficacy and the holistic view of all  
4 of the programs.

5 I guess it's inevitable that I would  
6 ask the question, but how can anybody except you  
7 people do that, because so many of your programs,  
8 I think, are just unknown, even to the FISA court?  
9 They're not all FISA supervised, and certainly the  
10 outside world doesn't know about many of them. So  
11 you know, how in effect can an outside assessment  
12 be made?

13 MR. DE: If I could just address it  
14 since it was in response to my comment. Certainly  
15 I think I would not suggest that there should be a  
16 public evaluation of all intelligence programs. I  
17 think, for example, this Board as access to  
18 information about counterterrorism programs and so  
19 I would expect that any evaluation would be in the  
20 context of the other CT programs that you have the  
21 jurisdiction to review.

22 As with Congress, as I mentioned, they

1 reevaluate programs on a periodic basis. And I  
2 think the public record now indicates that there  
3 is a fairly robust exchange between the executive  
4 branch and the legislative branch on a variety of  
5 programs. And so I think that's where  
6 traditionally the evaluation has occurred.

7 MR. LITT: Yeah, I was just going to  
8 say that we've managed, we've set the balance  
9 between public disclosure and the need for secrecy  
10 by empowering the congressional intelligence  
11 committees. We're required by statute to keep  
12 them fully and currently informed of intelligence  
13 activities, and we do. They know about these  
14 programs and they have the opportunity to evaluate  
15 them, and they do.

16 In fact, they passed an Intelligence  
17 Authorization Act that includes a lengthy  
18 classified annex that is very prescriptive with  
19 respect both to reports that it requires of us and  
20 directions as to what we should, you know, where  
21 we should be spending our money.

22 So that's sort of the external

1 oversight and the way we've said, okay, well, we  
2 need to have oversight of these but they still  
3 need to remain classified.

4 MR. MEDINE: Did you want to finish? I  
5 don't know, you wanted to make a point earlier  
6 about foreign intelligence.

7 MR. BAKER: I had several points I  
8 wanted to make. But let me just on that real  
9 quick, I mean I think the, even the addition of  
10 Congress having oversight of it, the courts in  
11 certain circumstances, and then also obviously the  
12 President and all of the executive branch  
13 officials, we have an obligation to make sure that  
14 in addition to adherence to the law and taking  
15 care that the laws are faithfully executed, to  
16 spend our time and spend our money on programs  
17 that are effective and not be wasting our time on  
18 things that are not.

19 I mean that flows from the President to  
20 the DNI, the Attorney General, Director of the  
21 FBI, Director of NSA and so on. We should be  
22 focused on things that are useful and collecting

1 information that produces the kind of intelligence  
2 information that I was talking about before.

3           So the other comment that I just wanted  
4 to make was just with respect to FBI, our  
5 personnel only have access to the databases when  
6 they've received the proper training with  
7 appropriate oversight and operating consistent  
8 with the court-approved standard minimization  
9 procedures when they're doing their query  
10 activity.

11           MR. MEDINE: I wanted to shift to a  
12 different subject, which is attorney client  
13 privilege. There were some press reports a couple  
14 of weeks ago about collection of information that  
15 may involve attorney client communications.

16           But I want to focus particularly on the  
17 NSA minimization procedures, which I understand do  
18 exclude attorney client communications but only in  
19 a very narrow context where the client is under  
20 criminal indictment and the United States,  
21 basically on a federal criminal indictment.

22           That seems like a very narrow

1 interpretation of attorney client privilege. I  
2 wanted to see if that is the interpretation you  
3 apply in minimizing communications, and if it is  
4 what impact there would be if it was expanded to  
5 the more normally accepted definition of attorney  
6 client privilege, which is basically lawyers and  
7 clients consulting with each other?

8 MR. DE: So we have written a letter to  
9 the ABA and commented on it to the Board and to  
10 the public, I think it's a public letter now,  
11 which explicates in fuller detail than I probably  
12 can off the top of my head as to our procedures.

13 But I think one fundamental premise is  
14 that analysts are under an obligation to identify  
15 for the Office of General Counsel any time they  
16 encounter something that may be potentially  
17 privileged.

18 And I think as all of us who are  
19 lawyers, I think that probably encompasses every  
20 one up here on the stage, knows just because a  
21 communication is with a lawyer does not mean it is  
22 in fact a privileged communication. So it's

1 helpful to have a lawyer involved to determine  
2 that.

3           While I can't speak to any particular  
4 incident that may have been written about in the  
5 press I think there's a couple of big picture  
6 points that are worth making. One is our office  
7 has historically provided a range of advice to  
8 minimize to the extent possible the collection of  
9 attorney privileged material.

10           MR. MEDINE: That's privilege just  
11 where there's a criminal indictment or are you  
12 viewing privilege --

13           MR. DE: Beyond the criminal. So the  
14 point I'm trying to make is that while there may  
15 be a specific provision in the 702 procedures that  
16 addresses the criminal context, there's a reason  
17 why we ask analysts to consult counsel, because  
18 the advice can often be tailored to the specifics  
19 of a circumstance far outside the criminal realm,  
20 recognizing the import of attorney client  
21 privileged material in context, even outside the  
22 criminal context.

1           MR. MEDINE: I want to talk a little  
2 bit about reverse targeting where you target  
3 someone overseas potentially with the view of  
4 collecting information about a U.S. person in the  
5 United States, and that's impermissible.

6           There seems, again maybe this is a  
7 somewhat technical point, but there seems to be  
8 somewhat of a quirk in the statute. It says that  
9 you can target people reasonably believed to be  
10 outside the United States, you cannot reverse  
11 target someone outside the United States if the  
12 purpose is to target a particular known person  
13 reasonably believed to be in the United States.

14           Does that permit targeting a person  
15 outside the United States with the intent of  
16 gathering information about U.S. persons not in  
17 the United States?

18           MR. WIEGMANN: No.

19           MR. MEDINE: Why not?

20           MR. WIEGMANN: There's a separate  
21 provision that bars targeting U.S. persons outside  
22 the United States and so if you were doing that

1 and you are trying to target a U.S. person outside  
2 the United States, you couldn't do that.

3 MR. MEDINE: So you wouldn't do the  
4 reverse targeting procedure?

5 MR. WIEGMANN: I don't know if you  
6 would call that reverse targeting --

7 MR. DE: There is another statutory  
8 provision that prohibits the targeting of U.S.  
9 persons outside the U.S. under 702 --

10 MR. MEDINE: Even reverse targeting?  
11 Again, I'm not talking about -- I agree it's clear  
12 that you can't target a U.S. person outside of the  
13 United States, but what if I find a non-U.S.  
14 person that I know is in communication with a U.S.  
15 person who's also outside of the United States, is  
16 that permissible?

17 MR. WIEGMANN: No.

18 MR. DE: No.

19 MR. MEDINE: Because?

20 MR. WIEGMANN: Because you would be  
21 targeting, if your real purpose is to target that  
22 U.S. person, you're targeting that person.

1           MR. MEDINE: So reverse targeting in  
2 your view is the same as targeting? The  
3 prohibition on reverse targeting is co-existent  
4 with the prohibition on targeting?

5           MR. WIEGMANN: Well, I mean again I  
6 think of reverse targeting as a geographic issue  
7 essentially when you're targeting, let's say you  
8 have a legitimate target overseas but you really  
9 want the communications of a U.S. person or a  
10 non-U.S. person inside the United States, but the  
11 statute says you can't do that.

12          MR. MEDINE: Right, but --

13          MR. WIEGMANN: But as we were just  
14 explaining which is if you have a U.S. person that  
15 you're interested in overseas, you can't use 702  
16 to target them either and I don't think --

17          MR. MEDINE: Or reverse target them?

18          MR. WIEGMANN: What's that?

19          MR. MEDINE: If you know that that U.S.  
20 person is in communication with a non-U.S. person  
21 and both of them are overseas --

22          MR. WIEGMANN: Right.

1                   MR. MEDINE: Could you target the  
2 non-U.S. person to get the U.S. person's  
3 communications?

4                   MR. WIEGMANN: You couldn't do it for  
5 that purpose but if the non-U.S. person overseas  
6 is a valid foreign intelligence target that you're  
7 interested in their communications, sure, you can  
8 target that person. And the fact that they're  
9 incidentally communicating with a U.S. person  
10 overseas, that's okay. I wouldn't consider that  
11 reverse targeting.

12                   You still have to have that legitimate  
13 target. I don't know if that answers your  
14 question, but.

15                   MR. MEDINE: It did.

16                   MR. BAKER: I'm not going to read it  
17 now and take up your time, but take a look at  
18 Section 704 A 2, and that may address the kind of  
19 concern that you're focused on perhaps, but  
20 perhaps not.

21                   MR. MEDINE: Okay. I wanted to get  
22 back to efficacy. As you know, our charge is to

1 look at the balance between national security and  
2 privacy and civil liberties, and I think following  
3 up on Ms. Cook's question -- sorry, I'll just hold  
4 that until the next round.

5 MS. BRAND: I wanted to go back to  
6 upstream collection a little bit. I've seen some  
7 statements in the public domain about the volume  
8 of upstream collection vis-a-vis the volume of  
9 PRISM collection. What can you tell us in a  
10 public setting about that?

11 MR. DE: I think the best publicly  
12 available information is from the October 11th,  
13 2011 opinion that has now been declassified in  
14 which there was a rough estimate there, and  
15 forgive me for if it's not precise, but that about  
16 10 percent of collection is upstream. On the  
17 order of magnitude, I just don't know the exact  
18 number.

19 MS. BRAND: Okay. So you said in an  
20 earlier round of questioning that upstream,  
21 collection from upstream is retained for a shorter  
22 period of time than collection from PRISM and you

1 said that the reason for that distinction is that  
2 there's a potentially greater privacy concern with  
3 respect to upstream collection.

4 Can you elaborate on why, whether the  
5 additional privacy concerns that pertain to  
6 upstream.

7 MR. DE: Sure. And a lot of this is  
8 laid out in this court opinion that's now public.  
9 This is from the fall of 2011. I think because of  
10 the nature of abouts collections, which we have  
11 discussed, there is potentially a greater  
12 likelihood of implicating incidental U.S. person  
13 communication or inadvertently collecting wholly  
14 domestic communications that therefore must need  
15 to be purged.

16 And for a variety of circumstances the  
17 court evaluated the minimization procedures we had  
18 in place and as a consequence of that evaluation  
19 the government put forth a shorter retention  
20 period to be sure that the court could reach  
21 comfort with the compliance of those procedures  
22 with the Fourth Amendment. And so two years was

1 one element of the revised procedures that are now  
2 public.

3 MS. BRAND: So from what you just said  
4 that if using a legitimately tasked about term a  
5 wholly domestic communication is collected, it has  
6 to be purged?

7 MR. DE: If one recognizes it, yes. In  
8 fact, there's a --

9 MS. BRAND: Even if it has foreign  
10 intelligence information?

11 MR. DE: There are specifics. Off the  
12 top of my head I can't articulate all the  
13 particular exceptions in the minimization  
14 procedures but there are an elaborate set of  
15 detailed procedures that are now public that  
16 discuss how upstream collection must be treated in  
17 order to account for this concern.

18 And it has things like data must be  
19 segregated in certain ways where the risk of  
20 collecting a wholly domestic communication is  
21 higher, there's a shorter retention period.

22 Wholly domestic communications are not

1 permitted under the statute, and so therefore as a  
2 default rule, yes, it must be purged.

3 MS. BRAND: Jim, was there something  
4 you wanted to add?

5 Okay. I want to use the word  
6 incidental collection there again, and your  
7 definition earlier seemed to be that by incidental  
8 you mean, by incidental U.S. person collection you  
9 mean that the person on the other end of the phone  
10 from the non-U.S. person abroad is a U.S. person.  
11 That's your definition, right?

12 Is there another definition that you're  
13 aware of? Because you seem to be -- okay.

14 I think there's been some frustration  
15 with the use the term incidental in that context  
16 because it's not accidental, it's intentional.  
17 It's actually unavoidable. And so I just wanted  
18 to make sure that we're all on the same page, that  
19 by incidental you mean not accidental, not  
20 unintentional, but this is actually what we're  
21 doing.

22 MR. LITT: It is incidental to the

1 collection on the target. It is not accidental,  
2 it is not inadvertent. Incidental is the  
3 appropriate term for it.

4 MS. BRAND: Okay.

5 MR. DE: And I'd say that term I think  
6 has been used far beyond this program and  
7 historically, so there's no judgement intended.  
8 That is just a term.

9 MS. BRAND: Okay, okay. I'll hold the  
10 other questions for another round.

11 MS. COLLINS COOK: Just following up on  
12 David's question, I think it goes to a broader  
13 point which is that there is a perception that  
14 this statute is fairly complicated, there's got to  
15 be loopholes or idiosyncrasies in there somewhere.

16 But let me just ask you, would it be  
17 the view of the United States government that it  
18 is appropriate to use 702 to intentionally target  
19 U.S. persons, whether directly or through reverse  
20 targeting, whether they are inside the United  
21 States or outside the United States?

22 MR. LITT: No, definitely not.

1 MR. DE: No.

2 MR. LITT: That is not permissible.

3 MS. COLLINS COOK: I wanted to also  
4 follow up on a question about the abouts. And I  
5 apologize, again just for folks understanding that  
6 we spent six and a half hours talking with folks  
7 about just the oversight mechanisms in place and  
8 were unable to get through that entire  
9 conversation. So I apologize if you've said this  
10 before today.

11 The collection methods, procedures that  
12 you use with respect to abouts, those procedures,  
13 are they approved by the FISA court?

14 MR. DE: Yes.

15 MS. COLLINS COOK: Are those  
16 transparent to Congress?

17 MR. DE: Yes.

18 MS. COLLINS COOK: I think we haven't  
19 necessarily, we started to allude to this but can  
20 you talk a little bit about your impression of how  
21 the intel committees in particular view their  
22 obligations with respect to oversight of your

1 programs and whether you have found in your  
2 experience that to be pro forma or in any way  
3 lacking?

4 And let the record reflect a few, not  
5 quite eye rolls, but I think the response was, no,  
6 they have not found this to be pro forma in any  
7 way.

8 MR. LITT: I've been on this job now  
9 for getting on towards five years and I have found  
10 nothing about my interactions or our institutional  
11 interactions with the intelligence committees to  
12 be pro forma.

13 They have fairly substantial staffs  
14 which have a lot of experience. Some of them come  
15 from the community. They know, they dig very  
16 deeply into what we do. The DNI occasionally uses  
17 the term wire-brushing for the interactions that  
18 we have with the committees, so it's not a pro  
19 forma interaction in any way.

20 MR. DE: If I could add one point, on  
21 programs like 702 that we're talking about today  
22 for example, we all lived through the

1 reauthorization of Section 702 in 2012.

2           That process was not simply in  
3 connection with the intelligence committees, but I  
4 can remember numerous briefings where we would go  
5 up for a member, for all member briefings that the  
6 intelligence committees would host for the  
7 Congress.

8           So I don't want to leave the impression  
9 that it's only with the intelligence committees,  
10 particularly for a program like 702 that needs to  
11 be voted on by all members of Congress on the  
12 basis of a sunset clause.

13           MS. COLLINS COOK: I want to make sure  
14 that my colleagues have time for their last round  
15 of questions so I'll cede my time.

16           MR. DEMPSEY: Going back to the  
17 minimization procedures question, and specifically  
18 the incidental collection question, am I right  
19 that the rule is that whether the information is  
20 inadvertently collected, that is you were tasking  
21 on the wrong selector or some mistake was made and  
22 you got something that you didn't intend to get

1 that's inadvertent, or you were correctly  
2 targeting the right account and then you collected  
3 communications to or from a U.S. person that's  
4 incidental, the procedures say, minimization  
5 procedures, rules say that if you never discover  
6 that it was inadvertent and never discover that it  
7 was incidental, you never realized that it was a  
8 U.S. person collection, it's deleted after five  
9 years?

10           The basic rule is you keep it for five  
11 years, you keep everything for five years, two  
12 years on upstream, five years on PRISM, and then  
13 it gets deleted. That's the baseline rule, right?

14           MR. LITT: Correct.

15           MR. DEMPSEY: And then you on top of  
16 that the rule is that if then you, through  
17 analysis, through reviewing it that it was  
18 inadvertent or incidental collection on a U.S.  
19 person you must immediately purge? Bob's shaking  
20 his head.

21           MR. LITT: There's a difference in the  
22 way inadvertent and incidental, as you're using

1 those terms, are very different concepts.

2 Inadvertent refers to a collection that  
3 was not authorized by law. That is purged.

4 Incidental --

5 MR. DEMPSEY: Purged unless?

6 MR. LITT: Unless, as Raj mentioned,  
7 that there are certain exceptions. I'm certainly  
8 not able to recite them but they do exist. But  
9 they're fairly narrow.

10 Incidental is collection that is  
11 authorized by law. And at that point the rules  
12 relating to U.S. persons kick in and if you  
13 determine that it has no foreign intelligence  
14 value you purge it.

15 MR. DEMPSEY: Right, but I mean what's  
16 your response to the argument, well, fine, that  
17 just means that if you think it's valuable you can  
18 keep it, if you don't think it's valuable then you  
19 purge it?

20 MR. LITT: But it's lawfully collected.

21 MR. DEMPSEY: Fair enough. But you do,  
22 if it is of interest to you, you do keep it?

1           MR. LITT:  If it's of potential foreign  
2 intelligence value --

3           MR. DEMPSEY:  Minimization means --

4           MR. LITT:  If it can be useful to  
5 providing the intelligence that policy makers need  
6 or to protecting the nation against threats, then  
7 yes, we keep it for the required period.

8           MR. WIEGMANN:  So again, to make it  
9 more concrete, if it's a terrorist overseas, he is  
10 calling a number in the United States that belongs  
11 to a U.S. person, we want to keep that  
12 information.  It is incidental, the fact that  
13 we're getting the U.S. person number and we're  
14 targeting that non-U.S. person overseas, but he's  
15 calling Minneapolis, we want to keep that  
16 communication because it's of high interest to us.

17           MR. DE:  One point I would add is just  
18 that minimization refers to steps in the process,  
19 everything from collection to review to  
20 dissemination.  And so I think we're talking about  
21 one element here, and to retention.  And so there  
22 are different stages in the process.

1           To disseminate that information a  
2       certain threshold would have to be met and so  
3       forth.

4           MR. DEMPSEY: Yeah, I wish there were  
5       some way, I mean I know it's totally now embedded  
6       both in law and guideline and practice, but  
7       minimization means different things.

8           Minimization means keep it for five  
9       years and then delete it, minimization means don't  
10      disseminate identifying information, minimization  
11      means delete it unless it's intelligence  
12      information. Those are very different.

13          MR. LITT: Well, they all fall within  
14      the statutory definition of minimization  
15      essentially. I'm going to mangle it a little bit,  
16      but it's procedures that are designed to minimize  
17      the acquisition, retention, and dissemination of  
18      information about unconsenting United States  
19      persons consistent with the need to produce  
20      foreign intelligence information.

21          And so you're going to have different  
22      minimization rules based on the particular

1 missions of the agencies. You're going to have  
2 different minimization rules depending on the  
3 nature of the activity you're governing. You're  
4 going to have different minimization rules  
5 depending upon the nature of the information. But  
6 minimization is that entire category of rules.

7 MR. DEMPSEY: But it is a little bit of  
8 a circular definition which means different things  
9 in different contexts. Sometimes it means  
10 you've --

11 MR. LITT: I'm not sure I'd say  
12 circular but I would say it means different things  
13 in different contexts.

14 MR. WIEGMANN: It's a balance.

15 MR. BAKER: If I could just real quick  
16 just to emphasize, you know, as Bob was just  
17 alluding to, the FBI does have its own standard  
18 minimization procedures with respect to this type  
19 of activity. I assume you've had access to those.

20 So anyway, there's a lot on the table  
21 that we just talked about with respect to  
22 minimization, but I would direct you to those as

1 well in terms of understanding the FBI's role.

2 MR. MEDINE: Judge Wald.

3 MS. WALD: When a U.S. person  
4 information that's been, quote, incidentally  
5 acquired and kept for legitimate reasons or  
6 whatever in the base is disseminated to foreign  
7 governments, as is permitted under certain  
8 circumstances, it said that it's usually masked.

9 I think it would be useful for public  
10 consumption to know what the masking process  
11 entails, and in what circumstances it isn't  
12 masked, and whether or not the different agencies  
13 can use different criterias for masking or it's  
14 all centralized by Justice or the Attorney  
15 General's provision.

16 MR. DE: Well, I can speak just for  
17 masking generally at NSA, and abstracting from the  
18 second party issue for a moment, is substituting a  
19 generic phrase like U.S. person for the name of  
20 the U.S. person that is actually collected.

21 And that U.S. person is a legal term.  
22 Obviously that means an individual or it could

1 mean a U.S. company or firm.

2 I don't think there's a centralized  
3 process. That's how we do it at NSA. I think  
4 that's how other agencies do it as well.

5 MS. WALD: But different agencies  
6 decide how to interpret their own criteria as to  
7 what should be masked and what shouldn't?

8 MR. LITT: It's part of the, in the 702  
9 context it's part of their minimization  
10 procedures.

11 MS. WALD: Well, so what does that tell  
12 me? No, I mean specifically as to whether or not  
13 in what circumstances it's not masked, that's up  
14 to each agency, or not?

15 MR. LITT: Yeah, it's done on an agency  
16 by agency basis.

17 MR. WIEGMANN: But generally speaking,  
18 I think the minimization rules of each agency  
19 generally would not permit you to disseminate U.S.  
20 person information where that is not either  
21 foreign intelligence or necessary to understand  
22 that foreign intelligence. So in other words --

1 MR. DE: Or evidence of a crime.

2 MR. WIEGMANN: Or evidence of a crime  
3 for FBI.

4 So in other words, if I need to, if  
5 it's Joe Smith and his name is necessary if I'm  
6 passing it to that foreign government and it's key  
7 that they understand that it's Joe Smith because  
8 that's relevant to understanding what the threat  
9 is, or what the information is, let's say he's a  
10 cyber, malicious cyber hacker or whatever, and it  
11 was key to know the information, then you might  
12 pass Joe Smith's name.

13 If it was not, if it was incidentally  
14 in the communication but was not pertinent to the  
15 information you're trying to convey, then that  
16 would be deleted. It would just say U.S. person.  
17 It would be blocked out.

18 So they were in communication with, and  
19 it would just say U.S. person. So that's  
20 essentially how it works I think more or less in  
21 all the agencies. Is that a fair description,  
22 Raj?

1           MR. DE: Yeah, the basic parameters for  
2 FISA collection are articulated in the statute,  
3 the big principles of necessary to understand  
4 foreign intelligence or evidence of a crime. And  
5 then that's effectuated through the minimization  
6 procedures that each agency has. That's for 12333  
7 collection. It's articulated, as Bob mentioned,  
8 in 12333.

9           MS. WALD: With those last subpart,  
10 would those, just take NSA as an example, would  
11 those mask criteria also include foreigners,  
12 non-U.S. person's information?

13           I mean suppose the government of  
14 Romania asks some question which might require a  
15 Rumanian non-targeted person who's in your PRISM  
16 base, would these masking procedures, etcetera,  
17 apply there too or are they just for U.S. persons?

18           MR. DE: In today's rule, masking  
19 procedures are for U.S. persons because they are  
20 derivative of the constitutional requirement, the  
21 minimization procedures that need to conform with  
22 the constitutional parameters for U.S. persons.

1 MS. WALD: So it would be up to the  
2 agency to decide whether they thought it was right  
3 or wrong to give that information to a foreign  
4 government?

5 MR. DE: I think there's two points to  
6 mention. One is no information would ever be  
7 disseminated unless it had foreign intelligence  
8 value.

9 MS. WALD: No, I know.

10 MR. DE: That's the entire point of  
11 disseminating that information.

12 MS. WALD: But having made that  
13 decision in terms --

14 MR. DE: If I may continue. The second  
15 point is that I think what the President has  
16 directed the DNI to examine in the PPD is what  
17 protections could be extended to non-U.S. persons.  
18 That's the study.

19 MS. WALD: And that's what you're  
20 working on?

21 MR. DE: That's the issue we're  
22 evaluating now.

1           MR. BAKER: One quick comment though.  
2     If I'm not mistaken, if you look in 50 USC 1806,  
3     which is Title I of FISA but I think also applies  
4     to Section 702, it says, and I don't think it  
5     restricts it with respect to U.S. person or  
6     non-U.S. person, that no federal officer or  
7     employee can disclose, can use or disclose  
8     information at all except for a lawful purpose.

9           So the information could only be  
10    disclosed for a lawful purpose. And I believe  
11    that's across the board.

12           MS. WALD: I don't have anything more.

13           MS. COLLINS COOK: I wanted to make  
14    sure I understood though both Judge Wald's  
15    question and the response.

16           I understood her to be asking under  
17    what circumstances dissemination could be made to  
18    a foreign government.

19           Are there separate agreements and  
20    procedures that might govern in that instance or  
21    are analysts able to simply decide they would like  
22    to provide foreign intelligence information to

1 foreign governments?

2 MR. DE: At least our procedures, our  
3 publicly available procedures have provisions that  
4 address sharing with second party partners. I  
5 don't have at my fingertips the details, but I can  
6 certainly get back to you on that. But they are  
7 now public and articulate the circumstances under  
8 which information can be shared with second party  
9 partners. Those procedures are approved by the  
10 FISC annually.

11 MR. LITT: I think that the critical  
12 point is that these are part of the minimization  
13 procedures that have to be approved by the FISA  
14 court to the extent we're talking again about  
15 Section 702.

16 MS. WALD: The minimization procedures  
17 are only for U.S. persons, aren't they?

18 MR. LITT: Yes, that's right.

19 MS. WALD: But I was talking --

20 MR. LITT: But there are general rules  
21 about when we can share FISA information.

22 MR. MEDINE: All right. Well, I want

1 to thank the panel very much for spending a fair  
2 amount of time with us today and discussing these  
3 issues in a public setting and we appreciate it.

4 And we'll take a short break and then  
5 we'll resume at eleven o'clock with our second  
6 panel. Thank you.

7 (Off the record)

8 MR. MEDINE: We're now ready to begin  
9 our second panel, and we are very pleased to be  
10 joined by Laura Donohue, who's a Professor of Law  
11 at Georgetown University Law School, Jameel  
12 Jaffer, for a return engagement, Deputy Legal  
13 Director at the ACLU, Julian Ku, who's a Professor  
14 of Law at Hofstra University, and Rachel  
15 Levinson-Waldman, who is Counsel for Liberty and  
16 National Security Program at the Brennan Center  
17 for Justice, and each will make a brief set of  
18 remarks, if you want to start.

19 MS. DONOHUE: Sure. Thank you very  
20 much for the opportunity to be here today. I'm  
21 looking forward to the discussion on 702.

22 I'd like to confine my remarks to four

1 central areas, just my initial remarks, and raise  
2 statutory and constitutional concerns.

3 First is with regard to targeting. I'm  
4 particularly concerned about four areas here.

5 First is the inclusion of information about  
6 targets, and not just to or from targets.

7 Second is the burden of proof regarding  
8 whether somebody is a U.S. person or not.

9 Third is with regard to the burden of  
10 proof regarding the location of the individual.  
11 That is, if the NSA in either instance does not  
12 confirm, does not actually know where they are,  
13 the assumption that is built into the minimization  
14 and targeting is that it is neither a U.S. person,  
15 nor are they domestically located. And there is  
16 no affirmative duty for due diligence on the NSA  
17 to actually check their databases to find out if  
18 that individual is or is not a U.S. person and is  
19 or is not in the United States. And then the  
20 implications for the right to privacy.

21 In the second area on the post-  
22 targeting analysis, I'm particularly concerned

1 about the role of FISC, that it's severely  
2 circumscribed and that we're having warrantless  
3 searches.

4           So in the last panel we heard about  
5 that moment at which the information is obtained  
6 is not a search because it's foreign intelligence  
7 and there's an exception for the gathering of the  
8 intelligence.

9           But when information is then used for  
10 criminal prosecution, then at that point when the  
11 data is searched, if it were a case where if I  
12 were, say, speaking with a mobster in the United  
13 States and they happened to overhear incidental to  
14 my communications that I was engaged in other  
15 criminal activity, they would have to go to a  
16 court to obtain a warrant to then put a wiretap on  
17 my phone and listen to the content of my  
18 communications.

19           In this situation they don't do that  
20 and then they find that individuals are implicated  
21 in criminal activity and refer it for criminal  
22 prosecution.

1                   And I would be happy to address the  
2   2002 Foreign Intelligence Surveillance Court of  
3   review opinion that addressed this aspect, but it  
4   was with regard to Title I where there was  
5   probable cause that had already been established  
6   that the target in that case was a foreign power,  
7   an agent of a foreign power.

8                   In this particular case, the individual  
9   is not themselves the target of any investigation  
10  and so the prerequisite Fourth Amendment threshold  
11  has not been met.

12                  The third area is the retention and the  
13  --

14                  MS. COLLINS COOK: Can you slow down  
15  just a bit? I can't keep up. Thank you.

16                  MR. MEDINE: And we also have a court  
17  reporter who's probably her fingers are slowing  
18  down.

19                  MS. DONOHUE: Sorry, I beg your pardon.  
20  I realize we only have a few minutes, and I also  
21  have written remarks which I'll be submitting.

22                  MS. COLLINS COOK: I have reviewed

1     them. Thank you. I've reviewed what you've  
2     submitted thus far.

3             MS. DONOHUE: Right. So I will be  
4     submitting on these particular points following  
5     the hearing.

6             On the third area, the retention and  
7     the dissemination of data, and this came up with  
8     Judge Wald's question on the previous panel, there  
9     are a number of exceptions in terms of when the  
10    information itself has to be expunged.

11            The foreign intelligence information  
12    exception I would direct your attention to. It's  
13    not defined in either Section 702 specifically, or  
14    in the minimization or targeting procedures.

15            It is, however, defined in FISA to  
16    include any information that would be helpful for  
17    foreign affairs, which would include economic  
18    information, it would include political  
19    information, it would include a whole range of  
20    data.

21            The retention, dissemination for  
22    criminal prosecution, I've raised the Fourth

1 Amendment concerns. We're starting to see now in  
2 courts what's called parallel construction where  
3 individuals where information has come from  
4 intelligence agencies' programs, is then passed on  
5 to law enforcement, who then must create a  
6 parallel trail for probable cause, but the actual  
7 tip or initial indication of criminal activity  
8 came from intelligence.

9           And it essentially covers the traces  
10 that this initially arose within FISA or within  
11 Section 702, and I have increasing concerns,  
12 certainly as a scholarly matter, about the growth  
13 of parallel construction.

14           The client attorney privilege you had  
15 already mentioned in the last panel. That  
16 continues to be, I think, an area of some concern,  
17 not just because it's, not just in the post-  
18 indictment stage but in terms of all  
19 communications with attorneys prior to and in the  
20 context of the interception of content.

21           The retention of encrypted  
22 communications was not mentioned in the last

1 panel. All encrypted communications are retained  
2 according to NSA documents, as well as the  
3 technical barriers. If there are technical  
4 barriers they also will simply keep the  
5 information.

6 The other aspects of this have to do  
7 with multiple databases and CIA access, which I  
8 was surprised you didn't have the General Counsel  
9 of the CIA on the last panel. We now understand  
10 from NSA documents that the CIA has a separate set  
11 of minimization procedures and also uses Section  
12 702. And I think that's important to take a look  
13 at what those procedures are, both the targeting  
14 and the minimization.

15 Finally, the fourth area that I'd just  
16 like to raise is the First Amendment concerns that  
17 I have. As has been well-recognized in the  
18 judicial system, First and Fourth Amendments often  
19 travel hand in hand, especially in national  
20 security when political matters are on the line.

21 And in this particular instance not  
22 only do we have a general First Amendment concern

1 but we know that if individuals visit IP  
2 addresses, for instance, that have been associated  
3 with particular targets, then their  
4 correspondence, communication, emails, etcetera,  
5 and other information is also retained.

6 What if that IP address is Al Jazeera,  
7 let's say? What if that IP address happens to be  
8 a media or a news site that's been associated with  
9 a particular area of concern? Then I think there  
10 are also First Amendment implications that follow  
11 from that.

12 So in conclusion I'd be happy to talk  
13 in more detail about each of these areas, the  
14 targeting, the post-targeting analysis, the  
15 retention and dissemination of data, and the final  
16 First Amendment concerns.

17 MR. MEDINE: Thank you very much.

18 Mr. Jaffer.

19 MS. DONOHUE: Thanks.

20 MR. JAFFER: Thanks for the opportunity  
21 to appear before the Board.

22 The ACLU's view, as you already know,

1 is that Section 702 is unconstitutional. The  
2 statute violates the Fourth Amendment because it  
3 permits the government to conduct large scale,  
4 warrantless surveillance of Americans'  
5 international communications, communications in  
6 which Americans have a reasonable expectation of  
7 privacy.

8 In our view, the statute would be  
9 unconstitutional even if the warrant requirement  
10 didn't apply because the surveillance it  
11 authorizes is unreasonable.

12 As I discuss in more length in my  
13 written testimony, the statute lacks any of the  
14 indicia of reasonableness that the courts have  
15 looked to in upholding other surveillance  
16 statutes, including Title III and FISA.

17 But the point that I would like to  
18 emphasize today is that even leaving the  
19 constitutionality of the statute to the side, the  
20 government is claiming and exercising more  
21 authority than the statute actually gives it.

22 I say that for three reasons. First,

1 while the statute was intended to augment the  
2 government's authority to acquire international  
3 communications, the NSA's minimization and  
4 targeting procedures give the government broad  
5 authority to acquire purely domestic  
6 communications as well.

7           That's because the NSA's procedures  
8 allow the agency to presume that its targets are  
9 foreign, absent specific evidence to the contrary,  
10 and because the procedures don't require the  
11 government to destroy purely domestic  
12 communications obtained inadvertently.

13           Instead, they permit the agency to  
14 retain those communications when they're believed  
15 to contain foreign intelligence information, a  
16 phrase that is defined very broadly.

17           Second, while the statute was intended  
18 to give the government authority to acquire  
19 communications to and from the government's  
20 targets, the NSA's procedures also permit the  
21 government to obtain communications that are  
22 merely about those targets.

1           And that practice, in my view, finds no  
2 support in the language of the statute or in the  
3 statute's legislative history. But it's a  
4 practice that has profound implications for  
5 individual privacy.

6           In order to identify the communications  
7 that are about its targets, the government has to  
8 inspect every communication. To endorse the  
9 practice of about surveillance is to say that the  
10 government can surveil literally everyone, or at  
11 the very least that it can surveil every  
12 communication in and out of the country.

13           Finally, while Section 702 prohibits  
14 reverse targeting, the NSA's procedures authorize  
15 the government to conduct so-called back door  
16 searches, searches of communications already  
17 acquired under the FAA using selectors associated  
18 with particular known Americans.

19           Given the absence of any meaningful  
20 limitation on the NSA's authority to acquire  
21 international communications under Section 702,  
22 it's likely that the NSA's databases already

1 include the communications of millions of  
2 Americans.

3           The NSA's procedures allow the NSA to  
4 search through those communications and to conduct  
5 the kind of targeted investigations that in other  
6 contexts would be permitted only after a judicial  
7 finding of probable cause.

8           And if I have thirty more seconds I  
9 would like to make just one final point. Today  
10 we're focused on Section 702, but it's important  
11 to understand that Section 702 is merely one  
12 expression of a broader philosophy.

13           Yesterday the Washington Post reported  
14 that the NSA has built a surveillance system  
15 called MYSTIC capable of recording all of a  
16 country's phone calls, allowing the NSA to rewind  
17 and review conversations as long as a month after  
18 they take place.

19           MYSTIC is the logical endpoint of the  
20 arguments that the government is making here  
21 today. So the stakes and the conversation that  
22 we're having today are very high. It's very

1 difficult to believe that democratic freedom would  
2 survive for long in a system in which the  
3 government has a permanent record of every  
4 citizen's associations, movements, and  
5 communications. Thank you.

6 MR. MEDINE: Thank you. Professor Ku.

7 MR. KU: Thank you, and thanks also for  
8 the opportunity to appear before the Board today.

9 I just want to remind -- I have a  
10 different view I think from most of the panelists,  
11 and I apologize for not getting my remarks ahead  
12 of time.

13 I just want to remind the Board of two  
14 under-emphasized points of constitutional law that  
15 I think should frame our understanding of the U.S.  
16 government's surveillance practices under Section  
17 702.

18 I mean first, it is important to  
19 remember that Section 702 and FISA itself need to  
20 be interpreted and understood against the history,  
21 and tradition, and the background of the  
22 President's broad, inherent executive power under

1 the Constitution to conduct electronic  
2 surveillance of foreign governments and foreign  
3 agents, especially overseas.

4 Second, although we often speak loosely  
5 of the Fourth Amendment's limitations on this  
6 presidential foreign surveillance power, it's  
7 worth noting that courts have repeatedly upheld  
8 wide-ranging, warrantless U.S. government  
9 surveillance overseas, even of U.S. citizens.

10 So these two constitutional  
11 observations should frame any legal assessment of  
12 Section 702 and FISA in general.

13 If you keep in mind the background and  
14 where we're coming from rather than where we are,  
15 702 is not an ineffectual attempt to regulate  
16 lawless executive conduct, as the critics would  
17 have it.

18 In actuality, Section 702 almost  
19 certainly requires more limitations than are  
20 actually required by the Constitution and may  
21 even, although I'm not taking that position, but  
22 could in some circumstances encroach on the

1 President's foreign affairs powers to conduct  
2 foreign intelligence activities.

3           So let me just briefly elaborate on  
4 these two claims about constitutional law, which  
5 I'm sure some folks might disagree with, but this  
6 is not a dispute that U.S. presidents have long  
7 exercised the power under the Constitution to  
8 conduct foreign intelligence, and this  
9 uncontroversially flows from the President's role  
10 as the chief of foreign affairs under the  
11 Constitution. And almost every court considering  
12 the question has concluded that the President, has  
13 agreed that the President possesses an inherent  
14 constitutional authority to conduct foreign  
15 surveillance. And this is undisputed by any  
16 court.

17           In other words, there does not need to  
18 be statutory authorization for the President to  
19 engage in foreign surveillance.

20           Prior to the enactment of FISA in 1978,  
21 the executive branch claimed, and the courts did  
22 not dispute that it possessed a broad

1 constitutional power to conduct surveillance for  
2 foreign intelligence purposes, even inside the  
3 United States and usually without a warrant.

4           So prior to the enactment of Section  
5 702 and its predecessors, the executive branch  
6 claimed a constitutional power to conduct  
7 warrantless surveillance in foreign countries for  
8 foreign intelligence purposes, whether or not that  
9 surveillance included a U.S. citizen who was  
10 physically overseas.

11           So given this history I'd ask the Board  
12 to keep in mind that Section 702 and its  
13 predecessors placed more constraints on the  
14 executive branch's conduct of overseas foreign  
15 intelligence gathering than has ever been imposed  
16 in prior, in the past.

17           You might conclude that we need even  
18 more constraints, but we should not kid ourselves  
19 that existing constraints or even more constraints  
20 as proposed by some other folks, are consistent  
21 with historical practice and tradition and moves  
22 us further toward constraints.

1           As to my second point, I do not believe  
2 the Fourth Amendment imposes limitations on  
3 foreign intelligence as strict as those employed,  
4 imposed by Section 702. And let me just briefly  
5 explain the two reasons why.

6           First, it is very clear the Fourth  
7 Amendment does not apply to non-U.S. citizens and  
8 when they are outside the territory of the United  
9 States. And the Supreme Court confirmed this in  
10 the 1990 decision of The United State versus  
11 Verdugo-Urquidez.

12           So foreign citizens or the surveillance  
13 of foreign citizens outside of the United States  
14 is completely unconstrained by the Fourth  
15 Amendment.

16           Second, the courts have confirmed that  
17 it's highly unlikely the Fourth Amendment's  
18 warrant requirement applies to surveillance of  
19 U.S. citizens when they're outside of the United  
20 States, especially when the surveillance is  
21 conducted for foreign intelligence purposes.

22           No court in the United States has held

1 that a warrant is required for a search of a U.S.  
2 citizen when they are overseas if that search was  
3 conducted for foreign intelligence purposes.

4 Some courts like the second circuit  
5 have even held that no warrant is ever required  
6 for an overseas search, while others have relied  
7 on a broader foreign intelligence exception.

8 So there is further details here about  
9 the reasonableness, and courts have generally  
10 interpreted the Fourth Amendment's reasonableness  
11 requirement very generously in favor of the  
12 government when conducting overseas searches.

13 Again, in light of this long history  
14 and tradition of the United States conducting  
15 essentially unsupervised foreign intelligence  
16 gathering without any statutory authority, this is  
17 actually the tradition in the U.S. system prior to  
18 the enactment of FISA, then more recently Section  
19 702.

20 So just to conclude, if you look at  
21 Section 702, the government faces a complete ban  
22 on the intentional targeting of any United States

1 person reasonably believed to be outside of the  
2 United States. And there are other procedural  
3 mechanisms, as you know about.

4 But I don't believe that actually the  
5 Fourth Amendment would actually require if there  
6 was no Section 702, the Fourth Amendment would  
7 require that the government could not  
8 intentionally target a U.S. citizen overseas and  
9 their communications.

10 So let me just conclude, I believe  
11 Section 702 should be understood as a sensible  
12 compromise between privacy interests and the  
13 continuing need to conduct aggressive foreign  
14 intelligence gathering. Congress has given its  
15 blessing to broad-based overseas surveillance that  
16 was already occurring pursuant to the President's  
17 inherent constitutional power.

18 Congress has now imposed limitations on  
19 those activities that go beyond what I believe the  
20 Fourth Amendment requires, but I think that's a  
21 small price to pay, and many of us agree, to  
22 minimize privacy intrusions into Americans'

1 overseas communications. And the courts are  
2 involved to provide oversight.

3 This is the type of political  
4 compromise and cooperation between different  
5 parties and different branches of government that  
6 we always wish, we always say we want, and so I  
7 think we should applaud it rather than condemn it.

8 MR. MEDINE: Thank you.

9 Ms. Levinson-Waldman.

10 MS. LEVINSON-WALDMAN: Thank you, of  
11 course, for having me here. I have a few brief  
12 comments and then I hope we'll also have a chance  
13 at some point potentially to respond to comments  
14 that were made during the first panel or during  
15 this panel.

16 So I'm just going to focus briefly on  
17 two primary issues that are reflected in my  
18 written submission for now.

19 First, I know of course that the Board  
20 is particularly interested in whether this about  
21 collection complies with the letter or spirit of  
22 Section 702. And based on the structure of the

1 statute, we believe that it doesn't.

2 Briefly, there are two main  
3 restrictions reflected in Section 702 on the  
4 collection of communications. So that would be  
5 the first, the acquisition cannot target U.S.  
6 persons or persons known to be within the United  
7 States. This is a geographic or nationality and  
8 residence restriction.

9 And second, that the purpose of the  
10 acquisition must be to acquire foreign  
11 intelligence information. And that's basically a  
12 content restriction. What that means is that the  
13 content of the communications that can be picked  
14 up by electronic surveillance is regulated by the  
15 foreign intelligence restriction, while the class  
16 of people who are subject to electronic  
17 surveillance is regulated by the targeting  
18 restrictions.

19 When communications that are about a  
20 target are collected, we believe sort of the what  
21 and the who of the collection are conflated, and  
22 that that's contrary to the clear structure of the

1 statute.

2           And we know that the results of the  
3 collection, our intention with the foreign  
4 intelligence requirement of the statute, that is,  
5 if communications that merely mention certain  
6 targets are collected then we know that  
7 significant quantities of communications that  
8 contain no foreign intelligence information  
9 whatsoever are acquired, which would appear to  
10 undermine the significant purpose requirement in  
11 the statute.

12           And of course this has been confirmed  
13 in the 2011 FISC opinion that was referred to  
14 that's been declassified. We learn in fact that  
15 the NSA does acquire tens of thousands of wholly  
16 domestic communication in the course of conducting  
17 that about collection.

18           And so for those reasons we do think  
19 that the about collection is contrary to the  
20 meaning and the structure of the statute.

21           And second, let me briefly mention one  
22 of the main contributions I think the Board can

1 make as part of its review, and I think that some  
2 of these questions came out in the first panel,  
3 which is to shed more light on some of the ways  
4 that Section 702 is being used.

5           It appears that what we don't know  
6 about Section 702, certainly for the public, still  
7 outweighs or outnumbered what we do know.

8           Obviously there will always be things  
9 that will be properly classified and kept secret,  
10 but it seems that there are many unanswered  
11 questions that the Board is in a position to help  
12 answer, help shed some light on.

13           So those questions would include  
14 certainly questions about how targets, and  
15 selectors, and key words are used. Some of those  
16 were answered in the first panel, but I think some  
17 of those answers also raised more questions.

18           There has been the suggestion, the  
19 strong suggestion from the 2011 minimization  
20 procedures that all encrypted communications can  
21 be retained by virtue of their being encrypted,  
22 and finding out if that, in fact, is true. And if

1 not, if the PCLOB can obtain and provide  
2 additional information about that provision.

3 And finally, and this is something that  
4 Laura mentioned as well, that domestic  
5 communications can be shared with law enforcement  
6 agencies if they are reasonably believed to  
7 contain evidence of a crime that has been, is  
8 being, or is about to be committed.

9 In addition to raising, I think, a host  
10 of constitutional issues at the very least, and  
11 practical issues, one of the things that we don't  
12 know is whether there are minimum standards for  
13 how severe, for instance, such a crime has to be  
14 in order to share this information, which of  
15 course has been collected without a warrant.

16 So I hope that the answers to some of  
17 these questions also will come out during this  
18 process. Again, thank you for the opportunity to  
19 address the Board.

20 MR. MEDINE: Great, thank you very much  
21 for your opening statements. I'm going to ask you  
22 some questions but any panelist should feel free,

1 I may ask them to a specific person but anyone  
2 should feel free to jump in.

3 Professor Ku, you talked about the  
4 limited applicability of the Fourth Amendment to  
5 overseas collections, and maybe, and suggesting  
6 there's certainly no warrant requirement and a  
7 very generous reasonableness standard.

8 One question I have is the collections  
9 that we're talking about under 702 technically are  
10 happening in the United States. That is, the  
11 electronic communications provider is in the  
12 United States while admittedly the target is  
13 outside of the United States. Is that a  
14 distinction that you think has any constitutional  
15 significance?

16 MR. KU: That's a great question. I  
17 mean I think it reflects the difficulty of this,  
18 which is the technology is changing our, the way  
19 the Fourth Amendment was interpreted in some of  
20 these older cases, right.

21 So in the classic Fourth Amendment  
22 overseas case it was the guy searching through the

1 house or the apartment physically overseas of the  
2 U.S. citizen, or of the phone call that occurred  
3 on the foreign networks, right, in the foreign  
4 country.

5           Here we have this kind of weird  
6 situation where you have phone or communications  
7 sort of transiting through the United States. And  
8 I do agree that that might raise a harder Fourth  
9 Amendment issue, but I do think that the larger  
10 thing to keep in mind is that the geography  
11 matters because if there's a foreign person on the  
12 other side of the line, so to speak, that's I  
13 think in part the way the communication is an  
14 international communication. It has different  
15 implications for that perspective.

16           But I do agree that the Fourth  
17 Amendment, the territorial aspect of the Fourth  
18 Amendment would be less significant in that  
19 context.

20           I think the broader point though is  
21 that the courts have been very generous, both  
22 domestically and internationally about

1 surveillance conducted for foreign intelligence  
2 purposes.

3           So even, so the territorial distinction  
4 was something that FISA created, because prior to  
5 that I think FISA, the foreign intelligence  
6 gathering occurred both domestically and  
7 internationally, and the fact that it was for  
8 foreign intelligence was what mattered.

9           FISA has created this sort of  
10 territorial division, which I think is becoming  
11 less important with the changes in the types of  
12 communication we have.

13           MS. DONOHUE: If I may add to that.  
14 You know, Professor Ku brings up the exception for  
15 foreign intelligence gathering for purposes of  
16 surveillance. That's very different from the  
17 acquisition of information for purposes of  
18 prosecution. And here courts have very clearly  
19 ruled that even in cases of national security or  
20 domestic security, a warrant is required.

21           This is U.S. vs. U.S. District Court, a  
22 case handed down in 1972 in which there were three

1 individuals conspiring to bomb the CIA. And the  
2 court said that the executive branch, quoting  
3 Justice Brownell (phonetic) and others said the  
4 court -- the executive branch is not a  
5 disinterested neutral observer and cannot be put  
6 in the position of having to determine whether a  
7 search will be reasonable. They have to seek a  
8 third opinion on that.

9           In Katz as well in 1967, some of the  
10 justices in that case, Justice Byron White said,  
11 went beyond the decision and said basically we  
12 should not require a warrant procedure for the  
13 magistrate's judgement if the President of the  
14 United States, or his chief legal officer, the  
15 Attorney General, has considered the requirements  
16 of national security and authorized electronic  
17 surveillance as reasonable.

18           And other justices responded very  
19 angrily to that statement. Justice William  
20 Brennan, Justice William O. Douglas, they pointed  
21 out that there was a conflict of interest here.  
22 They said, look, neither the President nor the

1 Attorney General is a magistrate. In matters  
2 where they believe national security may be  
3 involved they are not detached, disinterested, and  
4 neutral as a court where the magistrate must be.

5 The Foreign Intelligence Surveillance  
6 Court of Review has also considered whether or not  
7 information obtained from FISA warrants could be  
8 used in the event of a prosecution.

9 In the case that brought down the wall  
10 in 2002, the court looked to Title I of FISA where  
11 probable cause had been established that an  
12 individual was a target, sorry, that the target  
13 was a foreign power or an agent of a foreign power  
14 and said in that case you have this review that  
15 has gone on specific to that target by the Foreign  
16 Intelligence Surveillance Court.

17 In Section 702, individuals who may be  
18 brought up on criminal charges are not themselves  
19 the target of any investigation. No probable  
20 cause has been established for their involvement  
21 as a foreign power or an agent of a foreign power.

22 Instead, once the content of

1 conversations are obtained, then the government  
2 may go through, analyze the information and look  
3 for evidence of criminal activity, which can then  
4 bring them into a courtroom to face criminal  
5 charges, and at no point is this warrant  
6 requirement, which the court has held for domestic  
7 security cases. So here you have a U.S. person on  
8 U.S. soil and the court has said in U.S. vs. U.S.  
9 District Court, you have to have a warrant in that  
10 situation.

11 So to use the veneer of, well, we're  
12 just collecting foreign intelligence and the  
13 executive branch has the right to do this under  
14 Article II, yes, perhaps the executive branch can  
15 gather intelligence but if there are criminal  
16 penalties associated then you also need to meet  
17 the requirements of the Fourth Amendment for U.S.  
18 persons.

19 MR. MEDINE: I'd like to give Professor  
20 Ku a chance to respond, although I can do it on my  
21 next round.

22 MR. KU: Okay. Well, I mean I'm not

1 going to go through all the cases. And I think  
2 that the way I understand this is the way you  
3 think about this is the foreign intelligence  
4 purpose, right. The foreign intelligence purpose  
5 has been sort of an important part about whether  
6 there's an exception to the warrant requirement,  
7 or if there's a foreign intelligence purpose,  
8 sometimes a primary purpose, or a purpose,  
9 depending on how you define it. And then there's  
10 the, whether that gives a question of  
11 reasonableness, where there's legitimate  
12 government interests that goes to the  
13 reasonableness.

14           The reason I'm emphasizing the  
15 significance of the foreign intelligence purpose  
16 aspect of this and the territorial aspect of this  
17 is because I do think it's relevant to analysis.

18           This is, in fact, what's going on here  
19 is a collision between our law enforcement and  
20 intelligence goals here, right. So the U.S.  
21 government is gathering a lot of information for  
22 foreign intelligence purposes. It's also using

1 sometimes that information.

2           Some of that information is, although  
3 not I think so far frequently, leaking into  
4 criminal prosecutions. But if we start from the  
5 perspective of foreign intelligence gathering,  
6 right, this is Article II, this is where we start,  
7 and this is something that's largely been  
8 unregulated.

9           What's changed is that the nature of  
10 communications have changed so that many of the  
11 communications that were essentially gathered  
12 unsupervised for foreign intelligence purposes are  
13 being sort of routed in a different way so that it  
14 falls within, technically speaking, what we might  
15 consider a different sort of format, which then  
16 looks more like a classic Fourth Amendment case.

17           But I think that the larger point I'm  
18 trying to emphasize here is that this is, there  
19 are real Fourth Amendment issues here with respect  
20 to law enforcement.

21           But this is also about foreign  
22 intelligence gathering. It's not just a total

1 sham. It's not as if the government is claiming  
2 here that this whole thing is a scheme in order  
3 just to gather information for criminal  
4 prosecution.

5           Essentially they're both interests here  
6 that are part of this analysis. And that legal  
7 analysis with respect to foreign intelligence  
8 gathering needs to be considered and it should  
9 frame our analysis of what's going on here as  
10 well.

11           MS. BRAND: Thank you. So it's a good  
12 segue actually what you said, Professor Ku,  
13 because I want to understand, Professor Donohue,  
14 what you were saying, and I may not have taken the  
15 best notes, so forgive me.

16           But walk me through the argument,  
17 because a second ago you said that you were making  
18 a distinction between collection for foreign  
19 intelligence purposes and I think you said  
20 collection that was focused, was for the purpose  
21 of prosecution.

22           So are you, is it your view that 702

1 collection is for the purpose of prosecution?

2 MS. DONOHUE: It's one of the two  
3 stated purposes for which the information can be  
4 retained once it is collected. So it can be --

5 MS. BRAND: But that's different. But  
6 I'm asking about you said collected for the  
7 purpose of prosecution, I thought. I mean what  
8 is, I guess what I'm trying to get at is, is this  
9 distinction between foreign intelligence purpose  
10 and criminal purpose relevant at the collection  
11 stage only, or at all stages, or what? Help me  
12 understand what you're talking about.

13 MS. DONOHUE: Yeah, so in the previous  
14 panel Brad addressed this point. He mentioned  
15 that in the context of it's the moment at which  
16 the information's obtained that a search occurs,  
17 right.

18 So if we do our Fourth Amendment  
19 analysis at that point, then the moment at which  
20 you're obtaining the wiretap evidence is the  
21 search, at which point you would require a warrant  
22 under these.

1           And I believe Professor Ku's point is,  
2 no, you don't need a warrant if it's for foreign  
3 intelligence purposes at the moment you acquire  
4 the information with the international nexus to  
5 it. And he's citing Verdugo-Urquidez where there  
6 was no nexus to the United States and a search  
7 occurred overseas.

8           The problem is in the case, and this  
9 gets back to my first point, which I apologize if  
10 I spoke too quickly at the beginning of the panel,  
11 which is with regard to the targeting. If it is  
12 not just information to or from the target, or  
13 held by the target, but any information about or  
14 relating to the target.

15           And here, it's interesting, I was a  
16 little bit confused by the earlier panel because  
17 according to the actual documents the NSA has  
18 released, the NSA can actually use computer  
19 selection terms and other information such as  
20 words, or phrases, or discriminators to scan  
21 content.

22           So if it can collect all of the

1 international communications and then scan the  
2 content of those communications, then I would  
3 argue that is a search for purposes of the Fourth  
4 Amendment at the point of collection.

5 MS. BRAND: But let me get to this  
6 distinction though between foreign intelligence  
7 and a criminal purpose, because 702 requires not  
8 only that the collection be a non-U.S. person  
9 abroad but also that there be a foreign  
10 intelligence purpose, that the information be  
11 reasonably believed to be, to collect foreign  
12 intelligence. I'm not quoting the statute.

13 But doesn't that statutory requirement  
14 suggest that it has to be for a foreign  
15 intelligence purpose? And it might also then  
16 collect evidence of a crime, which then there are  
17 procedures for what to do with that information.

18 But it seems like you're suggesting  
19 that you think that the collection itself is for a  
20 criminal purpose, and that's what sort of piqued  
21 my interest and I wanted to understand what you  
22 were saying there.

1           MS. DONOHUE: Sure. So to push on this  
2 a little bit, under FISA to be a foreign power one  
3 is not a U.S. person, right, one is a foreign  
4 power or an agent of a foreign power. Not all of  
5 the agents of a foreign power require criminal  
6 showings, but many of them do.

7           So to say that this is purely a foreign  
8 intelligence purpose when an individual can be  
9 targeted based on being either a foreign power or  
10 an agent of a foreign power, in which case there  
11 is criminal activity involved and there may be the  
12 element of criminality from the outset. So it's  
13 not as though criminality is not an aspect of the  
14 foreign intelligence gathering generally.

15           MS. BRAND: Professor Ku, do you have  
16 -- Jameel, it looks like you wanted to respond.

17           MR. JAFFER: Well, I was just going to  
18 speak to the foreign intelligence exception more  
19 generally, if you want to pursue this.

20           MS. BRAND: Go ahead. Go ahead.

21           MR. JAFFER: Well, so I just want to  
22 caution the Board about starting from the premise

1 that there is in fact a foreign intelligence  
2 exception to the warrant requirement. The cases  
3 in which courts have held that there is such an  
4 exception predate FISA. There's arguably one  
5 exception to that, but the vast majority of them  
6 predate FISA.

7           And so their rationale has been  
8 undermined by practice under FISA over the last  
9 thirty-five years. The rationale for those cases  
10 was in large part that the courts might not be  
11 capable of overseeing collection or surveillance  
12 for foreign intelligence purposes. But the courts  
13 have been doing precisely that now since 1978.

14           But even if you accept that there is in  
15 fact a foreign intelligence exception to the  
16 warrant requirement, you have to ask the question  
17 of how broad that exception is.

18           And all of those cases, those pre-FISA  
19 cases, involve cases involved situations in which  
20 there was probable cause to believe that the  
21 target was a foreign agent, the surveillance was  
22 approved personally by the President or the

1 Attorney General, and the primary purpose of the  
2 surveillance was to gather foreign intelligence  
3 information.

4 And Section 702 doesn't include any of  
5 those requirements. So no court has ever approved  
6 a foreign intelligence exception to the warrant  
7 requirement that is broad enough to read Section  
8 702. Section 702 is a broader statute than any  
9 foreign intelligence exception recognized so far  
10 would allow.

11 I think that it may also be important  
12 to emphasize that concluding that the warrant  
13 requirement applies doesn't mean that the  
14 government has to get a warrant before surveilling  
15 legitimate foreign targets. It doesn't mean that  
16 in order to surveil, you know, some suspected  
17 terrorist outside the United States the government  
18 necessarily needs to get a warrant.

19 But at the very least it means that the  
20 government needs to take reasonable measures to  
21 avoid acquiring Americans' communications without  
22 warrants.

1           It means it has to not acquire them in  
2 the first place where it cannot acquire them.

3           When it does acquire them, it has to  
4 destroy the communications that it acquires  
5 relating to U.S. persons.

6           And when in narrow exceptions it  
7 retains those communications, there should be a  
8 back-end warrant requirement so the government  
9 doesn't access Americans' communications without a  
10 warrant. That's what compliance with the warrant  
11 clause would mean.

12           MR. MEDINE: Ms. Cook.

13           MS. COLLINS COOK: So thank you all for  
14 coming. I find these panels to be incredibly  
15 helpful and informative.

16           Ms. Donohue, I would like to --  
17 Professor Donohue, I apologize, I'd like to  
18 follow-up on something you mentioned at the very  
19 end of your opening remarks, and that's your  
20 position that 702 raises First Amendment concerns.

21           I think it's clear from my previous  
22 separate statement on our 215 report that I don't

1 necessarily approach the First Amendment analysis  
2 the same way, but what I would find helpful from  
3 you is if you could just describe your approach to  
4 when the First Amendment would be implicated, when  
5 concerns arise, and when something would be  
6 unconstitutional based on First Amendment  
7 concerns.

8           So for example, would a traditional  
9 wiretap raise First Amendment concerns, and would  
10 it potentially be unconstitutional under First  
11 Amendment concerns?

12           Would a traditional grand jury subpoena  
13 for bank records or credit card statements that  
14 could reveal payments to lawyers or payments to  
15 various charities or associations, would that  
16 raise First Amendment concerns? Would it be  
17 unconstitutional under the First Amendment?

18           So if you could just walk me through on  
19 the spectrum where you're finding concerns and  
20 where you're finding violations.

21           MS. DONOHUE: Sure. And just to return  
22 back to Ms. Brand's point, I agree with Jameel on

1 the analysis about what point it would kick in for  
2 a warrant requirement is the point at which it's  
3 either about the information, because I feel like  
4 I didn't quite answer what you were asking me and  
5 I want to make sure that I do, I answer it.

6 It's the point at which you're getting  
7 information about that particular individual,  
8 which is a different target, and then you analyze  
9 that information, then at that point I would  
10 believe that the Fourth Amendment warrant  
11 requirement would apply.

12 Okay, so in response to the First  
13 Amendment question, so the courts have recognized  
14 that there is a close link between the First and  
15 the Fourth Amendment. And I frequently find  
16 whether it's in remote biometric identification  
17 systems in view of public space and facial  
18 identification, you know, that there is a First  
19 Amendment context there as well. So it tends to  
20 be in the shadows in the room.

21 In this particular context, the way  
22 that I see it present is with regard to the target

1 that is in the statute. It's very clear that the  
2 target cannot be selected --

3 MS. COLLINS COOK: I'm sorry, can you  
4 actually answer the question that I had posed,  
5 which was, for example, starting with a  
6 traditional --

7 MS. DONOHUE: Oh, yeah, so I do not see  
8 a traditional wiretap as implicating First  
9 Amendment. I do not see --

10 MS. COLLINS COOK: Why?

11 MS. DONOHUE: Because --

12 MS. COLLINS COOK: Even though it  
13 could, for example, reveal the fact that I belong  
14 to the ACLU, or I have called my attorney, or I'm  
15 discussing, you know, private contents and  
16 communications. So why not?

17 MS. DONOHUE: Because there's a  
18 balancing that occurs with regard to the element,  
19 in this case of probable cause that you have  
20 committed, are committing, or are about to commit  
21 a crime under Title III, in which case having gone  
22 before a neutral, disinterested magistrate, a law

1 enforcement officer says, oh, no, I suspect that  
2 Professor Donohue is engaged in this bad activity.  
3 And I think that that balancing test basically  
4 takes that situation out of a First Amendment  
5 context.

6 MS. COLLINS COOK: So let's take a  
7 grand jury, and then a pen register trap and  
8 trace. So a pen register trap trace, there's  
9 definitely no determination, no probable cause.  
10 So does a traditional pen register trap trace,  
11 which would reveal potential phone calls to the  
12 ACLU, to my lawyer, very private, the existence of  
13 potentially private conversations, does that  
14 violate the First Amendment?

15 MS. DONOHUE: Again, with prior  
16 judicial approval and review, no.

17 MS. COLLINS COOK: Okay. So let's take  
18 a grand jury subpoena which can be issued by a  
19 prosecutor. So in the absence of beforehand  
20 judicial review, does that violate the First  
21 Amendment?

22 MS. DONOHUE: No. I would say --

1 MS. COLLINS COOK: So what's the factor

2 --

3 MS. DONOHUE: Well, it's the same for  
4 administrative warrants, I would say in the case  
5 of administrative warrants. Here's where the  
6 tipping point is for me with PRTT, let's take  
7 Section 215 as kind of a bulk metadata collection  
8 program, or Section, what is it, 402, right, for  
9 these bulk collections of pen register trap and  
10 trace type information.

11 When you have the bulk collection of  
12 information in a way that changes the political  
13 discourse in society, then I think you have a  
14 First Amendment question that arises.

15 MS. COLLINS COOK: Okay. So is if  
16 there is a perception that there is a change in  
17 political discourse, then you have a concern about  
18 a First Amendment? It's not necessarily prior  
19 judicial review, particularized probable cause?

20 I'm just struggling to understand, you  
21 know, at what point there's a First Amendment  
22 implication and at what point there's a First

1 Amendment violation, because to me, I think it's a  
2 bit of a sea change to look at either traditional  
3 or really these FISA authorities as violating the  
4 First Amendment. I do think that that's a fairly  
5 novel approach.

6 MR. JAFFER: But to be fair -- to be  
7 fair, the distinction between individualized  
8 surveillance and bulk surveillance is also a bit  
9 of a sea change. And so I think the question is  
10 whether the bulk surveillance, the fact that the  
11 government is now engaged in bulk surveillance, I  
12 mean I understand that there's some dispute over  
13 the vocabulary, but the fact that the government  
14 is engaged in bulk collection or bulk acquisition  
15 of this information makes the First Amendment  
16 relevant in a way that it perhaps wasn't relevant  
17 in the context of individualized surveillance of  
18 the kinds that you were describing.

19 I mean I think that your question  
20 perhaps goes more broadly to the question of  
21 incidental overhears, you know. When the  
22 government defends Section 702, one of the

1 government's defenses is that all of this  
2 information is, about Americans is overheard  
3 incidentally.

4           You know, I go into this in a little  
5 more detail in my written submission, but I don't  
6 think it's fair to call this kind of collection  
7 incidental in any conventional use of the term.  
8 The collection of Americans' information is  
9 entirely foreseeable, and in fact, it was the  
10 purpose of the statute.

11           If you look at the statements that  
12 administration, then Bush administration officials  
13 made to justify the statute or to advocate for the  
14 statute, they were quite forthright about the  
15 purpose of the statute. And the purpose in their  
16 view was to give the government broader authority  
17 to collect information, collect communications  
18 between people outside the United States, and  
19 people inside the United States.

20           And obviously there's no illegitimacy  
21 to the government's interest in collecting those  
22 communications. The question is whether there are

1 sufficient safeguards in place, but that's why I  
2 say that incidental is probably the wrong word.

3 But if the government is relying on the  
4 incidental overhear cases from the Fourth  
5 Amendment context, those cases were, involved very  
6 different contexts. Those were cases in which the  
7 surveillance was individualized. It was based on  
8 a probable cause warrant.

9 The scale of the surveillance of the  
10 incidental collection was much different. And the  
11 fact that there was judicial oversight at the  
12 front-end provided a kind of protection for  
13 incidentally overheard people that doesn't exist  
14 under a statute like 702.

15 MR. MEDINE: Let's give Jim the chance  
16 to ask some questions, then we can come around.

17 MS. DONOHUE: Okay.

18 MR. DEMPSEY: Thanks. Thanks to the  
19 witnesses.

20 A question for Jameel and for Rachel on  
21 the abouts. What actually is, quoting the words  
22 of the statute, what is the strongest textual

1 argument against about surveillance?

2           Because the statute says the targeting  
3 of persons, never really refers to even the  
4 collection of communications or interception,  
5 etcetera, so if you're collecting something about  
6 somebody, isn't that almost paradigmatically  
7 targeting the person? Where's the text?

8           MS. LEVINSON-WALDMAN: I mean I think  
9 one of the -- right, there's obviously ambiguity  
10 in the statute in part, and this is one the things  
11 that I mentioned in the written submission is that  
12 target isn't defined.

13           And I have to say some of the answers  
14 in the first panel, which answered some questions  
15 about target and selectors, I think also opened up  
16 new questions.

17           I do think the strongest statutory  
18 argument, literally looking at the language, is  
19 what the statute talks about.

20           So it says here, literally just looking  
21 at 1881 A, subpart A, Attorney General and  
22 Director of National Intelligence may authorize

1 jointly the targeting of persons reasonably  
2 believed to be outside the United States to  
3 acquire foreign intelligence information.

4           So as I say, you sort of see  
5 implicitly, but I think you do see implicitly  
6 these two sort of halves of the targeting  
7 requirement, the foreign intelligence requirement  
8 and this kind of nationality and geographic  
9 restriction, and that when what you're doing is  
10 collecting about communications, what you're doing  
11 is kind of adding together, you're kind of  
12 conflating, you're morphing together these  
13 different parts of the statute so that the  
14 targeting has usually been literally thinking  
15 about the facility that's being used --

16           MR. DEMPSEY: Excuse me. The  
17 government has determined that a person is outside  
18 the United States and that collecting information  
19 about that person will yield foreign intelligence.

20           MS. LEVINSON-WALDMAN: Well, but I  
21 think that may be what's suggested by the about  
22 collection, but I think the foreign intelligence

1 determination is a separate one, right.

2           The government identifies these targets  
3 or selectors which have generally been to or from.  
4 And in fact we know, especially from Judge Bates's  
5 opinion that thousands, tens of thousands of  
6 communications are collected using the about  
7 targeting, the about collection, that are wholly  
8 domestic, that have no foreign intelligence value,  
9 which I think undermines an argument that there  
10 has been some determination of foreign  
11 intelligence value there, because to some extent  
12 the results are sort of speaking for themselves.

13           MR. DEMPSEY: Because then you would be  
14 questioning the legitimacy of the to and froms  
15 because they only do abouts about people that they  
16 also do to and froms, so you can't say that the  
17 foreign intelligence determination of the abouts  
18 is illegitimate because then you call into  
19 question the to and from.

20           MS. LEVINSON-WALDMAN: Well, but I  
21 think the to and from is pretty clearly  
22 contemplated by the statute, right? You target a

1 person, you are trying to find communications to  
2 or from them, understanding that those will have  
3 foreign intelligence value.

4 MR. DEMPSEY: Let me go to Jameel.  
5 Jameel, what is the best textual argument against  
6 abouts?

7 MR. JAFFER: Right. Well, let me first  
8 I think agree with what I think Rachel was saying  
9 at the outset, which is that the statute I don't  
10 think explicitly forecloses about surveillance or  
11 explicitly authorizes about surveillance.

12 But I think a fair assessment of the  
13 statutory structure and some of the statutory text  
14 leads to the conclusion that about surveillance  
15 was not contemplated by Congress. And I'll answer  
16 your question.

17 MR. DEMPSEY: The text, yeah.

18 MR. JAFFER: So here are a few aspects  
19 of the statute that I think show that Congress was  
20 contemplating, that the target would, himself or  
21 herself, be the person whose communications were  
22 acquired.

1           First, a definition of electronic  
2 surveillance. It says the acquisition of the  
3 contents of any wire --

4           MR. DEMPSEY: This is not electronic  
5 surveillance. 702 explicitly does not cover  
6 electronic surveillance.

7           MR. JAFFER: Well, I think that the  
8 point I'm making is relevant nonetheless.

9           MR. DEMPSEY: Electronic surveillance  
10 definition is irrelevant to 702. It is not -- 702  
11 does not regulate electronic surveillance.

12           MR. JAFFER: I think the point that I'm  
13 trying to make is just that the entire statutory  
14 scheme, both FISA and the FAA, contemplate that  
15 the person who is the target will be the person  
16 whose communications are actually acquired.

17           If you look at the definition of  
18 aggrieved person, for example, which does apply in  
19 the FAA context, aggrieved person to implicitly  
20 contemplates that the person who will be raising  
21 the claim as an aggrieved person is a person whose  
22 communications are actually acquired.

1           And in fact, if you conclude otherwise  
2 what you are concluding is that the target would  
3 be an aggrieved person even if his or her  
4 communications weren't acquired, which I think is  
5 a nonsensical conclusion and one that the  
6 government itself would reject.

7           But I think it follows from accepting  
8 that about surveillance is contemplated by the  
9 statute.

10           And if I could just make a sort of  
11 broader point about about surveillance, we have  
12 sort of combed through the legislative history for  
13 discussions of this kind of surveillance, and it's  
14 possible we overlooked something, but we have not  
15 found any exchange in the legislative history  
16 around the FAA that suggests that Congress was  
17 contemplating about surveillance.

18           To the contrary, when people discuss,  
19 when legislators discuss the kind of surveillance  
20 that would take place under the statute, they  
21 discuss surveillance of the target.

22           And even on the government panel this

1 morning one of the panelists used the example, bad  
2 guy at Google.com, you know, which again is  
3 suggesting that the surveillance that's going on  
4 is of the target himself or herself.

5 And in defending the statute before the  
6 Supreme Court, the Solicitor General and the  
7 Justice Department more generally characterized  
8 the statute as one that allowed the government to  
9 collect targets' communications.

10 So you know, I think that this is an  
11 entirely a foreign concept, foreign to the  
12 legislative history and foreign to the text of the  
13 statute.

14 MR. MEDINE: Thank you. Judge Wald.

15 MS. WALD: Let me pick up on the about  
16 thing and pose one of those terrible  
17 hypotheticals. If you had a to and from, you had  
18 a targeted, a legitimately targeted person and in  
19 the process of collecting information you got, you  
20 came across this email between, I'll be facetious  
21 a bit, the grandmother of one of them to the  
22 grandmother of somebody else saying something

1 along the lines of, my grandson was talking to me  
2 and he was telling me all about this wonderful  
3 service he did by plotting, I'm using an extreme,  
4 plotting to blow up a facility kind of thing, I  
5 mean how would you take care of that situation  
6 where you had it between two people who are not  
7 the to and froms? You wouldn't ignore it, would  
8 you, or would you? I mean how would you handle  
9 that if you had no abouts?

10 MS. DONOHUE: I'm not sure whom that's  
11 directed to.

12 MS. WALD: I don't care.

13 MR. MEDINE: Who would you like it  
14 directed to?

15 MS. WALD: What?

16 MR. MEDINE: Who are you asking?

17 MS. WALD: Well, the two people who've  
18 talked about what about abouts, Mr. Jaffer and  
19 Ms. Levinson-Waldman, I think.

20 MR. JAFFER: Well, I'm not a hundred  
21 percent sure I understand the question. The  
22 question is, you know, if you were conducting

1 about surveillance and you come across evidence of  
2 a terrorist plot, do you really expect them to  
3 ignore it? Then no, I don't, you know.

4 But that's like asking, you know, if  
5 the government breaks into a home  
6 unconstitutionally and finds evidence of a  
7 terrorist plot, do I expect them to ignore it? I  
8 don't.

9 But we still need to ask the question  
10 what are the proper limits on the government's  
11 surveillance authority in the first place, and I  
12 think that we need to draw those limits in a way  
13 that's consistent with the Constitution.

14 I'm not sure that I'm answering your  
15 question.

16 MS. WALD: Well, you are except that  
17 I'm puzzled, too. I'm not sure I know the answer  
18 where, as I say, you had -- maybe that's an  
19 extreme example about where they have a plot, but  
20 where there's actually some foreign intelligence  
21 information which even everybody would agree had  
22 some relevance to a legitimately targeted

1 individual, and it's right there, and it's picked  
2 up.

3 MS. LEVINSON-WALDMAN: Then I think I  
4 would echo Jameel's points to some extent and sort  
5 of elaborate to say that I do think that there are  
6 always hypotheticals, presumably for any of these  
7 programs, for Section 702, for Section 215, for  
8 other collection programs that are going on where  
9 there could be some piece of information out there  
10 that might be useful that would be collected by a  
11 program.

12 I think it's dangerous to build  
13 surveillance programs and to think about the  
14 constitutionality and the practicality based on  
15 hypotheticals, and especially when we know that  
16 there is significant over-collection that occurs  
17 and significant collection of Americans'  
18 communications.

19 I think the hypotheticals are, may need  
20 to be thought about, but I don't think that they  
21 can drive how we think about the constitutionality  
22 and the statutory implications of the collection.

1 MS. WALD: In other words, you or  
2 anybody over there wouldn't consider if that  
3 happened, some other means that the government  
4 might have to take that about information and go  
5 to somebody, to some authority and say can we keep  
6 this, can we use this, etcetera, etcetera?

7 MS. DONOHUE: So what I'm a little bit  
8 confused about, and I did hear the previous panel  
9 say, oh, well, there would be all sorts of  
10 procedural implications if we had to return to a  
11 judge on the Foreign Intelligence Surveillance  
12 Court to get approval to do further monitoring.

13 What I'm a little bit confused about is  
14 if that information was appropriately obtained in  
15 the first place and it indicates that other people  
16 are implicated, why they wouldn't go back for a  
17 Title I electronic search and they would have what  
18 they need for that?

19 MS. WALD: Well, if it's two  
20 grandmothers, they're probably not -- they're just  
21 chatting. They're probably innocent. All I'm  
22 saying is I guess the only reason I raised it is

1 I'm trying myself to figure out are there not some  
2 gray areas here, and wondering if you had any  
3 solutions short of about authority which you find  
4 is too broad, and completely ignoring it?

5 But let me not use up my whole five  
6 minutes. Thank you.

7 I did want to ask you about, as you  
8 know, the President's review commission said they  
9 wanted to see a warrant, an actual, go get a  
10 warrant for probable cause before you could search  
11 the data using a U.S. person indicator.

12 My question to you is, and we've heard  
13 some reasons why they think that's very onerous,  
14 including the fact that the President's review  
15 commission's recommendation was it had to be a  
16 probable cause warrant that the person was about  
17 to commit something, do bodily injury, or about to  
18 commit some terrorism crime.

19 My question to you is if you think  
20 there are legitimate, and you do, problems under  
21 the Fourth Amendment with using U.S. person  
22 indicators to surveil the PRISM data, would

1 anything short of a probable cause warrant such as  
2 they recommended satisfy you, i.e., I'm just  
3 throwing this out, you know, having, going back  
4 to, say, to the FISA court and having them look at  
5 it to see if it, either post or pre, before they  
6 used it, approving this so-called, you know,  
7 selector, etcetera, that was in fact a reasonable  
8 cause to believe that the person had information  
9 or didn't have information?

10 MR. JAFFER: I don't think that would  
11 be sufficient. I think that you need a warrant at  
12 the back-end and --

13 MS. WALD: But what kind of a warrant  
14 warrants --

15 MR. JAFFER: A warrant based on  
16 probable cause and --

17 MS. WALD: Probable cause of what?

18 MR. JAFFER: Well, so I think it could  
19 be foreign intelligence probable cause, although I  
20 hope that the panel will, that the Board will  
21 think about the scope of the definition, the  
22 definitions of foreign agent, foreign power, and

1 foreign intelligence information.

2 But I think that foreign intelligence  
3 probable cause could be sufficient for that  
4 particular process, or obviously criminal probable  
5 cause.

6 But I also just want to say that I  
7 don't think back-end procedures alone are enough,  
8 no matter how strong they are. And I think that,  
9 you know, I know that the Board can't talk about  
10 the Washington Post report from yesterday, but if  
11 you just take it as a kind of hypothetical, you  
12 know, if you accept that back-end procedures are  
13 enough and that we'll focus solely on the  
14 protections on searching, and dissemination, and  
15 analysis of information in the government's hands,  
16 there's nothing to prevent the government from  
17 recording every phone call, copying every email,  
18 creating a permanent record of everybody's  
19 movements, associations, and communications. And  
20 the only question we'll be asking is when can the  
21 government access it.

22 But the creation of that kind of

1 massive database will have huge implications for  
2 the way that ordinary people operate in society,  
3 both the way that they interact with one another  
4 and the way that they interact with their  
5 government.

6           People who believe that the government  
7 is surveilling every movement and every  
8 communication, believe justifiably that it's doing  
9 it, will act differently. They won't go to  
10 controversial websites and they won't engage in  
11 controversial communications that are necessary  
12 for any democracy.

13           MS. WALD: I'll save, I know my time is  
14 up. I'll wait for the next round. I have another  
15 question.

16           MR. MEDINE: I want to go back to that  
17 back-end searching, basically the U.S. person  
18 searches, and this really is two questions.

19           One is the government panel asserts  
20 that this is lawfully obtained information and  
21 therefore should be permissibly used without any  
22 further Fourth Amendment implications. And why

1 that's not a persuasive argument.

2           And then two, if it's not persuasive,  
3 what is the procedure that you envision? And  
4 again, I think it's different from Professor  
5 Donohue where you're using that U.S. person  
6 information to get more information. You're just  
7 saying let's use the information we've already  
8 collected under some other, under authority for,  
9 say, criminal purposes or foreign intelligence  
10 purposes.

11           So I guess it's two parts. Why isn't  
12 is already legally usable? And if it's not, what  
13 procedure would you apply to access it? And  
14 that's to any panelists.

15           MS. DONOHUE: So as a statutory matter  
16 I would come back to the burden of proof with  
17 regard to whether that information that's being  
18 collected on targets, they are indeed U.S. persons  
19 or non-U.S. persons and located outside the United  
20 States.

21           So here the statute is silent, and I  
22 share Mr. Dempsey's textual analysis of the about

1 question. I think the statute is silent there as  
2 well. But in regard that the statute does say  
3 where you know that somebody is a U.S. person, you  
4 know, you have Sections 703 and 704 that you have  
5 to operate under.

6 MR. MEDINE: Again, we're not targeting  
7 the U.S. person, we're targeting a non-U.S.  
8 person, and Congress clearly knew that at the  
9 other end of that phone call could be a U.S.  
10 person and still authorized that kind of  
11 collection without a warrant.

12 And the question is, why isn't that  
13 sufficient to then say, okay, this information was  
14 lawfully collected, now we can do searches based  
15 on it?

16 MS. DONOHUE: Because it isn't  
17 certain that the person on whom you're collecting  
18 the information really is a non-U.S. person. So  
19 the burden of proof on the NSA is to say, to  
20 establish that this individual is a non-U.S.  
21 person.

22 But in fact, so the assumption that all

1 the collection that's going on currently is of  
2 non-U.S. persons I think is an erroneous one. And  
3 it's one -- and the reason why I think it's  
4 erroneous is because the NSA is under no  
5 obligation to check and see and make sure that  
6 that individual is not a U.S. person.

7 To the contrary, they have in their  
8 documents they say, well, they may check these  
9 databases, they may check these other databases.  
10 There's no obligation that they do so.

11 Mr. De in the previous panel referred  
12 to the totality of the circumstances type tests  
13 that say they have two strikes against, four  
14 strikes for, they look at everything. There is  
15 nothing that obliges them to then go back and dig  
16 up more information to find out in that particular  
17 circumstance.

18 And not only that, but actually if you  
19 look at the requirements for what is required to  
20 positively identify, to conclusively determine it  
21 in the minimization procedures, the bar is  
22 actually significantly high.

1           It means that you know their name, you  
2 know their title, you know their address, you  
3 know their personally identifiable information in  
4 the context of activities conducted by that person  
5 that are related to that particular person. A  
6 reference to a brand name, manufacturer's name,  
7 Monroe Doctrine, etcetera, that's not sufficient.

8           So not only are they under no  
9 obligation to establish that but in order to  
10 establish it, it's a very high bar. So it's not  
11 clear to me that that information is lawfully  
12 collected in the first place.

13           MR. MEDINE: Ms. Levinson-Waldman, do  
14 you want to weigh in on that?

15           MS. LEVINSON-WALDMAN: I think the  
16 other thing I was going to add, if I'm  
17 understanding the question correctly about why is  
18 it not okay to do searches on information that's  
19 been lawfully collected, I think there's also an  
20 element of bootstrapping.

21           So that it was lawfully collected for a  
22 purpose, for a foreign intelligence purpose, and

1 that you're right, of course Congress knew that  
2 U.S. person information was going to be  
3 incidentally collected through that process, but  
4 then there are these minimization procedures.

5           And so kind of almost bypassing those  
6 procedures and allowing that body of information  
7 to be collected without meeting a fairly high bar,  
8 some kind of probable cause warrant seems like  
9 kind of going back and bootstrapping your way into  
10 that information in a way that is very different  
11 from searches of, I think, any other, almost any  
12 other body of lawfully collected information,  
13 because the standard for which it's obtained, that  
14 foreign intelligence standard and purpose is so  
15 different.

16           MR. JAFFER: I mean I actually think  
17 there are two kinds of bootstrapping. The first  
18 is pointing to the fact that foreigners outside  
19 the United States lack Fourth Amendment rights in  
20 order to collect huge volumes of communications to  
21 which Americans are a party.

22           And then the other is pointing to the

1 foreign intelligence purpose to gather information  
2 which is then later used in criminal prosecutions.  
3 So that's to state the problem. It's not a  
4 solution to the problem, but I think that's where  
5 the concern comes from.

6 MR. MEDINE: Professor Ku.

7 MR. KU: If I could just add, I mean  
8 I'm not sure that's bootstrapping. I think that's  
9 sort of the purpose, right. The purpose is --  
10 it's not that they're not also collecting it for  
11 foreign intelligence purposes.

12 It's also true that if in the old days  
13 they came across a letter from an American person  
14 to a foreign person, it seems unlikely to me that  
15 because an American sent the letter that means  
16 they can't -- but they lawfully obtained the  
17 letter, it's unclear to me why they couldn't use  
18 that letter.

19 And so I'm a little, possibly it's  
20 bootstrapping, but it's, there's a long history of  
21 going after foreigners and doing foreign  
22 surveillance.

1 I'm not sure that -- I think the only  
2 difference I think is technology does make it  
3 easier for it to flip back into the states, but  
4 I'm not sure that fundamentally this is a really  
5 different thing.

6 MR. MEDINE: Thank you. Ms. Brand.

7 MS. BRAND: Thank you. Well, it seems  
8 like there are some fundamentally opposing world  
9 views about the Fourth Amendment on the panel, and  
10 I want to, I mean this Board is not going to move  
11 Fourth Amendment law. So I want to get to what  
12 you think the law is and what you think the law  
13 should be, because I think there might be some  
14 conflation of those two things going on here.

15 First of all, Professor Ku, thank you  
16 for submitting your comments this morning, your  
17 written comments. I haven't had a chance to read  
18 them yet so I just want to ask you a question to  
19 make sure I understand where you're coming from.

20 You talk about inherent executive  
21 authority to conduct surveillance abroad or even  
22 of non-U.S. persons abroad. In your view, does

1 that inherent executive power operate alongside  
2 the Fourth Amendment, or irrespective of the  
3 Fourth Amendment, or does that create an exception  
4 to the Fourth Amendment?

5 MR. KU: Right, no, I don't think it  
6 creates an exception to the Fourth Amendment. It  
7 operates within the constraints, whatever they  
8 might be, of the Fourth Amendment.

9 But I would like to point out that  
10 historically this -- I mean so just to clarify.  
11 The reason I raise this, it goes to the point that  
12 historically the U.S. government as operated  
13 without statutory authority to conduct foreign  
14 surveillance. It's been, the power was granted,  
15 was thought of as coming from the Constitution.

16 So the statutory scheme has not been  
17 thought of as necessary to authorize the type of  
18 intelligence gathering that's going on.

19 Now the Fourth Amendment does apply,  
20 but as I also emphasized, it hasn't always  
21 applied. It didn't originally was thought of to  
22 apply at all, even to U.S. citizens overseas, but

1 I think we understand that the courts have come  
2 around to view that it does apply to U.S. citizens  
3 overseas. But I think it still has a limited  
4 impact compared to the way it applies for purely  
5 domestic searches. So that's how I would analyze  
6 that.

7 MS. BRAND: And how does it apply to  
8 purely domestic searches where there's a purpose  
9 of foreign intelligence gathering?

10 MR. KU: Well, I think that -- well,  
11 here I think that, you know, it does. The Fourth  
12 Amendment has been interpreted in recent cases to  
13 be a much more robust protection for searches  
14 domestically, although even in some of those  
15 cases, right, a warrant has not been required or  
16 the exception to the warrant requirement has been  
17 found for foreign intelligence purposes. So it  
18 still continues to exist within the domestic  
19 sphere.

20 I would say that for me, at least my  
21 understanding is a lot of this has been supplanted  
22 by the FISA system. The rise of the FISA system

1 has to some degree made the Fourth Amendment  
2 analysis a little bit less onerous because what's  
3 been happening is that everything's been funneled  
4 through the FISA system and the challenges to the  
5 FISA system has not been sort of as robust.

6 I think if we hadn't had FISA maybe  
7 we'd have had more cases that would have clarified  
8 exactly what the Fourth Amendment limits on  
9 domestic foreign intelligence searches would be.  
10 I do think that it applies more strongly to  
11 domestic searches and I think it has more  
12 significance.

13 But I do think that ultimately the  
14 foreign intelligence exception to the warrant  
15 requirement is a reasonable one that does need to  
16 be respected. It has a long tradition in history.

17 In my view, really FISA is sort of on  
18 top of that to add additional privacy protections  
19 that I think Congress has judged, and probably  
20 rightly so, we need. But I'm not sure the Fourth  
21 Amendment itself standing alone would necessarily  
22 require all of the sort of procedural limitations

1 and minimization protections that we have.

2 MS. BRAND: Okay. And Jameel, can you  
3 very briefly, because I have another question for  
4 you, you do not think there is any foreign  
5 intelligence exception to the Fourth Amendment?  
6 Is that what I heard you say earlier?

7 MR. JAFFER: I don't think that there's  
8 any foreign intelligence exception broad enough to  
9 justify 702, and no court has --

10 MS. BRAND: But there is -- I mean I  
11 guess what I'm trying to get at is, do you think  
12 that the Fourth Amendment applies equally to  
13 collection for the purpose of foreign intelligence  
14 gathering as it applies to collection when the  
15 purpose is to gather evidence of a bank robbery,  
16 for example?

17 MR. JAFFER: I think that there are  
18 certainly narrow circumstances in which the courts  
19 have held that there is a foreign intelligence  
20 exception.

21 Again, those cases predate FISA, and so  
22 you know, you have to evaluate whether those cases

1 survived the thirty-five years of experience under  
2 FISA.

3 MS. BRAND: Okay. And then you  
4 referred earlier to, I think you were referring  
5 to, well, you're referring to 702 generally as  
6 large scale collection. I'm not sure if you were  
7 including both upstream or PRISM in that  
8 assessment.

9 But if you were here for the first  
10 panel and if you take the government's facts as  
11 they stated them to be true, what about that  
12 program strikes you as large scale? What's your  
13 justification for that description?

14 MR. JAFFER: Well, so two responses to  
15 that. The first is I think it's important to draw  
16 a distinction between statutory restrictions and  
17 executive restraint. So there's a question of  
18 what the statute allows and then there's a  
19 question of how the government is implementing it.

20 Obviously I know much less about how  
21 the government is implementing it than I do about  
22 what the statute on its face allows because I can

1 read the statute and I have access to only a  
2 portion of the government's documents.

3 But then as to, you know, whether it's  
4 large scale collection or not, I think that the  
5 problem is that everybody is using these words in  
6 different ways. The panelists this morning said  
7 that they weren't drawing a distinction between  
8 acquisition, surveillance, and collection. But  
9 their own documents do draw a distinction.

10 If you look at USD 18, for example,  
11 which is the Defense Department's implementation  
12 of the executive order on intelligence collection,  
13 it draws a distinction between electronic  
14 surveillance and acquisition on the one hand and  
15 collection on the other.

16 And collection involves the tasking of  
17 that, or tasking of communications, whereas  
18 electronic surveillance and acquisition do not.

19 And so, you know, we have always  
20 thought of this, putting the vocabulary to the  
21 side for a second, we've always thought of this in  
22 two stages. There is a kind of, just to -- there

1 is a kind of, you might call it scanning, you  
2 might call it collection, but there's a kind of  
3 large scale acquisition of data, and then there's  
4 the government tasking that data, and then there  
5 is the government's tasking that data with  
6 selectors.

7           So to be a little more concrete, if the  
8 government installs on a switch somewhere installs  
9 a device that either diverts all of the  
10 communications or a large portion of the  
11 communications, or scans a large portion of the  
12 communications, we would call that bulk  
13 collection.

14           I'm not sure that anything turns on  
15 vocabulary but we should all make sure we're  
16 talking about the same concepts.

17           MR. MEDINE: Ms. Cook.

18           MS. COLLINS COOK: Actually that was  
19 right at the top of the last piece. I think we've  
20 used, and in this conversation alone we've used  
21 scan, inspect, acquire, collect, access.

22           And so I guess my question is, if you

1 have access, so in your hypothetical you've  
2 installed something that gives you access to this  
3 stream of communications, is that a seizure or a  
4 search for the purpose of Fourth Amendment  
5 analysis in your view?

6 MR. JAFFER: Well, I think it would  
7 depend what you were accessing. You know, the  
8 question would be have you invaded a reasonable  
9 expectation of privacy?

10 But we have taken the position that,  
11 for example, the bulk accessing of telephone  
12 metadata is an invasion of a reasonable  
13 expectation of privacy, and we would certainly  
14 take the same position with respect to the bulk  
15 acquisition of telephone calls or emails.

16 The MYSTIC program, again, just  
17 discussing it as a kind of hypothetical, that  
18 program in my view involves the bulk collection of  
19 telephone calls, voicemail messages, and telephone  
20 calls, even if the government doesn't access more  
21 than a small proportion of them.

22 MS. DONOHUE: May I add something to

1 that just very quickly? I was a little bit  
2 confused in the earlier panel because on the one  
3 hand they were saying this is a very limited  
4 program. On the other hand they say that this  
5 SIGAD is the most used NSA SIGAD.

6 The slides that have been released say  
7 it draws from Microsoft, Google, Yahoo, Facebook,  
8 Paltalk, YouTube, Skype, AOL and Apple, that it  
9 gets voice over Internet protocol, email, chats,  
10 all this information, and it's hard to square  
11 that.

12 And what they say is the value of the  
13 program, with its limited nature --

14 MS. COLLINS COOK: I'm sorry, can we  
15 talk about -- I appreciate your desire to talk  
16 about the previous panel but I had a specific  
17 question out that I'm really trying to understand  
18 the panelists' view on when the Fourth Amendment  
19 is implicated and how.

20 And so if it's under your hypothetical  
21 if you have the acquisition of all phone calls  
22 from a country with subsequent access, at what

1 point would the Fourth Amendment attach?

2 MR. JAFFER: I would say certainly the  
3 moment you put it in your databases, by that  
4 moment the Fourth Amendment has attached.

5 MS. COLLINS COOK: So flipping that, if  
6 it's access to a wide swath of communications but  
7 acquisition into the government's possession or  
8 control, when would the Fourth Amendment attach?

9 MR. JAFFER: I'm sorry, but I've lost  
10 track of the difference between access and  
11 acquisition.

12 MS. COLLINS COOK: And this is part of  
13 the, I think you've used scanned, but some ability  
14 to review a stream of communications and pull,  
15 filter, something to that effect.

16 MR. JAFFER: Right. The scanning or  
17 the filtering would implicate the Fourth Amendment  
18 in my view.

19 MS. COLLINS COOK: That's helpful. I  
20 wanted to follow up on a different set of  
21 questions and just close the loop.

22 If the determination was made that the

1 acquisition of the information pursuant to 702 was  
2 lawful, it's lawfully acquired information, would  
3 you still take the position that a subsequent  
4 search, and by that I mean a query using a U.S.  
5 person identifier, would need some sort of  
6 probable cause determination, that there would be  
7 a separate Fourth Amendment analysis?

8           And can you explain why? I guess is  
9 this because there's a view that there's a lack of  
10 particularity of the front-end and therefore you  
11 have to have subsequent some particularized  
12 finding?

13           MR. JAFFER: Yes.

14           MS. DONOHUE: That would be my position  
15 as well.

16           MS. COLLINS COOK: Okay. One question  
17 for Professor Ku, if I could. We've heard that  
18 702 is silent, I think it's fair to say on the  
19 precise question of abouts. There are some  
20 structural arguments here and some purpose  
21 arguments that you can look to, but it's silent.

22           In view of the evolution of our

1 understanding of Article II of FISA, how would you  
2 as a constitutional matter assess a silence in  
3 702? Because Title VII is both an authorization  
4 and a restriction on Article II authority, so.

5 MR. KU: Right. So I think, I don't  
6 know if I have any sort of grand insights on the  
7 purely textual analysis, although I do think that  
8 the constitutional background is what can help us  
9 here with respect to, if we understand where we're  
10 coming from can help us analyze this.

11 If we understand that constitutionally  
12 that the U.S. government was engaged in broad  
13 searches prior to the enactment of 702 then you  
14 have to sort of think about, well, to what degree.

15 This is not really about authorizing,  
16 this is really about restricting, imposing  
17 restrictions on what I think the U.S. government  
18 had the authority to do prior to the enactment of  
19 the statute.

20 And so if you look at it from that  
21 perspective then, if it doesn't, the silence or  
22 the lack of clarity or specificity would then I

1 think lead me from that perspective to suggest  
2 that the President retains that power.

3 I would analogize this a little bit to  
4 the point that was made in the earlier FISA  
5 statute, how they excluded radio completely from  
6 the original FISA, radio communications, they just  
7 said nothing about it.

8 And there are a lot of people that  
9 argue that was on the assumption that most of the  
10 foreign intelligence was radio in 1973 and that  
11 the President would continue going on gathering as  
12 much radio signals intelligence as he could. And  
13 then at a certain time, no one used radio anymore.

14 But the point is that if you add the  
15 restriction in the statute it doesn't -- the  
16 previous or the other authority the President has  
17 to conduct the surveillance should in theory  
18 continue, and I think would likely to continue  
19 here too, assuming he had the authority prior to  
20 the enactment.

21 MR. MEDINE: Mr. Dempsey.

22 MR. DEMPSEY: A quick comment and then

1 a question. Going to the definition of  
2 distinctions between collect, acquire, etcetera,  
3 my comment is we really have to take yes for yes  
4 and no for no and move on. The government has  
5 said, to my mind totally clearly, they are not  
6 relying upon the USD 18 concepts in implementing  
7 702, so I think that we just have to move on from  
8 that. That's my comment.

9 My question is the following, and this  
10 is for Jameel or anybody, Rachel, in terms of the  
11 querying of data otherwise lawfully acquired, what  
12 is the best case law that would limit the  
13 proposition that data lawfully acquired can be  
14 subsequently queried without limitation?

15 MR. JAFFER: Well, so on your comment,  
16 I think you're certainly right that the government  
17 said on the panel earlier today that they were not  
18 relying on the distinction, any distinction  
19 between acquisition and collection.

20 But I think that the government also  
21 acknowledged that it was engaged in about  
22 surveillance, and to engage in about surveillance,

1 my understanding is that there is no way to engage  
2 in about surveillance without inspecting in some  
3 sense every communication within the universe of  
4 those that you are monitoring or surveilling.  
5 There's no way to do it.

6 Now you can call that bulk collection  
7 or you can call it something else, but that  
8 scanning of every communication in a particular  
9 universe raises constitutional issues, and if all  
10 you're saying, Mr. Dempsey, is we should just  
11 address those constitutional issues, then I  
12 entirely agree.

13 MR. DEMPSEY: So now as the querying of  
14 otherwise lawfully acquired communications, and  
15 let's take, you know, if I steal your computer, I  
16 think, and then I give it to the government, the  
17 government lawfully acquired it. I may have  
18 stolen it. Or certainly in the Title III context  
19 the government lawfully acquires, or in the normal  
20 search and seizure context, or in the voluntary  
21 disclosure context, where is there case law  
22 limiting the proposition that lawfully acquired

1 information cannot subsequently be queried  
2 essentially without prior authorization, without  
3 meeting any threshold? What is, is there any  
4 case law limiting that?

5 MS. DONOHUE: So we're starting to see  
6 cases come out of border security issues where  
7 computers -- border security issues, and I'd be  
8 happy to send you the names of the cases  
9 afterwards, where computers have been lawfully  
10 seized under customs laws but then they cannot be  
11 searched for all of the information on them  
12 because of the privacy implications that are  
13 involved and lack of a sufficient nexus to the  
14 suspected criminal activity.

15 So those cases might be one source that  
16 you would look to in a new age of data where so  
17 much information is available.

18 MR. JAFFER: You know, I think it's  
19 important to ask the question the other way around  
20 as well, which is, you know, where is there  
21 case law showing that the Constitution is  
22 indifferent to the government collecting huge

1 volumes of communications without any  
2 individualized suspicion or particularity, and  
3 then sort of bootstrapping its way into free rein  
4 or --

5 MR. DEMPSEY: Again, if we're in a  
6 situation, I'm just trying to pose the situation  
7 of let us assume, just let us assume that the  
8 collection was lawful.

9 MR. JAFFER: I'm not suggesting for  
10 these purposes that the collection was unlawful.  
11 What I'm saying is that the collection here is  
12 different in kind from the kind of collection that  
13 the courts have been concerned with in other cases  
14 involving the use of information lawfully  
15 acquired. You know, it was important to those  
16 cases not just --

17 MR. DEMPSEY: So then the license plate  
18 readers, the information collected by the license  
19 plate readers is lawfully acquired and then the  
20 government can subsequently query that license  
21 plate database. I mean that's standard procedure.

22 MR. JAFFER: I'm not sure that it's

1 established with any certainty that the bulk  
2 collection, that the querying of a database of  
3 bulk collected license plate reader information  
4 doesn't raise Fourth Amendment concerns, and I  
5 think that that's still an open question.

6 MR. DEMPSEY: Well, I'm looking for  
7 some cases. Professor Donohue has some border  
8 cases --

9 MS. DONOHUE: I'd be happy to send you  
10 the border doctrine cases.

11 MR. DEMPSEY: That may be relevant. I  
12 would welcome any other cases limiting that  
13 proposition.

14 MR. MEDINE: Judge Wald.

15 MS. WALD: This is probably an unfair  
16 question but I'll ask it anyway. Given the fact  
17 that the grievances about 702 as it operates today  
18 have included a whole series of things, one we  
19 didn't discuss here but it's been raised in  
20 written stuff is the lack of FISA review of  
21 particularized targeting designations. I know  
22 it's allowed by the statute, but nonetheless the

1 capture and use of incidental U.S. information to  
2 search database, the use and retention of the U.S.  
3 information.

4 But my question is, if you had to focus  
5 on one or maybe two important changes that you  
6 would like to see made now in 702, what would they  
7 be? Very quickly, anybody that wants to  
8 answer it.

9 MS. DONOHUE: I would say limiting the  
10 information to, or from, or held by the actual  
11 target and inserting a mechanism of judicial  
12 review if information is uncovered that would lead  
13 to subsequent criminal prosecution prior to  
14 analysis of the databases that are held.

15 MS. WALD: Okay, great. Down the line.

16 MR. JAFFER: The only thing that I  
17 would add to that is destruction of inadvertently  
18 acquired communications. Communications that the  
19 government itself acknowledges should not have  
20 been acquired in the first place should be  
21 destroyed immediately.

22 MS. WALD: Destruction, they say

1 they're purging them but you mean something --

2 MR. JAFFER: There are broad exceptions  
3 to the --

4 MS. WALD: I know there are exceptions,  
5 but you mean -- okay.

6 Do you have any, Professor Ku?

7 MR. KU: Actually, I mean this may be  
8 kind of not what you're looking for, but I do  
9 think that actually I would prefer the FISA  
10 section clarify the default that I've been arguing  
11 for, that it doesn't encroach, to clarify further  
12 that it doesn't encroach on, Section 702 doesn't  
13 encroach on the President's, you know, foreign  
14 intelligence authority. That would, I think, help  
15 our interpretation of the statute.

16 MS. LEVINSON-WALDMAN: And I just would  
17 mention three things. One is I agree more robust  
18 involvement by the FISC.

19 MS. WALD: I'm sorry, more?

20 MS. LEVINSON-WALD: More robust  
21 involvement by the FISC in terms of review.  
22 There's some review now that is sort of a

1 box-checking procedure, and have that review be  
2 more --

3 MS. WALD: Just the way they do what  
4 they do now, but more carefully?

5 MS. LEVINSON-WALDMAN: Well, I'd say  
6 not even, it's not so much that I think that  
7 they're not careful with it now, it's that the  
8 statute actually limits the scope of some of the  
9 review that they do, that they sort of don't get  
10 behind the curtain.

11 MS. WALD: Including the targeting.

12 MS. LEVINSON-WALDMAN: Right. I guess  
13 the second, thinking about, so if you think about  
14 Section 702 but having the minimization procedures  
15 be a natural part of that statute.

16 Certainly limiting and potentially  
17 eliminating the use of information for law  
18 enforcement purposes. And obviously this is  
19 something that the NSA, that the President's  
20 review group spoke to as well and made that  
21 recommendation.

22 And then the third quite honestly would

1 be to lift the standard back up to agent of a  
2 foreign power from the foreign intelligence  
3 requirement. And the foreign intelligence purpose  
4 is so loose and that that seems to be --

5 MS. WALD: For targeting?

6 MS. LEVINSON-WALDMAN: For targeting,  
7 yes, that's correct.

8 MS. WALD: Okay. I've got maybe one  
9 minute left so a quick question. Some of you, I  
10 don't remember now, all of you in a prior one,  
11 when we were doing 215, talked about the  
12 desirability/necessity of having an adversarial  
13 element in the FISA proceedings.

14 A very quick notion of how would you  
15 see an adversary, however appointed, in a 702  
16 proceeding? In other words, what function could  
17 they serve, he or she serve in a 702?

18 215 was a little bit more evident. A  
19 novel technological case coming up to the court,  
20 what would you say, do they have any, would they  
21 have any function in a 702?

22 MS. DONOHUE: So I would imagine them

1 having a function absolutely, yes. The ACLU tried  
2 to do this and was not allowed to intervene on a  
3 motion on a First Amendment grounds and it was  
4 denied by the court in part on the grounds that  
5 they would never succeed on the First Amendment to  
6 actually intervene.

7 I think having an advocate there would  
8 allow them to more carefully review minimization  
9 procedures, to more carefully review targeting  
10 procedures. It would allow them to evaluate the  
11 role that they play with regard to targeting.

12 MS. WALD: In individual cases in 702?

13 MS. DONOHUE: And in individual cases,  
14 yes, but you would have to change to insert some  
15 sort of a warrant requirement equivalent for  
16 criminal prosecution or further examination of the  
17 records.

18 MR. JAFFER: And I think that our  
19 biggest concern is with judicial rulings that have  
20 far-reaching implications and not just  
21 implications in the individual cases. So I think  
22 that when you're talking about the individual

1 cases, I do think that, you know, in theory an  
2 adversarial process would be a useful thing.

3 On the other hand, I think that the  
4 closer you get to an individualized warrant  
5 application, or court order application, or  
6 surveillance application, the more it looks like  
7 traditional Title III or a search warrant context,  
8 which is ex parte.

9 But you know, when you get to judicial  
10 opinions that authorize about surveillance at some  
11 level of generality, that is something that ought  
12 to be argued in open court, you know, with a  
13 closed hearing to follow if there is legitimate,  
14 if there are legitimate sources and methods to be  
15 protected.

16 But if I can just use the process to  
17 add one answer to your previous question, I agree  
18 very strongly with what Rachel said that reforming  
19 or revising the standard, the targeting standard  
20 is crucial.

21 Right now there is, there's really no  
22 limit on who the government can target overseas.

1 The example that the government panelist kept  
2 coming back to is bad guy at Google.com or bad guy  
3 at Yahoo.com. But it could as easily be  
4 journalist at Yahoo.com, or human rights activist  
5 at Yahoo.com. And I think it's crucial that some  
6 limits be drawn around the category of people whom  
7 the government can legitimately target.

8 MS. WALD: And by the FISA court?

9 MR. MEDINE: We only have a couple of  
10 minutes. If there's any members of the Board who  
11 want to ask any additional questions.

12 MS. COLLINS COOK: Can I ask just one  
13 quick follow-up question on this point actually?

14 MR. MEDINE: Sure.

15 MS. COLLINS COOK: And this is to  
16 Ms. Levinson-Waldman. You had said lift the  
17 standard back to agent of a foreign power or a  
18 foreign power. What were you referring to when  
19 you said back to?

20 MS. LEVINSON-WALDMAN: Right, I mean I  
21 guess back to, we're sort of envisioning to some  
22 extent Section 702 is sui generis and when it came

1 into being it was a foreign intelligence  
2 requirement. But I guess thinking of FISA more  
3 broadly, narrowing that foreign intelligence  
4 standard in some way to match what is in other  
5 sections.

6 Obviously one option would be matching  
7 what's in other sections of FISA, agent of a  
8 foreign power, I think that would be our  
9 preference, but narrowing that in some way. Back  
10 was probably an imprecise way of referring to it.

11 And if I could add one other brief  
12 thing, I think our other, you know, if we have a  
13 wish list it would be, and again, I'll say  
14 restore, but thinking about other parts of FISA,  
15 having the collection be, and you know, these may  
16 be one or the other but having the collection, the  
17 foreign intelligence be the primary purpose rather  
18 than a significant purpose, that that has also  
19 allowed, you know, potentially a fair amount of  
20 slippage in terms of what the collection is for.

21 MR. MEDINE: Any other final questions?  
22 I want to thank the panelists very much for

1 joining us today. It was a very enlightening  
2 discussion. We're now going to take a lunch break  
3 and we will resume with our third panel at 1:45.  
4 Thank you.

5 (Off the record)

6 MR. MEDINE: Good afternoon, and thanks  
7 everyone for rejoining us. And I want to  
8 introduce our third panel, which will be on  
9 transnational and policy issues.

10 We are joined by John Bellinger, who is  
11 a partner at Arnold & Porter, Dean Garfield, who  
12 is the President and CEO of the Information  
13 Technology Industry Council, Laura Pitter, who is  
14 a Senior National Security Researcher at the Human  
15 Rights Watch, Ulrich Sieber, who is the Director  
16 at the Max Planck Institute for Foreign and  
17 International Criminal Law in Freiburg, Germany,  
18 and Chris Wolf, who is a partner at Hogan Lovells.

19 Each of the panelists will make a brief  
20 opening statement and then we will proceed with  
21 the Board questioning.

22 I guess we can start alphabetically

1 with Mr. Bellinger.

2 MR. BELLINGER: It's me first then.

3 Well, thank you all very much for having me in,  
4 the members of the Board. I'm going to focus my  
5 comments on whether international law places any  
6 restrictions on electronic surveillance of foreign  
7 nationals outside the United States.

8 I think you know I served as the legal  
9 advisor for the Department of State from 2005 to  
10 2009, as the legal advisor for the National  
11 Security Council from 2001 to 2005, and then I was  
12 the national security advisor to the head of the  
13 Criminal Division at Justice Department before  
14 that, so I have extensive experience, both in  
15 intelligence activities and international law.

16 So in recent months I think you know  
17 many scholars and human rights advocates have  
18 argued that NSA surveillance of foreign nationals  
19 violates a so-called universal right to privacy  
20 recognized in international law.

21 They base their argument on Article 17  
22 of a human rights treaty called the International

1 Covenant on Civil and Political Rights, which the  
2 U.S. ratified in 1992.

3 Article 17 provides, and I quote, no  
4 one shall be subjected to arbitrary or unlawful  
5 interference with his privacy, family, home, or  
6 correspondence, end quote.

7 The argument that NSA surveillance  
8 violates Article 17 of the ICCPR is incorrect for  
9 several reasons. And I will say in my view  
10 international law, neither the ICCPR or any other  
11 part of international law placed international  
12 legal restrictions on the NSA, any of the NSA  
13 programs.

14 With respect to the ICCPR, first, for  
15 the last sixty-four years the United States  
16 government has taken the consistent position that  
17 it does not apply outside the borders of the  
18 United States. The U.S. took this position when  
19 we negotiated the treaty in 1950, and we  
20 re-articulated it in 1995, when the Clinton  
21 administration submitted its first report to the  
22 U.N. Human Rights Committee, which is the group

1 that oversees compliance with the ICCPR.

2 My predecessor at the time, the then  
3 legal advisor Conrad Harper, explained to the  
4 committee that the ICCPR imposes obligations on  
5 the United States only inside the United States.  
6 And that's because Article 2 of the ICCPR, which  
7 defines its scope, says that a state party is  
8 bound to respect and ensure the rights in the  
9 ICCPR only to all individuals within its territory  
10 and subject to its jurisdiction.

11 And as my predecessor, Conrad Harper  
12 said at the time, this is a dual requirement that  
13 establishes that treaty obligations apply only if  
14 both conditions are satisfied. An individual must  
15 be under United States jurisdiction and within  
16 United States territory.

17 And now the negotiating position of the  
18 United States of the treaty confirms that  
19 interpretation. The phrase, within its territory,  
20 was added at the request of the head of the U.S.  
21 delegation, Eleanor Roosevelt at the time in 1950.  
22 And she explained that, quote, the purpose of the

1 proposed addition is to make it clear that the  
2 draft covenant would apply only to persons within  
3 the territory and subject to the jurisdiction of  
4 the contracting states.

5           There was a vote held on that addition  
6 and that addition was adopted 8 to 2 in 1950.  
7 Subsequent efforts to change that have failed.

8           And again, in his statement to the  
9 Human Rights Committee in 1995, Conrad Harper  
10 explained that the words were added, quote, with  
11 the clear understanding that such wording would  
12 limit the obligations to within a party's  
13 territory.

14           Now it's true, and I know that Laura  
15 Pitter is going to talk about this, that the Human  
16 Rights Committee and a lot of human rights groups  
17 in other countries don't agree with the  
18 long-standing U.S. interpretation, but the Human  
19 Rights Committee's statements don't have binding  
20 legal effect on the United States or to any other  
21 country. We give respect to them but they're not  
22 binding on us.

1                   Both the Bush and the Obama  
2                   administrations have confirmed the Clinton  
3                   administration's position that the ICCPR does not  
4                   apply extra-territorially.

5                   In fact, just five days ago in Geneva  
6                   we were making our periodic report to the Human  
7                   Rights Committee and the acting legal advisor,  
8                   Mary McLeod, told the committee, quote, the United  
9                   States continues to believe that its  
10                  interpretation that covenant applies only to  
11                  individuals both within its territory and within  
12                  its jurisdiction is the most consistent with the  
13                  covenant's language and negotiating history.

14                  So we really have fifty years of U.S.  
15                  practice on this point recently reaffirmed by the  
16                  Obama administration.

17                  But even if the ICCPR did apply  
18                  extra-territorially, the treaty would still not  
19                  place limits on NSA surveillance because persons  
20                  in other countries are not subject to U.S.  
21                  jurisdiction.

22                  The Human Rights Committee itself has

1 defined the phrase subject to a party's  
2 jurisdiction to include people within the power or  
3 effective control, or effective control of the  
4 forces of a state party acting outside its  
5 territory. So not even the Human Rights Committee  
6 is suggesting that everybody who may be subject to  
7 NSA surveillance is actually within the power or  
8 effective control of the United States.

9           And I would want to hear more from my  
10 colleague who I've met before, Professor Sieber,  
11 but even if they're unhappy with NSA surveillance,  
12 I am not aware of any foreign government that  
13 believes that the ICCPR or any other provision of  
14 international law imposes an obligation to respect  
15 the privacy rights of non-citizens.

16           In fact, candidly, most foreign  
17 governments spend lots of time spying on foreign  
18 citizens. So they may be unhappy with what we're  
19 doing as a policy matter, human rights groups may  
20 suggest that there are binding legal norms, but  
21 I'm actually not aware that foreign governments  
22 are suggesting that there is an actual violation

1 of international law.

2 And finally, just to close on my  
3 analysis of the ICCPR, and then I'll wind up, even  
4 if the ICCPR did impose certain obligations on  
5 United States extraterritorial conduct, even if  
6 people outside the United States were considered  
7 to be within the jurisdiction of the United  
8 States, Article 17 of the ICCPR still only bans,  
9 quote, arbitrary and unlawful interference with  
10 privacy.

11 Now we can certainly argue about  
12 constitutes arbitrary and unlawful interference  
13 but there is no international norm on that point.  
14 I'm sure lots of people can suggest that the NSA  
15 program is arbitrary, that it's unlawful, but when  
16 we're talking about international law there has to  
17 be actually a specific norm that people have  
18 agreed to, and there is no generally accepted  
19 framework under international law that defines  
20 what kind of surveillance is unlawful or  
21 arbitrary.

22 So the bottom line, despite statements

1 that we are violating the Article 17 of the ICCPR,  
2 it just simply does not apply, nor does any other  
3 provision of international law.

4 And so let me close by saying that just  
5 because international law doesn't actually create  
6 a universal right of privacy that's binding on the  
7 United States, I'm by no means saying that we  
8 ought to be insensitive to the rights of  
9 non-citizens. Certainly if I were still in the  
10 White House I would be saying, you know, we need  
11 to be respectful of concerns both of individuals  
12 or of leaders. That's why we make these policy  
13 decisions.

14 President Obama's recent presidential  
15 policy directive states that signals intelligence  
16 activities must take into account that all persons  
17 should be treated with dignity and respect,  
18 regardless of their nationality or wherever they  
19 might reside, and that all persons have legitimate  
20 privacy interests in the handling of their  
21 personal information.

22 So it's perfectly appropriate to take

1 into account privacy interests, but international  
2 law does not place binding legal obligations on  
3 us. Thank you.

4 MR. MEDINE: Thank you. Mr. Garfield.

5 MR. GARFIELD: Thank you. Thank you  
6 members of PCLOB on behalf of fifty-six of the  
7 most dynamic and innovative companies in the  
8 world, thank you for inviting us to testify today.  
9 And thank you as well for your efforts to advance  
10 both national security and civil liberties.

11 From our perspective we have the firm  
12 view that those two concepts are mutually  
13 reinforcing and in fact are not mutually exclusive  
14 and so we want to do whatever we can to support  
15 your efforts.

16 I'd like to focus my testimony on two  
17 areas. One, what we're experiencing in the  
18 marketplace as a result of the NSA disclosures  
19 and, then share some solutions that may help  
20 remediate some of the challenges that we're  
21 facing.

22 On the first, the economic impact from

1 the NSA disclosures are significant and ongoing.  
2 The folks in this room are very familiar with  
3 Section 215 and the distinction between that and  
4 Section 702, but for folks outside of this room  
5 much of what they experience and what we're  
6 experiencing is diminishing trust, particularly  
7 diminishing trust in U.S.-based technologies. So  
8 rather than made in the U.S.A. being a badge of  
9 honor, it's increasingly becoming a basis to  
10 question the integrity and security of  
11 technologies.

12 That has a real world economic impact.  
13 In fact, there are a number of analyses out there  
14 that put the numbers of the impact in the tens of  
15 billions of dollars.

16 As significant, perhaps even more  
17 significant than the economic loss is the broader  
18 societal impact and the implications for the  
19 Internet more generally. We're celebrating this  
20 year the 25th anniversary of the commercialization  
21 of the Internet and are all very familiar with the  
22 benefits and the way it's transformed all of our

1 lives.

2           Increasingly, what we're seeing though  
3 are policies aimed at changing the open,  
4 ubiquitous, globally-integrated Internet into one  
5 of walled silos. And so the legislation that's  
6 actually being debated today in Brazil would  
7 create walled gardens around their data.

8           And it's not simply limited to Brazil.  
9 We're seeing the same in Europe, as you all know,  
10 where the parliament is questioning the continuing  
11 viability of the safe harbor, or in particular  
12 territories within Europe where they're calling  
13 for country-specific clouds that would again  
14 create these islands of walled silos rather than  
15 an open, integrated Internet, which we all know  
16 the implications of that.

17           And so what do we do about it? I'll  
18 offer up three sets of solutions that build on  
19 global principles that we released earlier this  
20 year after working with our members to forge  
21 consensus on it.

22           And I place the emphasis on global

1 because we firmly believe that in order to address  
2 these issues and to address them effectively, high  
3 level, global communication and engagement around  
4 surveillance is critically important.

5           The first aspect or screed of solutions  
6 is around transparency. This body, the PCLOB in  
7 its January report made the point that  
8 transparency is the foundation for democratic  
9 principles. We firmly agree. We also think it's  
10 the foundation for separating fact from fable.

11           And so to the extent that there's a  
12 greater awareness, particularly around 702 where  
13 there are protections in place already, for there  
14 to be greater awareness about that would be quite  
15 helpful.

16           As it relates to our companies, the  
17 ability to share with the public more about 702  
18 and 215 and the requests that come in pursuant to  
19 those, as well as the accounts, particularly the  
20 numbers, would be incredibly helpful. And so  
21 greater transparency is one element of what we  
22 would recommend.

1           The second relates to oversight. And  
2 as I've said in other places, including my  
3 testimony on the hill, our solutions are offered  
4 with a great deal of humility because we don't  
5 know what we don't know. I don't pretend to be  
6 able to offer the exact framework for making sure  
7 that there is a civil libertarian advocate or a  
8 civil liberties advocate within the FISA or FISC  
9 court process. But developing a framework for  
10 enabling that, we think is very important.

11           Finally, the last set of solutions are  
12 based on working to rebuild the trust that has  
13 been eroded, and there, a few unequivocal  
14 statements from our government would be quite  
15 helpful.

16           By way of example, there has been a lot  
17 of reporting around steps that may or may not have  
18 been taken to undermine encryption standards.  
19 NIST has been very firm in taking steps to make  
20 sure that they bolster the encryption standards  
21 that are being developed.

22           But a statement from our government

1 that they don't, do not intend to take steps to  
2 undermine the integrity of our cyber -- to  
3 undermine the integrity of those standards would  
4 be incredibly important.

5 Similarly, taking steps to affirm that  
6 data acquisition pursuant to 702 is not being done  
7 in an indiscriminate manner, I think would also be  
8 incredibly helpful. With that, I'll pause.

9 MR. MEDINE: Thank you. Ms. Pitter.

10 MS. PITTEr: First, thank you very much  
11 for this opportunity. Thank you for having me.  
12 We've filed a more lengthy statement with the  
13 Board so I'm just going to be a little bit more  
14 brief here.

15 I was asked to talk about U.S.  
16 obligations under the International Covenant for  
17 Civil and Political Rights so I'll start with  
18 that.

19 And obviously, I'm going to disagree  
20 with Mr. Bellinger on this issue, as did Harold  
21 Koh's recently released memo where he disagreed as  
22 well and tried to get the Obama administration to

1 take a different position, arguing that it was not  
2 actually in the U.S. interests to continue to not  
3 apply the ICCPR in an extraterritorial manner.

4           There has been debate about whether or  
5 not this treaty applies outside of U.S. borders  
6 and it stems from, as Mr. Bellinger said, the  
7 operative jurisdictional clause in the covenant  
8 which says that states have an obligation to  
9 respect and ensure that those within its territory  
10 and subject to its jurisdiction, the rights under  
11 the covenant.

12           So the word jurisdiction in that clause  
13 has been interpreted to mean power and effective  
14 control. But the U.S. does not accept that. It  
15 takes a strictly territorial stance. And this  
16 essentially means that a state has to abide by the  
17 covenant within its territory but then it can  
18 willfully violate the covenant outside its  
19 territory, killing and pillaging at will outside  
20 its borders, which doesn't really make any sense.

21           Treaty law requires that the language  
22 of the treaty be interpreted in accordance with

1 its context, as well as its object and purpose.  
2 And the context in this case was post-World War  
3 Two when the treaty drafters were aiming at  
4 empowering people with rights universally and not  
5 diminishing them, and responding effectively to  
6 Nazi atrocities.

7 To interpret the treaty in that limited  
8 way would allow, for example, Nazi Germany to run  
9 a concentration camp in Poland, as Marco  
10 Milanovic, a prominent scholar on this issue has  
11 pointed out.

12 And the U.S. is the clear outlier on  
13 this. Only the U.S. and Israel take such a strict  
14 interpretation of the treaty.

15 So how does this apply to surveillance  
16 and the right to privacy? Some have argued that  
17 even if the ICCPR applies extra-territorially it  
18 should only be in the case where the government  
19 has physical control over the individual, like in  
20 the context of detention or torture. And that  
21 doesn't apply to surveillance simply because the  
22 individual is not within a state's effective

1 control.

2 But the problem is that their  
3 communications are. And so to not recognize even  
4 a duty to respect the right to privacy in this  
5 context creates a kind of absurd situation where  
6 the U.S. would be barred from going into someone's  
7 house in Germany and taking letters out of  
8 someone's drawer but not barred from reaching into  
9 their computer and doing the very same thing  
10 remotely.

11 These are novel questions, and I won't  
12 deny that. The Human Rights Committee, which is  
13 the main interpretive body of the ICCPR, has not  
14 adjudicated this matter.

15 And though there is a body of case law  
16 in other jurisdictions, particularly in the  
17 European Court of Human Rights, that have the  
18 issue and they do provide some guidance on a  
19 framework for how to analyze surveillance laws.

20 That said, those decisions, they came  
21 out before the Snowden revelations so they're not  
22 informed by a lot of the information that's come

1 in the public domain about the vastness of the  
2 collection that's going on.

3 But these issues are novel in the U.S.  
4 too. Just because there may not be necessarily a  
5 case en point does not mean the obligations or the  
6 rights don't exist. They are in the treaty.

7 Just as like many in the U.S. have  
8 argued that U.S. law has to catch up with  
9 technology and recognize a reasonable expectation  
10 of privacy in metadata, international law has to  
11 acknowledge that when it comes to surveillance,  
12 though an individual may not necessarily be in a  
13 state's physical control, their communications  
14 are, and the right to privacy can be violated  
15 remotely through technical means.

16 But just because the obligation applies  
17 extra-territorially does not mean that the  
18 surveillance has to stop. There is a framework  
19 within which surveillance can take place, but also  
20 be in accordance with human rights obligations.  
21 The surveillance has to be lawful and  
22 non-arbitrary and necessary to a legitimate cause

1 that's proportional to that legitimate aim.

2 By all accounts, that's not what 702  
3 is. 702 may all be for the purpose of protecting  
4 U.S. national security, which would be a  
5 legitimate aim, but are there more narrowly  
6 tailored ways to achieve that aim?

7 And if the answer to that question is  
8 no, and I'm going to quote from the review group  
9 here, the question is not whether granting the  
10 government authority makes us incrementally safer  
11 but whether the additional safety is worth the  
12 sacrifice in terms of individual privacy, personal  
13 liberty, and public trust. And also, is it really  
14 worth the other harms that will result?

15 We're in a situation now in which  
16 countries are rushing to enact laws that would  
17 localize data collection and companies are rushing  
18 to offer alternatives to customer data being  
19 stored in the U.S.

20 And from a technological standpoint  
21 data flows are not necessarily based on geography  
22 but travel the cheapest, most efficient route.

1 This means a transfer to someone in the same  
2 country can mean data passing through many  
3 countries without the sender even knowing it. So  
4 a failure to respect the right to privacy  
5 extra-territorially imposes, exposes U.S. data to  
6 vulnerability when it's situated in other states.

7 The President has already essentially  
8 recognized all this. His presidential policy  
9 directive purports to bring the rules on retention  
10 and dissemination of data collection on foreigners  
11 closer to those that govern data on U.S. persons.

12 But it did not end bulk collection and  
13 specifically exempted data temporarily acquired to  
14 facilitate targeted collection.

15 Also, this was through an executive  
16 order not legislation, so it could be changed by  
17 future administrations.

18 The bottom line is that the U.S. is in  
19 a unique position because most of the world's data  
20 flows through its borders. And this confers an  
21 obligation to respect the privacy rights of those  
22 individuals whose communications fall within the

1 U.S. jurisdiction, but also to refrain from  
2 interfering with the ability of other countries to  
3 protect data, protect their own citizens' data.  
4 And a failure to recognize the value of this  
5 undermines U.S. business and long term national  
6 security interests.

7 The administration says it will make  
8 some changes but the law remains the same and that  
9 too has to change.

10 MR. MEDINE: Thank you. Mr. Sieber,  
11 Professor Sieber.

12 MR. SIEBER: Thank you very much for  
13 your kind invitation. It's a pleasure to be here.

14 International legal obligations for  
15 U.S. surveillance programs for which you are  
16 asking can be based on two different sources,  
17 interests of states and interests of persons. The  
18 two are interrelated since the protection of a  
19 state's territory also has effectual protective  
20 functions for its citizens.

21 Let me start therefore with a few  
22 remarks on this broader approach before turning to

1 specific human rights, which have been addressed  
2 here.

3 General international law and Article 2  
4 of the U.N. Charter protects the sovereign  
5 equality and territorial integrity of all states.

6 A state therefore violates territorial  
7 sovereignty if it accesses, copies, or manipulates  
8 non-public data in computer systems located in a  
9 foreign state because such acts initiate in data  
10 processing on the servers located in a foreign  
11 territory.

12 There are no norms in public  
13 international law that permit violating other  
14 states' sovereignty by across the board world-wide  
15 surveillance.

16 There is also no customary rule of  
17 international law that permits the infringement of  
18 sovereignty resulting from acts of espionage.

19 In addition, espionage committed from  
20 the premises of embassies violates the obligations  
21 under Article 3 of the Vienna Convention on  
22 Diplomatic Relations.

1           These infringements of the territorial  
2 integrity of many states by large scale  
3 surveillance programs have two impacts for our  
4 topic. First, with respect to policy  
5 considerations, infringements of the territorial  
6 integrity of foreign states violate international  
7 law, plus in addition also national cyber crime  
8 statutes that are globally agreed upon in the  
9 Budapest Convention.

10           These violations pose serious threat to  
11 the continuing trust and the integrity of the U.S.  
12 and its IT industry. This infringement may be  
13 more serious than the violations of privacy  
14 rights, the scope of which are controversially in  
15 dispute in most countries.

16           Secondly, transnational surveillance  
17 programs on foreign territory take over the  
18 security functions of the affected states. This  
19 transnational control deprives citizens of  
20 protection by their own state and any other legal  
21 protective systems in these security measures,  
22 since their home state cannot protect them against

1 unknown foreign violations of their privacy and  
2 the intercepting foreign state often does not  
3 recognize any aliens' rights outside its territory  
4 where the interception is taking place.

5 In such a global system the citizens,  
6 including U.S. citizens, are deprived of any  
7 protection, especially if authorities of different  
8 countries exchange certain data.

9 Thus we are all losing a protective  
10 system which mankind has won in a long historical  
11 battle dating back to the Enlightenment. Thus, if  
12 we are engaging in transnational surveillance  
13 programs we must at least recognize certain basic  
14 human rights apply to all humans, regardless of  
15 nationality and place of residence. And if we  
16 want to create an effective global solution this  
17 must be supported by international human rights,  
18 to which I will now turn.

19 In the field of international human  
20 rights I will also concentrate on Article 17 of  
21 the International Covenant of Civil and Political  
22 Rights. The International Court of Justice, the

1 U.N. Human Rights Committee, both in its case law  
2 and in its General Comment 31, as well as many  
3 national courts and governments acknowledge the  
4 extraterritorial applicability of the ICCPR.

5 I also simply refer to the well-founded  
6 memorandum presented by Harold Koh, former legal  
7 advisor at the U.S. State Department in 2010 and  
8 2013, with respect to the ICCPR. Koh is  
9 convincingly for the extraterritorial  
10 applicability of the conventions.

11 According to the prevailing opinion,  
12 the ICCPR is extra-territorially applicable to  
13 anybody within the power or effective control of  
14 the acting state party or its agents.

15 In the physical world, extraterritorial  
16 applicability of the ICCPR is thus limited to  
17 situations in which the government has total or  
18 special control, spatial control over a territory.

19 Since communications and privacy rights  
20 are by their very nature exercised in the virtual  
21 world and are prominently infringed upon there,  
22 the control of this virtual world by highly

1 extensive surveillance programs should be a  
2 decisive factor.

3           If we do not accept these conclusions  
4 we still must deal with an argument of the German  
5 Constitutional Court, which also might be relevant  
6 for the American discussion. The court argues  
7 that telecommunication interception not only  
8 infringes upon privacy rights by the first act of  
9 recording the telecommunication, it also infringes  
10 on these rights by the following data transmission  
11 to their home country, the analysis, the linking,  
12 the long-lasting storing, and by further  
13 transmissions to other recipients.

14           All these acts are repeating and  
15 deepening the infringements of privacy rights and  
16 they are undoubtedly committed on the territory of  
17 the surveilling states. Thus, even in cases of  
18 foreign intelligence gathering, we are not dealing  
19 only with actions outside the national territory.

20           Accepting the arguments for the  
21 transnational applicability of specific  
22 international human rights would promote then a

1 deeper discussion on the substantive scope of  
2 international human rights protection of privacy.

3 A first attempt to define the contours  
4 of the international concept of privacy can be  
5 seen in the already mentioned U.N. General  
6 Assembly Resolution 68167 of last December on the  
7 right to privacy in the digital age.

8 When this discussion proceeds, it will  
9 be most important to recognize that threats from  
10 abroad are different from internal threats. Thus  
11 the principle of proportionality as developed by  
12 international and national courts will lead to  
13 very different results in different circumstances,  
14 such as for data collection to homeland, in  
15 Afghanistan, or today in the Ukraine.

16 These necessary differentiations under  
17 the principle of proportionality can recognize  
18 many U.S. security concerns. Thus applying  
19 certain transnational privacy rights would not  
20 prevent a reasonable security policy, especially  
21 also since the ICCPR is self-executing in the  
22 U.S.A. and national foreign citizens could not

1 initiate judicial proceedings against the U.S.

2 In sum, I would advocate for an  
3 international solution and discussion in order to  
4 maintain or regain the leading role of the U.S. as  
5 an advocate for the rule of law and human rights  
6 in democratic societies, as well as for the trust  
7 in its IT industry and its clouds.

8 If time is not yet ripe for an  
9 international human rights solution, then more  
10 emphasis should be placed on national efforts to  
11 provide more guarantees for non-U.S. persons.

12 For that reason I welcome the  
13 respective U.S. Presidential Directive 28 of last  
14 January to applying certain safeguards for all  
15 individuals, regardless of the nationality of the  
16 individuals to whom the information pertains or  
17 where that individual resides.

18 This policy is also the position of the  
19 German constitutional law. In case of your  
20 interest it would be a pleasure for me to provide  
21 you with more details on these comparative legal  
22 aspects later on in the discussion. Thank you.

1 MR. MEDINE: Thank you. Mr. Wolf.

2 MR. WOLF: Thank you, Mr. Chairman. As  
3 Chairman Medine said at the outset, I'm the  
4 partner in the law firm of Hogan Lovells, where I  
5 lead the firm's global privacy practice.

6 And in 2013 Hogan Lovells published a  
7 white paper examining the similarities and  
8 differences among various legal regimes that  
9 authorize and limit governmental access to data.

10 And our work began before the Snowden  
11 NSA disclosures in response to the claims of  
12 certain EU cloud service providers that storage of  
13 data in the EU made it safer from surveillance  
14 than storage with a U.S.-based cloud provider.

15 Obviously following the Snowden  
16 revelations the argument in support of allegedly  
17 secure from surveillance regional clouds has been  
18 renewed loudly.

19 A previous white paper we did on  
20 governmental access to data internationally noted  
21 the availability of mutual legal assistance  
22 treaties and other forms of cross-border

1 governmental sharing addressing faulty claims of  
2 regional cloud service providers about the  
3 invulnerability to foreign government access that  
4 local cloud storage might provide.

5           Our 2013 white paper specifically  
6 looked at Section 702 surveillance and the  
7 frameworks in Australia, Canada, France, Germany,  
8 and the United Kingdom. My written and oral  
9 testimony today synthesizes the findings from this  
10 white paper and includes additional information on  
11 similar laws in Brazil, Italy, and Spain that we  
12 intend to publish soon.

13           I will note that our white paper  
14 foreshadowed last week's report of the European  
15 Parliament criticizing the practices of certain EU  
16 member states for the lack of transparency and  
17 controls on their surveillance activities.

18           My principle point today following our  
19 white paper is straightforward. While the  
20 policies and practices of the United States  
21 addressing surveillance and related privacy  
22 concerns obviously need to be and are being

1 reassessed, the U.S. has on its books greater due  
2 process and independent oversight of surveillance  
3 activities than many of our fellow democracies.

4 As you know, Section 702 surveillance  
5 requires court approval, surveillance is limited  
6 to foreign intelligence information, and oversight  
7 mechanisms exist for 702 surveillance.

8 As our white paper revealed those same  
9 limitations are not always found in the law of  
10 many of our counterparts. Australia, Canada,  
11 France, Germany, Italy, and the United Kingdom do  
12 not require court approval for national security  
13 surveillance.

14 In France, the intelligence agency is  
15 allowed to conduct surveillance to protect  
16 economic and scientific assets, even when national  
17 security interests are not at stake.

18 On the issue of intelligence agencies  
19 secretly and without any process at all asking  
20 companies for data, we have found that Australia,  
21 Canada, France, Germany, and the U.K. allow their  
22 governments to ask private entities voluntarily to

1 disclose data to the government.

2 In the U.S. the government is not  
3 allowed to seek voluntary transfers. A neutral  
4 judicial body must approve the government's  
5 request for data.

6 Last week's resolution by the European  
7 Parliament recognized extensive surveillance  
8 systems in EU member states, and the lack of  
9 control and effective oversight that some EU  
10 member states have over their intelligence  
11 community.

12 The resolution also questioned the  
13 compatibility of some member state's massive  
14 economic espionage activities within the EU, with  
15 the EU internal market and competition laws. The  
16 parliament did not go into the detail of our white  
17 paper, but its resolution reflected the baseline  
18 findings of our research, that there are  
19 substantial deficiencies in transparency about and  
20 controls over national security access to data in  
21 countries outside the U.S.

22 Thus when also considering the cross-

1 border sharing arrangements available to  
2 governments for information they collect through  
3 surveillance, it is misleading in the extreme to  
4 contend that so-called regional clouds provide  
5 individuals with security from government  
6 surveillance.

7 I commend this Board for engaging in an  
8 assessment of U.S. surveillance practices and  
9 looking at how these practices relate to our  
10 counterparts. There are no guarantees in the U.S.  
11 or elsewhere that agencies will abide by the laws  
12 restricting national security surveillance, but  
13 the degree of authorization required and the kind  
14 of review that occurs is obviously relevant to a  
15 determination of how well personal privacy and  
16 personal liberty are protected.

17 Thank you again for the opportunity to  
18 present the findings of our white paper and I'll  
19 look forward to your questions.

20 MR. MEDINE: Thank you very much.

21 I want to turn to the ICCPR for a  
22 moment, and as I understand it there are really

1 two issues here. One is the jurisdictional test,  
2 and if you pass that then the substantive test  
3 with regard to evaluating whether the 702 program  
4 affords appropriate protections or is arbitrary in  
5 some fashion.

6 I want to start with the jurisdictional  
7 issues, and that is, I guess there are three  
8 interpretations of the applicability of the  
9 treaty. One is that there has to be both  
10 territorial presence and jurisdiction. The other  
11 is there could be one or the other. And I guess  
12 the co-approach, which is they sort of split it,  
13 and that is there is a respect requirement across  
14 the board and an ensure requirement only subject  
15 to the territorial and jurisdictional issues.

16 I want to ask about the jurisdictional  
17 side. As we know from discussion earlier today  
18 and what's been made public is the information  
19 that's being collected under the 702 program is  
20 being collected in the United States, albeit about  
21 non-U.S. persons.

22 I guess my question is for the

1 panelists, how should we, how should one interpret  
2 jurisdiction? It's not going to be up to us to  
3 interpret it, but in terms of understanding  
4 jurisdiction, is it jurisdiction over the  
5 information, which may be here, is it jurisdiction  
6 over the person, who may be elsewhere? And how  
7 would that apply, both in sort of friendly and  
8 unfriendly countries, in terms of the scope of our  
9 responsibilities?

10 MR. BELLINGER: I'll take a stab at  
11 that. Let me say a couple of things. One, just  
12 to reiterate that the U.S. has in fact reaffirmed  
13 its position again that the ICCPR does not apply  
14 extra-territorially and the point that the  
15 individuals have to be under the power and  
16 control.

17 You know, I get sort of the novel  
18 suggestion that anybody who is subject to  
19 electronic surveillance is therefore under U.S.  
20 power and control. But I don't think that's  
21 actually a credible argument.

22 Even the Human Rights Committee I think

1 would not go so far as to say that if one can  
2 touch a foreign national through surveillance that  
3 that is someone who is under U.S. power and  
4 control.

5           The fact that the surveillance may be  
6 then collected ultimately inside the United States  
7 I think does not change the fact that the  
8 collection is being done of persons who are  
9 outside the United States. And so I think that  
10 does not change the, either the essential  
11 jurisdictional element that it does not apply  
12 extra-territorially outside the United States, and  
13 that those individuals are within the power and  
14 control of the United States.

15           Again, these are things that one might  
16 wish were so, and I'm not sure that there's as  
17 much of a disagreement between me and Laura Pitter  
18 as she suggests.

19           If one were writing a new treaty and  
20 could get people to agree to certain things one  
21 might agree that there might be, you know, policy  
22 limitations that one might accept.

1           But the way this particular treaty is  
2 written now, certainly the view of the United  
3 States government, and I frankly think I am not  
4 aware of any single government in the world, and I  
5 mean this is what I mean, governments who believe  
6 that their right to conduct electronic  
7 surveillance of people outside their territory is  
8 controlled by the ICCPR. I would be very  
9 surprised if we found any European government, as  
10 upset as they might be with electronic  
11 surveillance by the United States, who would say  
12 the Article 17 of the ICCPR limits our ability to  
13 collect outside our borders.

14           And in fact, the German government in a  
15 submission made to the European Court of Human  
16 Rights interpreting the European Convention on  
17 Human Rights argued that that convention did not  
18 limit its electronic surveillance of Uruguayans  
19 outside of Germany.

20           So again, the view of governments is  
21 that this does not have jurisdictional control  
22 over people who are outside their territory.

1                   MR. MEDINE: I just wanted to follow  
2 up. What is the scenario where someone would be  
3 in our territory and not within our jurisdiction?  
4 Because the statute, the treaty says both  
5 territory and jurisdiction. Are there other  
6 situations where one would apply but not the  
7 other?

8                   MR. BELLINGER: Well, certainly there  
9 would be people who would be, theoretically there  
10 could be people who are not in our territory and  
11 who could be subject to our jurisdiction. That  
12 was the problem that Eleanor Roosevelt was trying  
13 to solve at the time, to think about what the  
14 converse might create.

15                   MR. MEDINE: Okay, thanks. Ms. Pitter.

16                   MS. PITTER: Well, first of all, the  
17 German position was taken in 2008 before these  
18 revelations came forward and they've since  
19 sponsored a U.N. resolution which underscores the  
20 importance of respecting the right to privacy.

21                   So I would say that, you know, Koh's  
22 interpretation is that there's on the one hand a

1 duty to ensure the rights in the covenant to those  
2 within a state's territory and jurisdiction, and  
3 then there's also a duty to respect the rights of  
4 individuals outside of the territory, the actual  
5 territory of the United States.

6 So there's the duty to respect is  
7 what's important here, and so there is an  
8 obligation under the ICCPR, even with the  
9 jurisdictional clause, to respect the rights to  
10 privacy of those outside the United States.

11 But this all, as you said, is happening  
12 in the United States. I mean the data is flowing  
13 through U.S. borders, although I'm not sure about  
14 the backbone upstream collection, where exactly  
15 that's taking place. So absolutely, yeah,  
16 absolutely, I mean I think that it would be the  
17 duty to respect the right to privacy is what's  
18 implicated here.

19 MR. MEDINE: Thank you. Judge Wald.

20 MS. WALD: I've got two questions I  
21 think for Mr. Bellinger. First is I think we  
22 recognize that the government has now reaffirmed

1 its earlier position about what the ICCPR means in  
2 relation to people abroad. But I wondered if  
3 you'd just say a word about how they dealt with  
4 the question of Article 31 of the Vienna  
5 Convention on the interpretation of treaties  
6 insofar as, as I remember it, you know, deference  
7 should be given to the official interpreters of  
8 the -- which in this case I believe, you know,  
9 have taken a much broader interpretation of that.

10 And I think a couple of our Supreme  
11 Court justices have said in several cases that  
12 when you're interpreting, when they're  
13 interpreting a treaty one should look to the  
14 interpretations, maybe for guidance, maybe not  
15 controlling, of other parties to the same treaty.  
16 Just a word or two on those two aspects of the  
17 reasoning which led to what is, is the  
18 reaffirmance of it.

19 MR. BELLINGER: Right, and I think what  
20 you're talking about is the General Comment 31 of  
21 the Human Rights Committee.

22 MS. WALD: Yeah, yeah.

1 MR. BELLINGER: Which certainly in the  
2 view of the United States, and again, I'm not  
3 aware of any government in the world who believes  
4 that the views of the Human Rights Committee  
5 actually are legally binding.

6 The Human Rights Committee was set up  
7 to monitor compliance and it makes statements  
8 which governments, including the United States,  
9 give respect to but we certainly don't, neither we  
10 nor other countries believe that that is the  
11 definitive interpretation of the treaty, nor do we  
12 believe that it's legally binding.

13 MS. WALD: Okay. My second question --

14 MS. PITTER: I was just going to add,  
15 sorry.

16 MS. WALD: Go ahead.

17 MS. PITTER: That it is, the Human  
18 Rights Committee is a very authoritative source  
19 regarding the interpretation of the covenant. And  
20 I mean the U.S. is under an obligation to give  
21 effect to the rights in the treaty in good faith.  
22 So what the Human Rights Committee has said in

1 that regard is very important.

2 MR. BELLINGER: And if I could just  
3 say, because these are important points right now,  
4 including for treaties, frankly the Human Rights  
5 Watch is extremely interested and having gotten  
6 through the senate the U.N. Convention on  
7 Disabilities.

8 So you know, Human Rights Watch can  
9 speak for itself, but certainly the view of the  
10 U.S. government and of most human rights  
11 organizations is that the statements made by these  
12 treaty compliance groups, while due great respect,  
13 are not binding on the United States.

14 If they were in fact considered to be  
15 binding on the United States, those would in fact  
16 fundamentally change U.S. obligations under the  
17 treaties and we would never get any treaties  
18 through the senate, including the treaty that both  
19 Laura and I would very much like to get through  
20 the senate, the U.N. Disabilities Convention.

21 MS. WALD: Okay. My second question  
22 very quickly is that acknowledging what

1 everybody's about, that this big debate in the  
2 international world will continue probably despite  
3 the most recent position we've taken, and given,  
4 you know, all of the people allied with it, the  
5 official interpreters, whatever they're called,  
6 Harold Koh, Sara Cleveland, Manfred Nowak, who's  
7 the U.N.'s leading expert on the ICCPR, my  
8 question to you deals with the last paragraph of  
9 your both oral and written testimony, and that is  
10 that you would see no problem with a policy which  
11 gave greater consideration to the rights of  
12 non-U.S. persons within the surveillance context,  
13 alluding to the fact that the President in his  
14 directive suggested that.

15 But I'm wondering if you, having served  
16 the position you did as counselor in the State  
17 Department, have any more specific ideas about in  
18 this context 701, or maybe even in other  
19 surveillance programs we could do just that?

20 MR. BELLINGER: Thank you, Judge. It  
21 is a great question. I have not actually given a  
22 lot of thought to that.

1 MS. WALD: Maybe a little.

2 MR. BELLINGER: My general sense from  
3 the surveillance that I saw was in fact that we  
4 are very targeted on specific intelligence  
5 requirements.

6 These are not broad dragnets of the  
7 surveillance of average individuals and so this is  
8 not a great violation of the rights of privacy of  
9 every single foreign national, that's very much  
10 focused on individuals who may pose a national  
11 security threat or for which the United States has  
12 a valid intelligence interest.

13 MS. WALD: Would you, for instance,  
14 think that taking national security, assuming you  
15 didn't have a national security risk, that  
16 basically non-U.S. persons we should try to  
17 approximate as much as we can within those  
18 restrictions the equal treatment in use,  
19 retention, that kind of thing of non-U.S. persons  
20 in our surveillance, or not?

21 MR. BELLINGER: I think that some of  
22 the things that the Obama administration,

1 President Obama has been focusing on to ensure  
2 that, particularly for the information that is  
3 collected, that we ensure that it is kept private.

4 I mean I would be personally, I haven't  
5 seen this happen, but I would be personally  
6 extremely concerned if we found that the United  
7 States had collected information about foreigners  
8 great or small, either a world leader or a lesser  
9 known person, and then we're not careful with that  
10 information and were to let it out. That would  
11 very much interfere with that individual's right  
12 to privacy.

13 I think, you know, as a national  
14 security official it's important for us to collect  
15 the information that we've collected, but we need  
16 to be extremely careful with it. So my sense is  
17 that as a policy matter these privacy concerns are  
18 important.

19 MR. MEDINE: Mr. Dempsey.

20 MR. DEMPSEY: My question I guess for  
21 Laura Pitter and maybe also for Mr. Sieber. Among  
22 the major, certainly the countries that Chris Wolf

1 looked at and cited, but among the other major  
2 democracies that do foreign intelligence  
3 surveillance, is there anyone that has a law which  
4 you would point to as a better model?

5 MR. SIEBER: Could you ask the  
6 question?

7 MR. MEDINE: Is there a country that  
8 has a better model of surveillance than ours? Is  
9 that --

10 MR. DEMPSEY: Yeah. In other words,  
11 what other country has a better model, a better  
12 law, more checks and balances, more controls, more  
13 limits?

14 MR. SIEBER: In general.

15 MR. MEDINE: In general, checks and  
16 controls balancing privacy and civil liberties and  
17 national security.

18 MR. SIEBER: It's a very broad  
19 question --

20 MR. DEMPSEY: Just pick one.

21 MR. SIEBER: Because you have to  
22 consider many, many aspects, not only the

1 extraterritorial implication. I just can give you  
2 some reliable differences a between the German  
3 system and the U.S. American, that's what I can  
4 witness on.

5           If you have a look at the German system  
6 you have to see that Germany has a very strong  
7 constitutional court and is very much attached to  
8 fundamental rights. This is a reaction to the  
9 Nazi cruelties and any steps towards this  
10 direction should be prevented. This is the reason  
11 for some very basic differences between the U.S.  
12 and Germany.

13           The first one, for example, is that  
14 intelligence agencies in Germany have no executive  
15 powers. So they cannot execute arrest warrants or  
16 anything like that. They just can collect the  
17 information. This is based on the idea that the  
18 lack of control which we have in this area of  
19 intelligence agencies must be balanced by lesser  
20 constrained measures.

21           Secondly, Germany has constitutionally  
22 founded strong separation of powers and separation

1 between the police and the intelligence agencies.  
2 This has been changed a little bit after 9/11 but  
3 still there is a fundamental separation.

4 Information exchange is only possible  
5 in a very limited way for very, very serious,  
6 serious crimes.

7 So I would say the differentiation  
8 between the institutions is stricter. We don't  
9 have multipurpose institutions like the FBI.

10 On the institutional side there is an  
11 absolute strong separation between these  
12 institutions, despite certain common datas and  
13 things which we have done after 9/11.

14 You could go further, if I compare it  
15 and look around at the control agencies which you  
16 have. In Germany it's separated. For internal  
17 surveillance we have a special commission  
18 appointed by the parliament, G-10 Commission who  
19 is doing the job. It's not called a court but the  
20 functions are similar.

21 And for foreign intelligence agency,  
22 the BND, there is a parliamentary commission who

1 does these things.

2           Maybe one last point, if you look at  
3 the aspect of protection of foreigners' rights and  
4 applicability of the constitution abroad, the  
5 German attitude is more in favor of applying the  
6 national constitutional guarantees.

7           With respect to the first question,  
8 which is foreign territoriality, section 1 of the  
9 basic law says that the basic law binds all public  
10 authority. And this is in general irrespective of  
11 whether it's in the country or outside the  
12 country.

13           There are differences of course, but  
14 they have more to do with the different  
15 circumstances, because the risks coming from  
16 abroad might be bigger than coming from within the  
17 countries, and for that reason I absolutely agree  
18 that the systems might be different for internal  
19 intelligence and external.

20           But it's not based on the fact that we  
21 do not apply the constitutional guarantees abroad,  
22 and it's definitely not based on the fact that we

1 are giving different rights to foreigners and to  
2 citizens, at least in this area of dignity rights,  
3 of human rights, and especially in the privacy  
4 rights.

5 So for example, there was a German  
6 decision of the court which was controlling  
7 intelligence gathering for abroad and which  
8 checked these systems.

9 So with respect to this question which  
10 we are dealing here, if I generalize it I would  
11 say we are more open to applying these  
12 fundamental rules. We do not reject it as it's  
13 not applicable. We don't go into these  
14 (inaudible) stay out of it. We would apply it,  
15 but then we have a proportionality principle and  
16 we check whether the things are justified.

17 And for example, in this decision I  
18 mentioned, the court said, yes, dangers coming  
19 from abroad are bigger, bigger dangers, and with  
20 balances and this law was in general justified  
21 with one exception.

22 It was applied also by law to internal

1 conflicts, and the constitutional court said it  
2 cannot apply just like that.

3 So I think these are the main interests  
4 which I could tell you. It's impossible to say  
5 better or worse. I would never, never do that.

6 MR. MEDINE: Thank you. Ms. Cook.

7 MR. DEMPSEY: We'll come back around.

8 MR. SIEBER: And if you permit  
9 afterwards I would like to say a few words with  
10 these International Convention 17, the  
11 applicability, but I don't want to --

12 MR. MEDINE: We'll come around at the  
13 end.

14 MS. COLLINS COOK: So I wanted to thank  
15 you all for coming and to congratulate you for  
16 being the panel that has come the farthest set of  
17 distances to participate today. I think it's very  
18 helpful to have this type of discussion in an open  
19 forum.

20 We've talked a fair amount today and  
21 all through the day about skepticism about U.S.  
22 law and U.S. practices. I think it's fair to say

1 there is also a high degree of skepticism about  
2 the contours -- let me get closer here.

3 I think it's fair to say that there's a  
4 high degree of -- if I can get through this  
5 question without hurting someone, this is really  
6 going to be my goal for the day.

7 (Laughter)

8 MS. COLLINS COOK: There's a high  
9 degree of skepticism about the contours and  
10 applicability of international law as well. So  
11 having experts who are able to speak to these  
12 issues is critical, I think, to us.

13 And I wanted to draw off of something,  
14 Professor Sieber, that you had mentioned and I  
15 have to confess it was not a focus of mine coming  
16 into today. I had been focused on the ICCPR and  
17 the potential applicability of Article 17.

18 But you talked about the interests of  
19 states, and if I understood what you said  
20 correctly, that the interest of a state in its own  
21 sovereignty is inviolate, that surveillance by one  
22 country in another country is a violation of that

1 sovereignty, there is no exception under customary  
2 international law that would make that any less of  
3 a violation of the state's sovereign status or  
4 rights.

5           So that's the academic point. That  
6 would lead me to think that no one was conducting  
7 surveillance on anyone else, that no country is  
8 doing surveillance.

9           But as a practical matter I think it's  
10 fair to say that every country is either engaging  
11 in foreign intelligence collection or attempting  
12 to engage in foreign intelligence collection.

13           So if you can explain to me how you can  
14 have a principle of customary international law,  
15 here the absence of an exception that is honored  
16 by not one country in the world, as I understand  
17 it.

18           MR. SIEBER: Yes, I remain with the  
19 saying that there is no permission of espionage  
20 under international law because the principle of  
21 self-defense, that needs an armed conflict for it.  
22 It's not there for the ordinary case.

1           And customary law would require an  
2       *opinio juris*, the conviction of the people that  
3       espionage is right.

4           But our estimations, that are split.  
5       If we are considering our own law, we say, yes, we  
6       do it and we give them a medal if they are  
7       successful. If we are considering the other, we  
8       say it's illegal.

9           So there are two regimes of law which  
10       come to different results. We live with that but  
11       we cannot say that international law has a general  
12       view that we can, that we can do it.

13           We have this problem in a very  
14       interesting case with the German reunification  
15       because when the two parts of Germany came  
16       together, there have been people doing espionage  
17       in East Germany and they are now under our  
18       jurisdiction.

19           This question came up and here again  
20       the Constitutional Court said there is no general  
21       violation of international law, and I think you  
22       agree with that. We have to live with this

1 conflict.

2           And in the global world that's normal.  
3 The world is getting so diverse that we have many  
4 conflicting regimes today now, so we can stand  
5 with that.

6           MS. COLLINS COOK: So I guess my  
7 question, perhaps Mr. Bellinger, you can speak to  
8 this, is it a violation of international law in  
9 terms of infringing the interests of another state  
10 to engage in sort of foreign surveillance?

11           MR. BELLINGER: I was going to jump on  
12 that as well. And the answer to that I think is  
13 clearly no. I am not aware of any country who  
14 believes that the U.N. Charter's statement on the  
15 protection of territorial integrity and sovereign  
16 equality of states actually prohibits electronic  
17 surveillance of another country.

18           Certainly if that were the  
19 understanding of our senate that in becoming party  
20 to the U.N. Charter that prohibited us from spying  
21 on another country because it would violate their  
22 sovereign equality or territorial integrity, then

1 we would get out of the U.N. Charter immediately.

2 But I am not aware that any other country believes  
3 that as well.

4 So there is not, the principle of  
5 territorial integrity and sovereignty would apply  
6 to, say, for example, use of force. International  
7 law does not prohibit electronic surveillance or  
8 spying. Domestic law may.

9 And so that's really, you know, when we  
10 talk about international law, that basically means  
11 that there is a compact between countries. Judge  
12 Wald knows this very well, you know. Countries  
13 have to have agreed that they are not going to do  
14 these things to each other.

15 And in the U.N. Charter, the U.N.  
16 Charter was not saying we promise not to spy upon  
17 one another, we were saying we promise not to use  
18 force against one another.

19 U.S. surveillance in another country  
20 might violate the other country's law, but it is  
21 not a violation of international law.

22 MR. MEDINE: Let's go on to another

1 question. We'll give Ms. Brand a chance and then  
2 we'll come back.

3 MR. SIEBER: Because I think I have to  
4 contradict.

5 MS. BRAND: All right. Let's see if  
6 this microphone will work now.

7 Thank you all for being here today.  
8 One of the things I find frustrating about this  
9 discussion, not here specifically but in general  
10 is that there is a tendency to not distinguish  
11 between what is law and what is -- it's not  
12 working is it?

13 And what is either what people would  
14 like to be the law or what is a matter of policy.

15 And John, thank you for making that  
16 distinction very clearly in your remarks.

17 I was having a little bit of a harder  
18 time, Laura, following where you were moving from  
19 what you think is actually binding law to what is  
20 not.

21 And so I wanted to know if we are  
22 looking, setting aside policy, aspirational policy

1 for a moment, if we were trying to determine  
2 whether what the government is doing under 702 is  
3 legal, do you think there is some binding  
4 international law instrument that affects that  
5 questions?

6 MS. PITTER: Yes. I mean from my  
7 position it is a violation of Article 17 of the  
8 International Covenant on Civil and Political  
9 Rights. The United States does not recognize  
10 that, and that's part of the problem.

11 MS. BRAND: So let me just ask a  
12 question then. If the U.S. government doesn't  
13 recognize that, what is the body, what is the  
14 document, what is it that then makes that law  
15 binding on the U.S., on the agencies implementing  
16 702?

17 MS. PITTER: It's the treaty itself.  
18 As Mr. Bellinger said, you know, a treaty is  
19 something that governments have agreed to abide by  
20 and to honor the commitments in the treaty in good  
21 faith.

22 MS. BRAND: And what is the body that

1 has the last say on the interpretation of the  
2 treaty, right? Because obviously the U.S.  
3 government interprets the treaty differently from  
4 the way you interpret the treaty.

5 Is there some other body besides the  
6 U.S. government itself whose interpretation of the  
7 treaty is then binding on the way the U.S.  
8 agencies implement it?

9 MS. PITTER: Well, the Human Rights  
10 Committee is one of the most authoritative sources  
11 on this, but --

12 MS. BRAND: But is it legally binding,  
13 right? That's my question, not is it persuasive,  
14 is it binding?

15 MS. PITTER: I mean from the opinion of  
16 many other governments it is. The treaty is  
17 binding upon them. The United States does not  
18 recognize the extraterritorial application of it.

19 MS. BRAND: And this is an honest  
20 question, give me an example of a country that  
21 views the ICCPR to have extraterritorial  
22 application with respect to surveillance of

1 foreigners abroad that itself that takes its own  
2 advice or heeds its own interpretation.

3 MS. PITTER: So this surveillance, as I  
4 said, is a novel issue. It's not something that's  
5 been addressed by the case law, and especially not  
6 since the revelations from Snowden which have  
7 disclosed, I think even to policy makers in many  
8 countries, the degree to which the law, the  
9 domestic law on the books is actually being  
10 applied, and the vastness of the programs, how  
11 much data is actually being collected.

12 So it's a novel interpretation, I mean  
13 it's a novel question, as it is in the United  
14 States --

15 MS. BRAND: I'm sorry to cut you off  
16 but we have a strict timekeeper here, the  
17 Chairman, and I want one last question.

18 I'm interested in your interpretation  
19 of what constitutes control and how being  
20 surveilled essentially would put someone within  
21 the control.

22 My concern about that interpretation in

1 part is that I'm not sure what meaning is left in  
2 the phrase, under its jurisdiction. If the  
3 statute talks about territory and jurisdiction, if  
4 jurisdiction means something in addition to  
5 territory, it seems like a meaningless phrase if  
6 it can include surveillance.

7 MS. PITTER: Well, it is meaningless in  
8 the sense that the United States has taken up,  
9 used the technology to conduct surveillance on a  
10 very mass scale. So it affects an enormous number  
11 of people.

12 The, you know, jurisdictional clause  
13 has been interpreted extra-territorially in the  
14 context of detention and torture, in which a  
15 smaller number of people have been affected. But  
16 when you're talking about surveillance --

17 MS. BRAND: But detention, I mean  
18 someone being detained or tortured is, I would  
19 say, much more clearly within the control of the  
20 government who has detained or is torturing them,  
21 right?

22 So my question is when you get into

1 surveillance and the person is clearly not within  
2 the physical custody of the government in  
3 question, what is it within the ambit of the  
4 treaty?

5 MS. PITTER: So you can look at it two  
6 ways there. You know, their communications are  
7 within the effective control of the government and  
8 so that's one way to look at the obligation.

9 But in addition, they have an  
10 obligation to ensure the rights within the  
11 covenant territorially, but also to respect the  
12 rights in the covenant extra-territorially.

13 So although they are not necessarily  
14 bound, you know, to enact legislation domestically  
15 regarding, you know -- well, they're not  
16 necessarily bound to ensure the rights of  
17 individuals with regards to privacy  
18 extra-territorially, they are bound to respect  
19 those rights extra-territorially.

20 MS. BRAND: I see my time is up.

21 MR. MEDINE: Mr. Garfield, in your  
22 statement earlier you indicated that the

1    revelations about the surveillance programs,  
2    particularly 702, has had significant  
3    international impact with regard to business  
4    dealings with U.S. firms, and you proposed a  
5    number of steps to ameliorate that, and I wanted  
6    to ask you about some of them.

7                   And you also mentioned one of them,  
8    namely transparency in your remarks earlier. Do  
9    you have thoughts about what level of transparency  
10   would be helpful to companies, but taking into  
11   account national security concerns?

12                   As you know, our first report on 215  
13   did recommend greater transparency, but in terms  
14   of disclosures that a company can make about  
15   surveillance requests from the U.S. government, so  
16   long as that took into account national security.

17                   And I guess in particular if you have  
18   comments on the agreement that was reached between  
19   the Department of Justice and a number of firms,  
20   whether that agreement goes far enough and  
21   provides sufficient detail to give comfort to  
22   business partners of those firms overseas.

1           MR. GARFIELD: Thank you for the  
2 question, first of all. The agreement with the  
3 Justice Department is viewed as a significant step  
4 forward. There are additional steps that can be  
5 taken that would be helpful as well.

6           One is the level of detail that the  
7 companies are able to share, including  
8 disaggregation of data between Section 215 and  
9 702, or whether it's a national security letter.  
10 So a greater level of granularity would be  
11 helpful.

12           The second part of that is it is not  
13 only important that the companies be able to share  
14 out information but that the government share  
15 information as well and provide greater  
16 transparency, which is often lost in these  
17 discussions.

18           The debate that's been taking place  
19 today speaks to the importance of greater  
20 transparency because 702 already includes a number  
21 of protections that are not generally known,  
22 particularly internationally.

1           To Christopher Wolf's point, if they  
2 were more well-known it would be clearer the  
3 extent to which steps are being taken in the  
4 United States that are not necessarily being taken  
5 in other countries.

6           MR. MEDINE: And you also recommended,  
7 made a couple of other recommendations that you  
8 put forward were oversight, the importance of  
9 oversight and in discriminant collection.

10           And I guess the question is in the 702  
11 program isn't there already oversight through the  
12 Foreign Intelligence Surveillance Court and some  
13 of the internal government processes?

14           And with regard to indiscriminate  
15 collection, I think as we heard earlier there has  
16 to be a foreign intelligence purpose, and so it's  
17 somewhat constrained. Do you think that with  
18 regard to this program it meets those  
19 requirements?

20           MR. GARFIELD: Correct. My  
21 recommendations there weren't intended to suggest  
22 that it in fact was indiscriminate. It was

1 suggested, it was a suggestion that taking steps  
2 to be clear about the protections that are in  
3 place and to the extent it is not, it is in fact  
4 not indiscriminate, to reaffirm that would be  
5 helpful as we go about doing our business  
6 internationally.

7 MR. MEDINE: And Mr. Wolf, you analyzed  
8 other country's laws and shown that they're not  
9 only not better but maybe not even as good as our  
10 laws by some criteria. What lessons should we  
11 draw from that in terms of how countries should  
12 conduct their surveillance programs?

13 MR. WOLF: So the purpose of our white  
14 paper and our research was really to be expository  
15 than to reach judgements and to pick winners and  
16 losers or to decide whose was better or best.

17 But we thought it was important in  
18 light of the claims that were being made,  
19 particularly by the cloud industry in Europe that  
20 there is national security access obviously that  
21 goes on in the EU and elsewhere around the world,  
22 and often without the controls and safeguards and

1 transparency that we have here.

2           So the overall conclusion that we  
3 reached is that this is a global problem.  
4 Obviously it's one that has been focused on  
5 intensively here in the United States because of  
6 the Snowden revelations, but it is an  
7 international issue that needs to be resolved  
8 internationally, particularly with the sharing  
9 that goes on among intelligence authorities.

10           It is heartening that the European  
11 Parliament in its resolution last week adopted the  
12 draft report that came out in January that focused  
13 on the European intelligence gathering practices.

14           We hope that the data protection  
15 authorities in Europe who've been vigorous critics  
16 of the NSA practices will comment on their own  
17 country's practices. They've been relatively  
18 silent on that, and we think the debate that has  
19 to be made should be among all those interested in  
20 privacy protection, and obviously that would  
21 include the privacy commissioners abroad.

22           MR. MEDINE: Obviously countries have a

1 lot of self-interest in conducting surveillance  
2 programs. Do you see a forum in which countries  
3 can or even should agree with the methods by which  
4 they conduct surveillance?

5 MR. WOLF: So that's well above my pay  
6 grade. I really don't have a view on that.

7 I do have, if I can just mention on the  
8 transparency point, we did a white paper in August  
9 that then general counsel of the Commerce  
10 Department Kerry cited in his speech at the German  
11 Marshall Fund that actually showed on a per capita  
12 basis access by national security and law  
13 enforcement on a per capita basis is larger  
14 outside the United States in many instances.

15 MR. MEDINE: Judge Wald.

16 MS. WALD: I have two questions for  
17 Ms. Pitter. Given what most or many observers  
18 concede are widely varying practices in different  
19 countries about surveilling their own and other  
20 country's citizens, would you advocate, as we  
21 sitting here have to make some observations, maybe  
22 recommendations on 702, would you advocate that we

1 unilaterally, we recommend unilaterally putting in  
2 place one and the same protections for non-U.S.  
3 person surveillance that we have for U.S.  
4 citizens? Or two, raising the non-U.S. citizen  
5 person protections to the level that the official  
6 bodies of these international organizations that  
7 we've talked about say they should be?

8           If you come out on the second, what  
9 specific criteria do we have to go on as to what  
10 those practices would be?

11           In other words, there's a slightly  
12 cynical end to the question, what would be the  
13 additional protections in real time to privacy  
14 interests of non-U.S. persons if the U.S. took a  
15 position that the ICCPR does apply to our  
16 activities outside territorial U.S., but that  
17 we've already met those standards, such as seems  
18 to be the case with some of the other countries  
19 who espouse the official broader interpretation of  
20 ICCPR but then go on their way, as Mr. Wolf  
21 suggested, and don't really raise those?

22           MS. PITTER: This is to me?

1 MS. WALD: Yes, this is to you.

2 MS. PITTER: So, I mean I think one  
3 clear change that needs to be made is the purpose  
4 of the surveillance needs to be much more  
5 targeted. The definition of foreign intelligence  
6 information is just much too broad. It  
7 encompasses, you know, things that, conversations  
8 that could be just about generally the foreign  
9 affairs of the United States.

10 And I know we heard in the panel  
11 testimony earlier that that is somewhat reined in  
12 by certifications but those are not public and  
13 we've not seen them.

14 There should be a lot more transparency  
15 in the law. I think the difference in the German  
16 law is that there is a lot more transparency. The  
17 capacity also is less in Germany. I mean the U.S.  
18 has vast capacity, so you know it affects a lot  
19 more people.

20 But definitely a more narrow, a more  
21 targeted approach, and applying, you know,  
22 necessary and proportionate principles to the

1 surveillance as well, I think would go a long way.

2           There's probably plenty of room for  
3 recommendations. I probably can't get into all of  
4 them here but that would be --

5           MS. WALD: In general would your  
6 standard be that there should be a presumption  
7 that we treat non-U.S. persons like U.S. persons  
8 in our surveillance activities, or rather that we  
9 go to the best practices we can pull from that  
10 people who endorse the ICCPR, even if we don't  
11 actually endorse that application?

12           MS. PITTER: So I think that there can  
13 be differences in the law itself but it has to,  
14 the differences have to be ones that don't impair  
15 the impact of the right itself.

16           So the right to privacy has to be part  
17 of, it has to be made part and parcel of the  
18 assurances, but they can be different for  
19 practical reasons when it comes to --

20           MS. WALD: Can you give us, in my  
21 remaining few seconds, some application of what  
22 you've just said to 702?

1 MS. PITTER: Well, I'd like to go into,  
2 you know, a more detailed analysis here but right  
3 now there's --

4 MS. WALD: Well, just quickly.

5 MS. PITTER: There's not a warrant  
6 requirement, for example, under 702 for  
7 individuals, but there should be -- it may be that  
8 it's not a practical requirement to have a warrant  
9 for individuals outside of the United States.

10 And it's not just individuals under  
11 702, it's also facilities and about targeting as  
12 well.

13 But the procedures that are in place to  
14 protect against sort of suspicionless, you know,  
15 there's no standard for what authority has to find  
16 before it can target an individual. The main  
17 distinguishing principle is that it's a foreigner,  
18 and that that information is going to be acquired  
19 for foreign intelligence purpose, for foreign  
20 intelligence purpose, so that is too broad.

21 MS. WALD: Okay.

22 MS. PITTER: Does that make sense?

1 MS. WALD: Yes. All right, very  
2 quickly I guess, Mr. Wolf, your testimony, you  
3 know, recited the report about the lesser,  
4 basically the lesser protections most other  
5 countries including our close allies give to  
6 privacy, at least despite some of their countries  
7 adherence to the ICCPR's broader definition of  
8 privacy, yet you also note that the economic risks  
9 to U.S.-based telecommunication companies from  
10 threats both from competing companies inside those  
11 countries and from the governments themselves that  
12 they may balkanize and insist on collection and  
13 storage activities being conducted in-country  
14 poses a real risk.

15 Is it above your pay grade to give us  
16 some indication of what line or policies the U.S.  
17 should follow given those two competing concerns?

18 MR. WOLF: Well, I think our concern in  
19 doing the work that we did on the white paper was  
20 the misperception that was arising --

21 MS. WALD: Let's assume you've done  
22 those and that they are real, but also are real

1 the threats to the competitiveness of U.S.  
2 companies if foreign governments and peoples get  
3 very excited and want to keep everything inside  
4 their own countries.

5 MR. WOLF: So our position is that  
6 they're deceiving themselves if they think that  
7 when they keep data presumably within the four  
8 borders, four corners of their own country that  
9 it's safer from surveillance, not only from their  
10 own surveillance authorities, but of course  
11 through the sharing arrangements from surveillance  
12 authorities from elsewhere around the world, and  
13 that the Balkanization of data is not a useful  
14 global phenomenon at all.

15 MS. WALD: Well, what can the U.S., or  
16 what could we recommend they bring them together?

17 MR. MEDINE: Judge, your time has  
18 expired. Mr. Dempsey.

19 MS. WALD: Right. You can think about  
20 it.

21 (Laughter)

22 MR. DEMPSEY: On my last round we were

1 talking about what were, if any country's laws  
2 that did a better job here, and Mr. Garfield, you  
3 were ready to jump in. Do you remember what you  
4 wanted to jump in on? I wanted to give you a  
5 chance to make the point, if you still remember  
6 what it was.

7 MR. GARFIELD: It really was the point  
8 that was made in response, which is that in fact  
9 our experience in carrying out our business is  
10 that there aren't many, if any, other countries  
11 that have as many safeguards in place.

12 The lack of open discussion through  
13 multinational engagement as well as transparency  
14 here in the U.S. furthers that false perception  
15 that somehow other nations are doing more than we  
16 are. And that is certainly something that whether  
17 through legislation or recommendations from the  
18 PCLOB, we can do something about.

19 MR. DEMPSEY: The question for Laura  
20 Pitter, a couple of other witnesses have raised  
21 this and a couple of times I grabbed for the book  
22 in order to raise it and didn't get a chance to,

1 the definition of foreign intelligence, as I read  
2 it, it means information that relates to the  
3 ability of the United States to protect against  
4 actual or potential attack, grave hostile acts of  
5 a foreign power, sabotage, international  
6 terrorism, international proliferation of weapons  
7 of mass destruction, or clandestine intelligence  
8 activities. None of those are too broad, I would  
9 think.

10 And then it says, information with  
11 respect to a foreign power or foreign territory  
12 that relates to the conduct of the foreign affairs  
13 of the United States.

14 I mean isn't that precisely what  
15 foreign intelligence is supposed to be about,  
16 information with respect to what foreign countries  
17 are doing that might affect our foreign affairs?  
18 Why is that too broad?

19 MS. PITTEr: I think that the first  
20 category of information that you said could, it  
21 would be permissible. But the general foreign  
22 affairs of the United States allows for the

1 collection of a vast amount of information that  
2 does not necessarily have any national security  
3 purpose.

4 MR. DEMPSEY: No, but it has foreign  
5 affairs purpose. It is by definition about the  
6 intent of foreign governments, and are you saying  
7 that other countries self-restrain themselves from  
8 trying to understand what their adversaries are  
9 doing, even in matters that don't involve attack  
10 and so on?

11 MS. PITTER: I mean if other country's  
12 laws are overbroad and vague then they're in  
13 violation of, you know, the International Covenant  
14 on Civil and Political Rights as well.

15 MR. DEMPSEY: Well, I think John would  
16 say that if everybody is doing it, it probably  
17 isn't a violation of the treaty. Everybody didn't  
18 bind themselves not to do what they all were doing  
19 at the time they bound themselves to the treaty.

20 MS. PITTER: Well, you know, the  
21 revelations about how this is applied are just  
22 coming out now and there are going to be

1 challenges and there already are challenges to the  
2 law.

3 And I think we're going to find that  
4 there is room certainly for reining in the  
5 overbreadth of some of the statutes as they  
6 exist right now.

7 I think that because it allows for the  
8 communications of things that don't necessarily  
9 have to do with national security, that it just,  
10 it's overbroad and it's impacting, you know, the  
11 United States in other ways.

12 MR. DEMPSEY: In what way is the  
13 collection of information about foreign affairs  
14 overbroad?

15 MS. PITTER: Because it could be, you  
16 know, someone talking about, you know, their  
17 opinions about the foreign affairs of the United  
18 States --

19 MR. DEMPSEY: Not someone talking about  
20 their opinions, it's the information with respect  
21 to a foreign power. So this is not Joe Schmo in  
22 Germany saying I like or don't like the United

1 States, this is about what Germany thinks about  
2 the United States.

3 MS. PITTER: It merely has to relate to  
4 the foreign affairs of the United States --

5 MR. DEMPSEY: Yes.

6 MS. PITTER: In my opinion it's too  
7 broad. It allows in for much too broad a type of  
8 communication.

9 MR. DEMPSEY: No, I'll yield. I'd like  
10 to have another round, a third round if we could,  
11 but I'll yield for now.

12 MS. COLLINS COOK: Mr. Bellinger, I  
13 think you had put your finger up midway through  
14 that and I'd like to follow on this conversation  
15 as well because it struck me.

16 First, where would you draw the line?  
17 And I'm struggling to determine what precisely is  
18 impermissible about collecting foreign  
19 intelligence in the category of foreign affairs as  
20 set forth in FISA.

21 MR. BELLINGER: Yeah, so thanks for  
22 that question. And I think this is a very

1 important point, and Judge Wald started it and you  
2 have continued it.

3 We have to be really very clear about  
4 what international law is. International law is  
5 not principles that we think would be fine, policy  
6 principles that you and I might agree.

7 International law, if we are serious  
8 about international law, and this actually is the  
9 definition of international law, are things that  
10 nations agree to, to be bound by, by treaty or  
11 that is customary internationally, meaning that  
12 countries do it so often that everybody does it  
13 and they do it by a sense of binding legal  
14 obligation.

15 So two points here, and Judge Wald, I  
16 heard you say that while it is true that other  
17 countries actually take a broader definition of  
18 whether the ICCPR applies extra-territorially, I'm  
19 not aware of any country in the world that  
20 believes that the ICCPR actually binds them with  
21 respect to electronic surveillance, that that  
22 right to privacy in Article 17 actually limits

1 their ability to conduct electronic surveillance  
2 of foreign nationals. So that is just not a  
3 treaty obligation that countries have accepted,  
4 even under the ICCPR.

5 It might be something that human rights  
6 groups wish were the case, but it is not something  
7 that governments have accepted, and certainly not  
8 something the United States government has  
9 accepted.

10 And then just one more round on the  
11 Human Rights Committee. Again, the treaty itself  
12 does not say that the decisions of the Human  
13 Rights Committee, which is basically a group of  
14 academic experts, are binding. Governments who  
15 write treaties know how to write language.

16 For example, the U.N. Charter says that  
17 we undertake to comply with rulings of the ICJ.  
18 But the human rights monitoring groups, countries  
19 have not said that we undertake to comply with  
20 their decisions.

21 And in fact, the senate, and all of you  
22 know this, the senate would never agree to cede

1 responsibility for the future interpretation of a  
2 treaty to a group of academic experts. That would  
3 take completely out of the hands of the shared  
4 understanding between the executive and senate,  
5 the interpretation of a treaty.

6 So you know, the United States, and  
7 this is the view of the Obama administration as  
8 well, you know, recognizes that other people may  
9 not agree on the extraterritorial application of  
10 the ICCPR, but you know, no country believes that  
11 the ICCPR actually limits electronic surveillance.

12 MS. COLLINS COOK: So I just wanted to  
13 as a follow-up question to Ms. Pitter. Thank you.  
14 I know we've aimed a lot of our questions at you.

15 I think there's a sense within the  
16 United States government, a little bit of  
17 exasperation, the concern is that our surveillance  
18 lacks transparency or that we are somehow outside  
19 the mainstream of what other countries are doing.

20 And I look at 702 in particular and I  
21 see something where our legislative branch has  
22 specifically said exactly what our executive

1 branch can do. The executive branch, which is  
2 headed by democratically accountable individuals  
3 then oversees the execution of that authority, it  
4 is subject to the oversight of the judicial branch  
5 and it is subject to the oversight of our  
6 legislative branch.

7 So I guess my question is systemically  
8 what else could the United States be doing to help  
9 build the confidence and trust of other countries?

10 MS. PITTER: So the oversight so far  
11 has all been in secret. I think that's one  
12 problem. I mean even the first panel today said  
13 they were in the process of declassifying a large  
14 number of documents and they were looking at doing  
15 that because they recognize the importance of  
16 transparency.

17 The oversight has not, I mean if you  
18 look at what happened with 215, even --

19 MS. COLLINS COOK: I was talking about  
20 Section 702, which is the focus of our --

21 MS. PITTER: We don't know the details  
22 of the oversight regarding 702, so the only

1 information I have about oversight would be  
2 regarding 215. And we saw that the judicial  
3 oversight in that context, you know, would up,  
4 there was an opinion that had an impact on the  
5 vast number of communications of Americans that  
6 was kept secret from the Americans, so --

7 MS. COLLINS COOK: Well, let me push  
8 back a little bit on this notion that the  
9 oversight is not transparent.

10 So again, we have a statute that tells  
11 the world exactly what the executive branch must  
12 present to the judiciary, what findings the  
13 judiciary must make, what authority judiciary has  
14 vis-a-vis that application, and the framework for  
15 this surveillance.

16 We have a public statute that also  
17 tells you exactly what the executive branch is  
18 obligated to share with Congress. So where's the  
19 lack of transparency in that?

20 MS. PITTER: Well, the judicial  
21 oversight for the 702 program is annual. They  
22 look at just the procedures. They don't actually

1 look at the individual targeting requirements.  
2 That's done by an NSA analyst at his computer  
3 desk.

4 MS. COLLINS COOK: Actually I think if  
5 you were here for the first panel the testimony by  
6 the first panel was that that is not in fact the  
7 case, that it is an ongoing process of oversight.  
8 There are regular reporting requirements, both to  
9 the court and to the Congress, so.

10 MS. PITTER: I was, I did hear the  
11 first panel, and I believe he said that those  
12 targeting decisions by the analysts are reviewed  
13 eventually, but it's not something that's done at  
14 the beginning. So the --

15 MS. COLLINS COOK: So if there's not  
16 public review of specific targeting decisions, so  
17 this, the United States government saying we would  
18 like to collect foreign intelligence information  
19 about this specific selector, that's a lack of  
20 transparency that is problematic for you?

21 MS. PITTER: Well, the transparency,  
22 even the certifications that the FISC court gets,

1 there's no, they don't even see the identifiers or  
2 the selectors, they just approve the procedures.  
3 So you know, that's a problem with the oversight.  
4 In terms of --

5 MR. MEDINE: I'm going to let Ms. Brand  
6 pick up since we're at time. So thank you.

7 MS. BRAND: Okay. I guess maybe this  
8 question is directed at John but if anyone wants  
9 to jump in, that's fine.

10 If the ICCPR did have application to  
11 the U.S. government surveillance of non-U.S.  
12 persons abroad, setting aside the territorial  
13 issue for a minute, what does privacy mean in that  
14 context?

15 I have found the lack of a universally  
16 accepted definition of privacy very frustrating  
17 writ large across everything that we do, and I  
18 mean the same issue pertains here. So I guess is  
19 there a universally accepted definition of  
20 privacy? Is there a definition of privacy that is  
21 binding on the U.S. government? If not, how would  
22 we find, who would supply such a definition? If

1 you can sort of help us understand that.

2 MR. BELLINGER: Yeah, so that's a great  
3 question. And that's really the third prong. I  
4 mean the reason that the ICCPR doesn't apply is,  
5 one, there's the within its territory and subject  
6 to its jurisdiction. Then even if it were subject  
7 to our jurisdiction, then it has to be within the  
8 power and control.

9 And you know, no one is really going to  
10 legitimately argue that, as I think you said  
11 earlier, power and control in the view of those  
12 who take that interpretation of power and control  
13 is someone that you actually physically have in  
14 your custody, not electronic surveillance.

15 And then there's the issue, even if  
16 those applied, is something unlawful or arbitrary  
17 violation of privacy? And there are not  
18 definitions that are universally accepted.

19 You know, people can argue about these  
20 things but for it to be law that a country  
21 actually violates, there has to be an agreed  
22 definition on privacy and there has to be an

1 agreed definition on what is arbitrary, and there  
2 just are not those definitions.

3           You know, again, someone can say that  
4 someone has an absolute right not to have any  
5 country pry into anything that they're doing and  
6 that that's a violation of their privacy, but  
7 there's not an accepted definition of that.

8           I mean I could frankly imagine if one  
9 were to accept the first part of your premise,  
10 which is that it were to apply extra-  
11 territorially, and let's also say that it were  
12 someone within the U.S. jurisdiction, let's say  
13 someone, the United States is actually holding a  
14 terrorist in another country and we agreed that  
15 the ICCPR applied, we agreed the person was within  
16 our power and control, and then we were to do  
17 extensive interviews of that person about the  
18 person's private life, and then we just publish it  
19 willy-nilly, not as part of a criminal proceeding  
20 but essentially just as a leak, well, you know,  
21 there might be an argument that that might be an  
22 arbitrary intervention with that person's right to

1 privacy.

2 But I think that's -- there's not a  
3 definition of privacy, or of arbitrary, or  
4 unlawful that is binding as a matter of  
5 international law.

6 MS. BRAND: Chris or Laura, any  
7 thoughts on that question?

8 MS. PITTER: Would you repeat that  
9 question again?

10 MS. BRAND: Just what does privacy mean  
11 in the ICCPR context? Where does the definition  
12 come from? How would you find the definition?

13 MS. PITTER: Well, it guards against  
14 unlawful and arbitrary interference with an  
15 individual's privacy, so there has to be a respect  
16 for correspondence, for example, and a respect for  
17 an individual's personal space, and there has to  
18 be an ability to have personal space to  
19 communicate.

20 MS. BRAND: Where are you getting that  
21 definition?

22 MS. PITTER: Well, that's, I mean

1 that's coming from the interpretation of, the  
2 right to privacy is connected to freedom of  
3 expression, freedom of association. It impacts  
4 that. And you know, the right to correspondence  
5 comes from that as well. So I mean it's defined  
6 in the treaty itself, and --

7 MS. BRAND: What is the definition?  
8 Humor me.

9 MS. PITTER: I mean --

10 MS. BRAND: I can look it up,  
11 never mind. But it sounds like what you're giving  
12 me is sort of your sense of what privacy entails,  
13 not a sort of legally defined or legally  
14 articulated definition. Chris?

15 MR. WOLF: So a privacy lawyer's answer  
16 goes back to Brandeis and Warren who said the  
17 right to privacy is the right to be left alone.  
18 But they recognized and I think it's been  
19 recognized ever since, that was 1890, that there  
20 are exceptions for the good of society, for law  
21 and order, for social good.

22 And that's really where the rubber hits

1 the road. What are the permissible exceptions for  
2 national security surveillance? And you know,  
3 that's the discussion that needs to be had  
4 globally.

5           You know, Judge Wald asked what should  
6 the U.S. government do? I think it should promote  
7 that discussion as a global matter, and at the  
8 same time I think it should promote the decoupling  
9 of national security surveillance from cross-  
10 border data flows for commercial purposes.

11           The threat to withdraw safe harbor, for  
12 example, the declaration that the transatlantic  
13 trade and investment partnership shouldn't address  
14 data because of what happened with national  
15 security surveillance is a non sequitur.

16           Those issues need to be dealt with  
17 between governments, but that shouldn't interfere  
18 with cross-border data flows, which have to have  
19 privacy protections built-in, no question. But  
20 those are not something, that isn't something, the  
21 surveillance issue is not something that the  
22 companies themselves can really address and

1 they've done about as much as they can in pushing  
2 for transparency, pushing very hard.

3 MR. MEDINE: Dean, did you want to add  
4 something?

5 MR. GARFIELD: The question was asked  
6 earlier about what the appropriate venue is and I  
7 would say a reminder that the strategic and  
8 economic dialogue didn't exist beyond five years  
9 ago, and so this is one issue that's getting left  
10 behind in the discussion, the importance of  
11 creating a framework and a venue for greater  
12 multinational dialogue around the surveillance  
13 issue. And I think the PCLOB in its  
14 recommendations can have a dramatic effect in this  
15 area.

16 MR. SIEBER: It's clear that we have  
17 not an international definition because the  
18 countries are too different. However, in the  
19 countries and national law, and European law and  
20 in other legal bodies these definitions are  
21 emerging. And of course they have to develop.

22 What is sure is that there is a core

1 area of privacy where we all would agree that  
2 privacy is infringed. For example, if you  
3 directly do intelligence gathering on the sexual  
4 life of somebody who is not a suspect, there's no  
5 reason, that's a clear core area infringement of  
6 privacy.

7 Now if you go further, it's becoming of  
8 course a difficult, mass surveillance of people  
9 against which there is no suspicion would be one  
10 aspect where we'd have to investigate.

11 Another one is to create a complete  
12 picture of the private life of somebody going back  
13 to his birth, whatever did he do, did he  
14 demonstrate in school? So collecting enormous  
15 mass of data on one person would be another  
16 aspect, just illustrating. There are cases which  
17 fall under something like that.

18 And we should work on this definition  
19 and the fact that we do not have something like  
20 that would not lead me to the conclusion we  
21 shouldn't go in these things.

22 It's the same with this attitude on

1 extraterritorial application and things like that.  
2 These questions are so new that you cannot find  
3 any government's position here. So for me, that's  
4 not a valid argument. If you are pioneers on  
5 these questions, we cannot say the governments are  
6 not yet there.

7 I agree with you it's a political  
8 question on this issue.

9 One final point where I do not agree  
10 what was said is the question with respect to  
11 territoriality. If you are collecting data in a  
12 foreign country from (inaudible) it's clear that's  
13 legal. You are not infringing the foreign  
14 territory.

15 But if you go to a foreign territory  
16 and you switch on servers, you download countries  
17 -- the electronic pulses, you are changing and you  
18 do a function that usually the police does, this  
19 is a clear infringement of territoriality.

20 And you can see this especially in the  
21 cyber crime convention where we are fighting about  
22 these questions. We have Article 32 B with a big

1 struggle between the U.S. and Russia, which is  
2 bringing down the complete process of the cyber  
3 crime convention. We all agree that except these  
4 cases mentioned in Article 32 of the cyber crime  
5 convention ratified by the U.S., any police  
6 activities doing access to foreign countries are  
7 of course infringements of privacy. Nobody would  
8 claim that this is legal. We could stop the  
9 process of the cyber crime convention if your  
10 statement would be, all right, like that in this  
11 generality.

12           So I would say that we have to  
13 remain -- these surveillance activities do not in  
14 any case infringe territoriality but there are  
15 many cases, especially looking at the cyber crime  
16 convention, our agreements which we have on this  
17 committee, we all would say that's a clear  
18 infringement of the sovereign territoriality of a  
19 country. And it is also undisputed that the  
20 protection of territoriality is guaranteed, not  
21 only by Article 2 of the U.N. Charter, but also by  
22 customary law. It's one of the basic principles

1 since the Westphalia Peace Accord.

2 MR. MEDINE: Let's give John a chance  
3 to respond.

4 MR. BELLINGER: I'll be brief. On the  
5 second point, again I would say that I don't think  
6 any country in the world would say that the  
7 Article 2 of the U.N. Charter's protection of the  
8 territorial integrity and sovereignty of states  
9 would mean that they cannot conduct essentially  
10 espionage activities from anywhere. I just don't  
11 think that's what the U.N. Charter says.

12 But more importantly, the first thing  
13 you said really goes to the heart of our  
14 discussion here, where you said this is an  
15 evolving national dialogue about privacy and it is  
16 a dialogue that is going on nationally in  
17 different countries, and it therefore is going on  
18 internationally.

19 But the question at least that was put  
20 to several of us, to me and Laura in particular  
21 is, is there a binding international law standard  
22 right now? And the answer to that is clearly no.

1           Germany may have laws inside Germany,  
2           given its particular past. Other countries may  
3           have particular national laws. Sooner or later  
4           countries may get together and agree on things,  
5           but right now there is not an international legal  
6           standard, either in the ICCPR or anywhere else  
7           that limits electronic surveillance from the  
8           United States, or again, from any other country.

9           Other countries would not agree that  
10          there's not an international legal standard -- or  
11          that there is an international legal standard.

12                 MR. MEDINE: We have time for just a  
13                 quick round that Jim had requested. Let me just  
14                 ask just to clarify one point, John, the treaty  
15                 ICCPR is not self-executing. What does that mean  
16                 and is there any forum in which enforcement action  
17                 could take place?

18                 MR. BELLINGER: That means that it  
19                 would require implementing legislation for it to  
20                 be, so it's binding as a matter of international  
21                 law and we have implemented it already and are in  
22                 compliance with it in certain ways because of laws

1 that we already had on our books, or might thereby  
2 have our Congress pass. But it does not have  
3 automatic legal effect merely by the United States  
4 becoming party to it.

5 MR. MEDINE: And is there any forum in  
6 the world where we could be held accountable for  
7 compliance with the ICCPR?

8 MR. BELLINGER: The U.N. Human Rights  
9 Committee monitors our compliance and comments  
10 upon things that we are doing. That's what  
11 happened last week when we presented our report.  
12 And the United States commented on or responded to  
13 these comments, but that's not judicially or  
14 legally enforceable.

15 MR. MEDINE: Thanks. Judge Wald.

16 MS. WALD: Just a quick comment. Am I  
17 not right, John, that not in this context of  
18 surveillance, but hasn't England at times relied  
19 in some of its judicial decisions on the ICCPR for  
20 the, to disallow, I think in dealing with some  
21 detainees or asylum people, etcetera?

22 So my impression was there are courts

1 who have actually relied upon the ICCPR, not in  
2 the surveillance context but in other contexts.

3 MR. BELLINGER: You and I would have to  
4 look at those together. It may have been the  
5 European Convention on Human Rights. There has  
6 been a fair amount of jurisprudence recently on  
7 the extent to which the European Convention on  
8 Human Rights creates obligations on British and  
9 European forces who actually do have someone  
10 within their control of their military outside of  
11 Britain, or Germany, or elsewhere.

12 MS. WALD: Okay. I'll let you off.  
13 Very quickly I have one question, quickly, for  
14 Mr. Garfield, and that is that the statement that  
15 your organization provided to us spoke of the need  
16 for meaningful oversight by an independent body in  
17 government as to the surveillance programs,  
18 including access to collected data.

19 Just wondered very quickly, who you had  
20 in mind, was it the IGs, us, FISA, Congress? Did  
21 you have particular independent bodies who would  
22 provide the meaningful insight, which included in

1 your statement oversight of collected, access to  
2 the collected data?

3 MR. GARFIELD: We did not.

4 MS. WALD: Okay, that's a succinct  
5 answer.

6 MR. MEDINE: Gives you a concise  
7 answer.

8 MR. DEMPSEY: Rather than a question  
9 I'll just offer an invitation, which is if any of  
10 the witnesses could provide us with guidance on  
11 the question I posed, what would be a better way  
12 of structuring a foreign intelligence system.

13 I think at the end of the day any  
14 concept of law, any set of rules is going to  
15 recognize that different countries are going to  
16 have somewhat different structures. So the German  
17 structure is robust but different from the United  
18 States. The United States believes it has a  
19 robust system with different elements than Germany  
20 has, etcetera.

21 Has anybody put together or could  
22 anybody put together a list of the elements of a

1 system and then some sense of how you come up with  
2 what is the minimum?

3 We talked a lot about judicial  
4 oversight but Germany does not have. The court  
5 reviews the statutory structure but not the  
6 individual implementation, does not do individual  
7 targeting on the strategic surveillance in  
8 Germany. In the U.K. it's all administrative, not  
9 judicial.

10 Secondly, if any further thoughts on  
11 how we get from here to there. So several  
12 witnesses have said it's an evolving situation.  
13 We have new questions, questions which to my view  
14 are not answered in the existing documents. Let's  
15 just say that it's not answered. They don't  
16 apply. No one thought about this. It hasn't been  
17 answered. How do we move forward, we, the world,  
18 or maybe the U.S. and Europe, which have more  
19 shared values than we sometimes admit, how do we  
20 move forward in getting that kind of commitment?

21 And the industry in Garfield's paper is  
22 that a global, I think implicitly recognizes we

1 need global understanding, even if not all of the  
2 laws are the same.

3 So any thoughts that you can offer us.  
4 Not right now because we want to move along, but  
5 any further follow-up thoughts you could offer us  
6 in writing, please, it would be very helpful on  
7 both of those points.

8 MS. COLLINS COOK: I just wanted to  
9 thank you all for coming. As I said at the  
10 beginning I think it's important to have these  
11 discussions. I won't assign homework or request  
12 any follow-up, but it's an education process for  
13 us, as well as for the American people,  
14 particularly on these issues.

15 So if there is information you think  
16 should be a part of the public record, which will  
17 remain open, I'm sure David will explain, it is  
18 welcomed.

19 MS. BRAND: I won't take up anymore of  
20 your time since we are at the end of our schedule  
21 here. But I want to thank all of you for coming.  
22 It was very helpful to me, so thank you for taking

1 the time to prepare and to be here.

2 MR. MEDINE: Thanks again to all the  
3 speakers and the Board staff that made this  
4 hearing possible. The Board's activities for  
5 today are now complete.

6 The Board encourages all those who are  
7 interested to submit, panelists and members of the  
8 public, to submit written comments on this topic  
9 at our website of [www.regulations.gov](http://www.regulations.gov). And the  
10 deadline for submitting comments is March 28th.  
11 All comments submitted will be available for  
12 review by the public. A transcript of today's  
13 hearing will be posted on [PCLOB.gov](http://PCLOB.gov).

14 And I will now move to adjourn the  
15 hearing. All in favor of adjourning the hearing  
16 please say aye.

17 (Aye)

18 MR. MEDINE: Upon receiving unanimous  
19 consent to adjourn, we will now adjourn. The time  
20 is 3:40. Thank you.

21 (Whereupon, at 3:40 p.m., the hearing  
22 was adjourned.)

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 the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

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 10, 2014

<b>A</b>	<b>academic</b> 262:5 290:14 291:2	<b>accountable</b> 292:2 307:6	<b>acquires</b> 38:5 152:4 197:19	<b>acts</b> 231:9,18 235:14 285:4
<b>a.m</b> 1:17 4:6	<b>academics</b> 6:17 6:22	<b>accounts</b> 52:12 55:5 221:19 228:2	<b>acquiring</b> 151:21	<b>actual</b> 48:17 118:6 147:17 172:9 201:10 215:22 248:4 285:4
<b>abide</b> 224:16 242:11 267:19	<b>accept</b> 150:14 174:12 224:14 235:3 245:22 297:9	<b>accuracy</b> 73:1 74:15	<b>acquisition</b> 9:20 17:7 38:8,12 38:15,16 104:17 133:5 133:10 139:17 158:14 165:2 188:8,14,18 189:3 190:15 191:21 192:7 192:11 193:1 196:19 223:6	<b>actuality</b> 126:18
<b>ability</b> 74:13 192:13 221:17 230:2 246:12 285:3 290:1 298:18	<b>accepted</b> 87:5 216:18 290:3,7 290:9 295:16 295:19 296:18 297:7	<b>accurate</b> 67:19	<b>act</b> 1:8 2:11 3:3 5:11,12,16 7:18 29:10 84:17 175:9 235:8	<b>add</b> 13:18 21:16 30:8 31:14 34:13 42:9 43:6 49:12 65:19 77:18 96:4 99:20 103:17 139:13 179:16 181:7 185:18 190:22 195:14 201:17 206:17 208:11 250:14 301:3
<b>able</b> 102:8 111:21 222:6 261:11 273:7 273:13	<b>accepting</b> 166:7 235:20	<b>achieve</b> 228:6	<b>acting</b> 214:7 215:4 234:14	<b>added</b> 68:19 212:20 213:10
<b>abouts</b> 55:6 56:9 57:7 63:2 94:10 98:4,12 160:21 163:15 163:17 164:6 168:9,18 193:19	<b>access</b> 76:22 77:10,12,14 83:17 86:5 105:19 119:7 152:9 174:21 176:13 188:1 189:21 190:1,2 190:20 191:22 192:6,10 238:9 238:20 239:3 241:20 275:20 277:12 304:6 308:18 309:1	<b>achievements</b> 13:10	<b>action</b> 306:16 313:11	<b>adding</b> 30:20 162:11
<b>abroad</b> 37:12 40:10,20 41:1 41:7,21 49:21 58:15 96:10 148:9 182:21 182:22 236:10 249:2 258:4,16 258:21 259:7 259:19 269:1 276:21 295:12	<b>accesses</b> 231:7	<b>acknowledge</b> 227:11 234:3	<b>actions</b> 235:19	<b>addition</b> 22:3 23:3 85:9,14 136:9 213:1,5 213:6 231:19 232:7 270:4 271:9
<b>absence</b> 123:19 156:19 262:15	<b>accessing</b> 190:7 190:11	<b>acknowledged</b> 196:21	<b>activist</b> 207:4	<b>activities</b> 11:8 11:18 84:13 127:2 131:19 179:4 210:15 217:16 239:17 240:3 241:14 278:16 280:8 282:13 285:8 304:6,13 305:10 312:4
<b>absent</b> 122:9	<b>accidental</b> 96:16 96:19 97:1	<b>acknowledges</b> 201:19	<b>activity</b> 19:5 38:10 86:10 105:3,19 115:15,21 118:7 142:3 149:11 156:2 198:14	<b>additional</b> 33:5 35:2 63:2 94:5 136:2 185:18 207:11 228:11 239:10 273:4 278:13
<b>absolute</b> 66:21 257:11 297:4	<b>accord</b> 305:1	<b>acknowledging</b> 251:22	<b>actors</b> 67:22	<b>address</b> 13:18 15:2 17:2,6,7 18:8 19:16 30:6 51:8 54:18,20 67:12 79:5 83:13 92:18 112:4 116:1 120:6,7
<b>absolutely</b> 37:9 67:2 76:18 205:1 248:15 248:16 258:17	<b>account</b> 41:10 42:6 43:1 51:5 51:12,17,20 52:2 53:5,6 54:15 55:20,22 56:4,7 60:16 73:21 95:17 101:2 217:16 218:1 272:11 272:16	<b>ACLU</b> 113:13 155:14 156:12 205:1		
<b>abstracting</b> 106:17	<b>accessing</b> 190:7 190:11	<b>ACLU's</b> 120:22		
<b>absurd</b> 226:5	<b>acquired</b> 28:2 32:12 37:4,5 38:21 52:13 79:21 106:5 123:17 134:9 164:22 165:16 165:22 166:4 193:2 196:11 196:13 197:14 197:17,22 199:15,19 201:18,20 229:13 281:18	<b>acquire</b> 7:22 38:2 39:3 68:6 122:2,5,18 123:20 133:10 134:15 147:3 152:1,2,3 162:3 189:21 196:2		

136:19 179:2 197:11 221:1,2 300:13,22 <b>addressed</b> 116:3 146:14 231:1 269:5 <b>addresses</b> 9:5 10:8 25:12 52:7,10 71:6 88:16 120:2 <b>addressing</b> 239:1,21 <b>adherence</b> 85:14 282:7 <b>adjourn</b> 312:14 312:19,19 <b>adjourned</b> 312:22 <b>adjourning</b> 312:15 <b>adjudicated</b> 226:14 <b>adjustable</b> 47:11 <b>administerial</b> 310:8 <b>administration</b> 159:12,12 211:21 214:16 223:22 230:7 253:22 291:7 <b>administratio...</b> 214:3 <b>administrations</b> 214:2 229:17 <b>administrative</b> 157:4,5 <b>admit</b> 310:19 <b>admittedly</b> 137:12 <b>adopted</b> 213:6 276:11 <b>advance</b> 59:19 218:9	<b>adversarial</b> 204:12 206:2 <b>adversaries</b> 286:8 <b>adversary</b> 204:15 <b>advice</b> 88:7,18 269:2 <b>advisor</b> 210:9 210:10,12 212:3 214:7 234:7 <b>advocate</b> 159:13 205:7 222:7,8 237:2,5 277:20 277:22 <b>advocates</b> 6:17 6:22 210:17 <b>affairs</b> 117:17 127:1,10 279:9 285:12,17,22 286:5 287:13 287:17 288:4 288:19 <b>affect</b> 285:17 <b>affirm</b> 223:5 <b>affirmative</b> 42:11 74:10 114:16 <b>affords</b> 243:4 <b>Afghanistan</b> 236:15 <b>afraid</b> 36:19 <b>afternoon</b> 209:6 <b>age</b> 198:16 236:7 <b>agencies</b> 6:13 19:9 22:9 36:3 36:6 49:6 67:7 78:21 79:3 80:18 105:1 106:12 107:4,5 108:21 118:4 136:6 240:18	242:11 256:14 256:19 257:1 257:15 267:15 268:8 <b>agency</b> 2:16 18:3,16 107:14 107:15,16,18 109:6 110:2 122:8,13 240:14 257:21 <b>agent</b> 29:7 116:7 141:13,21 149:4,10 150:21 173:22 204:1 207:17 208:7 <b>agents</b> 67:21 126:3 149:5 234:14 <b>aggressive</b> 131:13 <b>aggrieved</b> 165:18,19,21 166:3 <b>ago</b> 86:14 145:17 214:5 301:9 <b>agree</b> 42:21 64:11 68:17 69:8 90:11 131:21 138:8 138:16 153:22 164:8 169:21 197:12 202:17 206:17 213:17 221:9 245:20 245:21 258:17 263:22 277:3 289:6,10 290:22 291:9 302:1 303:7,9 304:3 306:4,9 <b>agreed</b> 5:8 127:13 216:18	232:8 265:13 267:19 296:21 297:1,14,15 <b>agreeing</b> 5:2 <b>agreement</b> 272:18,20 273:2 <b>agreements</b> 111:19 304:16 <b>ahead</b> 125:11 149:20,20 250:16 <b>aim</b> 228:1,5,6 <b>aimed</b> 60:13 220:3 291:14 <b>aiming</b> 225:3 <b>AI</b> 120:6 <b>albeit</b> 243:20 <b>alien</b> 8:3 <b>aliens</b> 233:3 <b>allegedly</b> 238:16 <b>allied</b> 252:4 <b>allies</b> 282:5 <b>allocated</b> 64:20 <b>allow</b> 40:13,14 40:15,16 122:8 124:3 151:10 205:8,10 225:8 240:21 <b>allowed</b> 30:14 30:19 167:8 200:22 205:2 208:19 240:15 241:3 <b>allowing</b> 13:4 26:16 124:16 180:6 <b>allows</b> 187:18 187:22 285:22 287:7 288:7 <b>allude</b> 98:19 <b>alluding</b> 105:17 252:13 <b>alongside</b> 183:1	<b>alphabetically</b> 209:22 <b>alternatives</b> 228:18 <b>ambiguities</b> 37:8 <b>ambiguity</b> 161:9 <b>ambit</b> 59:9 271:3 <b>ameliorate</b> 272:5 <b>Amendment</b> 10:16 13:1 14:9,12 15:2,7 15:9,13,14,18 16:2,9 17:4 18:1 20:7,10 20:11,12 21:5 21:7,9,11,13 22:5,11,13,19 27:13,19 28:8 28:15 39:4,6 39:15 43:4 74:22 75:19,21 80:13 94:22 116:10 118:1 119:16,22 120:10,16 121:2 129:2,7 129:15 131:5,6 131:20 137:4 137:19,21 138:9,17,18 142:17 144:16 144:19 146:18 148:4 152:20 153:1,4,6,9,11 153:16,17 154:10,13,15 154:19 155:9 156:4,14,21 157:14,18,21 158:1,4,15 160:5 172:21
---	--	---	---	---

175:22 180:19 182:9,11 183:2 183:3,4,6,8,19 184:12 185:1,8 185:21 186:5 186:12 190:4 191:18 192:1,4 192:8,17 193:7 200:4 205:3,5 <b>Amendment's</b> 126:5 129:17 130:10 <b>Amendments</b> 5:12,16 119:18 <b>American</b> 3:6 181:13,15 235:6 256:3 311:13 <b>Americans</b> 121:4,6 123:18 124:2 131:22 151:21 152:9 159:2,8 170:17 180:21 293:5,6 <b>amount</b> 36:5,10 68:5 113:2 208:19 260:20 286:1 308:6 <b>analogize</b> 195:3 <b>analogizing</b> 14:16 <b>analyses</b> 219:13 <b>analysis</b> 15:9 20:10,11 21:11 22:5,11,14,19 23:4,8 46:15 75:20,22 77:8 101:17 114:22 120:14 143:17 145:6,7,9 146:19 153:1 154:1 174:15 176:22 185:2 190:5 193:7	194:7 201:14 216:3 235:11 281:2 <b>analyst</b> 41:10,11 45:8 59:14 79:14,15 294:2 <b>analysts</b> 41:19 42:11 46:9,10 47:1 62:5 74:11 87:14 88:17 111:21 294:12 <b>analyze</b> 80:19 142:2 154:8 184:5 194:10 226:19 <b>analyzed</b> 275:7 <b>angrily</b> 140:19 <b>annex</b> 84:18 <b>anniversary</b> 219:20 <b>announced</b> 4:9 <b>annual</b> 8:22 22:7,12,17,20 62:13,15 293:21 <b>annually</b> 22:4 22:21 43:2 59:11 112:10 <b>answer</b> 37:20 42:3 70:2 135:12 154:4,5 155:4 164:15 169:17 201:8 206:17 228:7 264:12 299:15 305:22 309:5,7 <b>answered</b> 36:9 135:16 161:14 310:14,15,17 <b>answering</b> 82:22 169:14 <b>answers</b> 16:15 92:13 135:17	136:16 161:13 <b>ante</b> 42:16 59:19 82:11 <b>anybody</b> 40:14 83:6 171:2 196:10 201:7 234:13 244:18 309:21,22 <b>anymore</b> 195:13 311:19 <b>anyway</b> 62:10 105:20 200:16 <b>AOL</b> 191:8 <b>apartment</b> 138:1 <b>apologize</b> 98:5,9 125:11 147:9 152:17 <b>apparent</b> 32:2 <b>apparently</b> 80:2 <b>appear</b> 8:11 120:21 125:8 134:9 <b>appears</b> 135:5 <b>applaud</b> 132:7 <b>Apple</b> 191:8 <b>applicability</b> 137:4 234:4,10 234:16 235:21 243:8 258:4 260:11 261:10 261:17 <b>applicable</b> 16:17 234:12 259:13 <b>application</b> 206:5,5,6 268:18,22 280:11,21 291:9 293:14 295:10 303:1 <b>applications</b> 21:20 <b>applied</b> 82:15	183:21 259:22 269:10 286:21 296:16 297:15 <b>applies</b> 111:3 129:18 151:13 184:4 185:10 186:12,14 214:10 224:5 225:17 227:16 289:18 <b>apply</b> 18:21 26:21 50:21 81:13 87:3 109:17 121:10 129:7 154:11 165:18 176:13 183:19,22 184:2,7 211:17 212:13 213:2 214:4,17 217:2 224:3 225:15 225:21 233:14 244:7,13 245:11 247:6 258:21 259:14 260:2 265:5 278:15 296:4 297:10 310:16 <b>applying</b> 236:18 237:14 258:5 259:11 279:21 <b>appointed</b> 204:15 257:18 <b>appreciate</b> 20:3 27:8 36:10 46:16 113:3 191:15 <b>approach</b> 19:18 22:1 65:12 153:1,3 158:5 230:22 279:21 <b>appropriate</b> 48:3 86:7 97:3 97:18 217:22	243:4 301:6 <b>appropriately</b> 81:10 171:14 <b>approval</b> 7:20 14:21,21 20:11 28:17 29:6 156:16 171:12 240:5,12 <b>approvals</b> 29:16 <b>approve</b> 9:9 49:3 241:4 295:2 <b>approved</b> 43:3 48:1 53:11 98:13 112:9,13 150:22 151:5 <b>approves</b> 8:22 12:22 59:10 <b>approving</b> 173:6 <b>approximate</b> 253:17 <b>arbitrary</b> 211:4 216:9,12,15,21 243:4 296:16 297:1,22 298:3 298:14 <b>arcane</b> 52:5 <b>area</b> 71:9 77:22 114:21 116:12 117:6 118:16 119:15 120:9 256:18 259:2 301:15 302:1,5 <b>areas</b> 69:14 114:1,4 120:13 172:2 218:17 <b>arguably</b> 150:4 <b>argue</b> 148:3 195:9 216:11 296:10,19 <b>argued</b> 206:12 210:18 225:16 227:8 246:17
--	--	--	--	---

<b>argues</b> 235:6	266:22 295:12	<b>association</b>	<b>augment</b> 122:1	47:3 93:12
<b>arguing</b> 202:10	<b>asked</b> 81:12	299:3	<b>August</b> 277:8	112:3 198:17
224:1	223:15 300:5	<b>associations</b>	<b>Australia</b> 239:7	242:1 312:11
<b>argument</b>	301:5	125:4 153:15	240:10,20	<b>Avenue</b> 1:16 4:8
102:16 145:16	<b>asking</b> 58:4	174:19	<b>authoritative</b>	<b>average</b> 253:7
161:1,18 163:9	111:16 146:6	<b>assume</b> 76:10	250:18 268:10	<b>avoid</b> 151:21
164:5 176:1	154:4 168:16	77:1 105:19	<b>authorities</b>	<b>Awang</b> 5:6
210:21 211:7	169:4 174:20	199:7,7 282:21	158:3 233:7	<b>aware</b> 11:1
235:4 238:16	230:16 240:19	<b>assuming</b>	276:9,15	96:13 215:12
244:21 297:21	<b>asks</b> 109:14	195:19 253:14	283:10,12	215:21 246:4
303:4	<b>aspect</b> 62:18	<b>assumption</b>	<b>authority</b> 11:1	250:3 264:13
<b>arguments</b>	116:3 138:17	114:13 177:22	121:21 122:2,5	265:2 289:19
124:20 193:20	143:16,16	195:9	122:18 123:20	<b>awareness</b> 69:18
193:21 235:20	149:13 221:5	<b>assurances</b>	127:14 130:16	221:12,14
<b>arises</b> 37:16	258:3 302:10	280:18	159:16 169:11	<b>aye</b> 4:18,19
157:14	302:16	<b>asylum</b> 307:21	171:5 172:3	312:16,17
<b>arising</b> 282:20	<b>aspects</b> 119:6	<b>atrocities</b> 225:6	176:8 182:21	
<b>armed</b> 262:21	164:18 237:22	<b>attach</b> 192:1,8	183:13 194:4	<b>B</b>
<b>Arnold</b> 3:15	249:16 255:22	<b>attached</b> 192:4	194:18 195:16	<b>B</b> 303:22
209:11	<b>aspirational</b>	256:7	195:19 202:14	<b>back</b> 25:2 29:18
<b>arose</b> 118:10	266:22	<b>attack</b> 285:4	228:10 258:10	30:1,4 44:8
<b>arrangements</b>	<b>Assembly</b> 236:6	286:9	281:15 292:3	50:14 60:17
242:1 283:11	<b>asserts</b> 175:19	<b>attempt</b> 126:15	293:13	71:11 74:18
<b>arrest</b> 256:15	<b>assess</b> 63:13,18	236:3	<b>authorization</b>	80:22 92:22
<b>Article</b> 142:14	64:6,8 81:2,13	<b>attempted</b> 64:19	84:17 127:18	93:5 100:16
144:6 194:1,4	83:1 194:2	<b>attempting</b>	194:3 198:2	112:6 123:15
210:21 211:3,8	<b>assessing</b> 63:19	262:11	242:13	147:9 153:22
212:6 216:8	<b>assessment</b> 46:7	<b>attention</b> 72:10	<b>authorize</b>	171:16 173:3
217:1 231:3,21	83:11 126:11	117:12	123:14 161:22	175:16 176:16
233:20 246:12	164:12 187:8	<b>attitude</b> 258:5	183:17 206:10	178:15 180:9
249:4 261:17	242:8	302:22	238:9	182:3 204:1
267:7 289:22	<b>assessments</b>	<b>attorney</b> 2:19	<b>authorized</b>	207:2,17,19,21
303:22 304:4	62:14	7:21 9:1 35:17	102:3,11	208:9 233:11
304:21 305:7	<b>assets</b> 240:16	85:20 86:12,15	140:16 177:10	260:7 266:2
<b>articulable</b>	<b>assign</b> 311:11	86:18 87:1,5	<b>authorizes</b>	293:8 299:16
48:19	<b>assist</b> 70:21	88:9,20 106:14	121:11 164:11	302:12
<b>articulate</b> 63:13	<b>assistance</b> 25:15	118:14 140:15	<b>authorizing</b>	<b>back-end</b> 152:8
95:12 112:7	26:2 69:21	141:1 151:1	194:15	173:12 174:7
<b>articulated</b> 27:3	238:21	155:14 161:21	<b>automatic</b> 307:3	174:12 175:17
30:13,16 40:11	<b>Assistant</b> 2:19	<b>attorneys</b>	<b>availability</b>	<b>backbone</b> 26:7
109:2,7 299:14	35:17	118:19	238:21	248:14
<b>articulating</b>	<b>associated</b> 68:4	<b>audience</b> 35:11	<b>available</b> 9:21	<b>background</b>
22:3 82:6	120:2,8 123:17	35:12	20:5 26:17	125:21 126:13
<b>aside</b> 73:19	142:16	<b>audits</b> 62:6	32:2 41:11	194:8

<b>bad</b> 55:3,8 60:16 73:10 156:2 167:1 207:2,2	73:18 104:22 132:22 149:9 153:6 160:7 170:14 173:15 177:14 219:7	<b>belief</b> 40:19 <b>believe</b> 10:9 14:10 17:17 23:8 51:9 60:15 73:10	<b>benefits</b> 219:22 <b>best</b> 45:1 93:11 145:15 164:5 196:12 275:16 280:9	28:19 30:7 39:18 44:12 45:6 61:2 80:3 82:8 89:2 93:6 98:20 104:15
<b>badge</b> 219:8 <b>Baker</b> 2:13 22:22 32:6 35:12 61:18 67:10 70:2 73:2 82:18 85:7 92:16 105:15 111:1	222:12 228:21 230:16 238:14 256:17 258:20 258:22 282:9 <b>baseline</b> 101:13 241:17 <b>basic</b> 30:11 101:10 109:1 233:13 256:11 258:9,9 304:22	80:16 111:10 125:1 129:1 131:4,10,19 133:1,20 141:2 147:1 150:20 154:10 173:8 175:6,8 214:9 221:1 246:5 249:8 250:10 250:12 294:11	<b>Beth</b> 34:13 82:22 <b>better</b> 25:1 26:7 34:22 255:4,8 255:11,11 260:5 275:9,16 284:2 309:11 <b>beyond</b> 59:8 88:13 97:6 131:19 140:11 301:8 <b>big</b> 48:5 88:5 109:3 252:1 303:22 <b>bigger</b> 40:6 42:10 46:14 258:16 259:19 259:19	105:7 116:15 147:16 149:2 158:2,8 167:21 171:7,13 185:2 191:1 195:3 204:18 223:13 257:2 266:17 291:16 293:8
<b>balance</b> 84:8 93:1 105:14 <b>balanced</b> 256:19 <b>balances</b> 255:12 259:20 <b>balancing</b> 155:18 156:3 255:16 <b>Balkanization</b> 283:13 <b>balkanize</b> 282:12 <b>ballroom</b> 4:7 <b>Baltimore</b> 313:5 <b>ban</b> 130:21 <b>bank</b> 153:13 186:15 <b>bans</b> 216:8 <b>bar</b> 178:21 179:10 180:7 <b>barred</b> 226:6,8 <b>barriers</b> 34:20 119:3,4 <b>bars</b> 89:21 <b>base</b> 78:11 106:6 109:16 210:21 <b>based</b> 5:21 7:20 10:7 18:13,17 26:10,14 41:7 56:10 57:12 60:7 71:5	<b>basically</b> 43:10 50:11 86:21 87:6 133:11 140:11 156:3 175:17 253:16 265:10 282:4 290:13 <b>basis</b> 37:5 61:13 74:12 76:10 78:17 84:1 100:12 107:16 219:9 277:12 277:13 <b>Bates's</b> 163:4 <b>battle</b> 233:11 <b>bear</b> 58:4 <b>bears</b> 74:8 <b>becoming</b> 139:10 219:9 264:19 302:7 307:4 <b>beg</b> 116:19 <b>began</b> 238:10 <b>beginning</b> 147:10 294:14 311:10 <b>begun</b> 63:15 <b>behalf</b> 8:11 218:6	<b>believed</b> 9:11 37:11 39:20 40:10,20 58:15 71:17 89:9,13 122:14 131:1 136:6 148:11 162:2 <b>believes</b> 215:13 250:3 264:14 265:2 289:20 291:10 309:18 <b>Bellinger</b> 3:15 209:10 210:1,2 223:20 224:6 244:10 247:8 248:21 249:19 250:1 251:2 252:20 253:2 253:21 264:7 264:11 267:18 288:12,21 296:2 305:4 306:18 307:8 308:3 <b>belong</b> 53:12 155:13 <b>belongs</b> 52:21 73:10 103:10 <b>benefit</b> 35:10,12	<b>blanket</b> 219:22 219:12 275:16 280:9 <b>Beth</b> 34:13 82:22 <b>better</b> 25:1 26:7 34:22 255:4,8 255:11,11 260:5 275:9,16 284:2 309:11 <b>beyond</b> 59:8 88:13 97:6 131:19 140:11 301:8 <b>big</b> 48:5 88:5 109:3 252:1 303:22 <b>bigger</b> 40:6 42:10 46:14 258:16 259:19 259:19 <b>biggest</b> 205:19 <b>billions</b> 219:15 <b>bind</b> 286:18 <b>binding</b> 213:19 213:22 215:20 217:6 218:2 250:5,12 251:13,15 266:19 267:3 267:15 268:7 268:12,14,17 289:13 290:14 295:21 298:4 305:21 306:20 <b>binds</b> 258:9 289:20 <b>biometric</b> 154:16 <b>birth</b> 302:13 <b>bit</b> 20:17 23:19 23:21 24:20	725:16 725:16 280:9 105:7 116:15 147:16 149:2 158:2,8 167:21 171:7,13 185:2 191:1 195:3 204:18 223:13 257:2 266:17 291:16 293:8 <b>blank</b> 67:1 <b>blanket</b> 60:12 <b>blessing</b> 131:15 <b>blind</b> 33:21 <b>blocked</b> 108:17 <b>blow</b> 168:4 <b>BND</b> 257:22 <b>board</b> 1:3 2:1 4:12,13 5:2 6:8 7:3,5 18:21 36:9 76:22 77:2,10 83:17 87:9 111:11 120:21 125:8 125:13 128:11 132:19 134:22 135:11 136:19 149:22 173:20 174:9 182:10 207:10 209:21 210:4 223:13 231:14 242:7 243:14 312:3,6 <b>Board's</b> 4:3 5:3 312:4 <b>Bob</b> 8:8 15:5 23:17 25:8 35:14 40:11 48:11 68:19 76:6 105:16 109:7

<b>Bob's</b> 101:19	84:4 85:12	223:14 305:4	<b>Budapest</b> 232:9	155:14 210:22
<b>bodies</b> 278:6	127:21 128:5	<b>briefing</b> 20:21	<b>budget</b> 64:21	252:5 257:19
301:20 308:21	140:2,4 142:13	21:15	<b>build</b> 51:3	<b>calling</b> 103:10
<b>bodily</b> 172:17	142:14 291:21	<b>briefings</b> 100:4	170:12 220:18	103:15 220:12
<b>body</b> 64:5 180:6	292:1,1,4,6	100:5	292:9	<b>calls</b> 46:2 47:22
180:12 221:6	293:11,17	<b>briefly</b> 39:18	<b>building</b> 54:12	124:16 156:11
226:13,15	<b>branch's</b> 128:14	127:3 129:4	<b>built</b> 80:10	190:15,19,20
241:4 267:13	<b>branches</b> 11:5	132:16 133:2	114:13 124:14	191:21
267:22 268:5	132:5	134:21 186:3	<b>built-in</b> 300:19	<b>camp</b> 225:9
308:16	<b>brand</b> 2:4 4:14	<b>briefs</b> 77:21	<b>bulk</b> 10:6,6,12	<b>Canada</b> 239:7
<b>bolster</b> 222:20	20:2 22:13	78:5	23:18,19,22	240:10,21
<b>bomb</b> 140:1	23:2,17 24:19	<b>bring</b> 79:22	24:2,6,17 48:8	<b>candidate</b> 75:6
<b>bomber</b> 34:18	27:6 56:14,19	142:4 229:9	71:6 157:7,9	<b>candidates</b> 75:8
<b>book</b> 284:21	57:1,2,9,16,21	283:16	157:11 158:8	<b>candidly</b> 215:16
<b>books</b> 19:16	60:21 61:14	<b>bringing</b> 304:2	158:10,11,14	<b>capabilities</b>
240:1 269:9	62:21 93:5,19	<b>brings</b> 11:2	158:14 189:12	67:20
307:1	95:3,9 96:3	139:14	190:11,14,18	<b>capable</b> 124:15
<b>bootstrapping</b>	97:4,9 145:11	<b>Britain</b> 308:11	197:6 200:1,3	150:11
179:20 180:9	146:5 148:5	<b>British</b> 308:8	229:12	<b>capacity</b> 279:17
180:17 181:8	149:15,20	<b>broad</b> 14:20	<b>bunch</b> 24:11	279:18
181:20 199:3	179:6 182:6,7	122:4 125:22	<b>burden</b> 48:15	<b>capita</b> 277:11,13
<b>border</b> 198:6,7	184:7 186:2,10	127:22 150:17	114:7,9 176:16	<b>capture</b> 201:1
200:7,10 242:1	187:3 266:1,5	151:7 172:4	177:19	<b>card</b> 153:13
300:10	267:11,22	186:8 194:12	<b>burdensome</b>	<b>care</b> 85:15 168:5
<b>borders</b> 211:17	268:12,19	202:2 253:6	30:4	168:12
224:5,20	269:15 270:17	255:18 279:6	<b>bureau</b> 2:13	<b>careful</b> 203:7
229:20 246:13	271:20 295:5,7	281:20 285:8	30:10	254:9,16
248:13 283:8	298:6,10,20	285:18 288:7,7	<b>Bush</b> 159:12	<b>carefully</b> 11:17
<b>bottom</b> 216:22	299:7,10	<b>broad-based</b>	214:1	203:4 205:8,9
229:18	311:19	68:12 131:15	<b>business</b> 230:5	<b>carrying</b> 284:9
<b>bound</b> 212:8	<b>Brand's</b> 153:22	<b>broader</b> 62:2,19	272:3,22 275:5	<b>carve</b> 33:7
271:14,16,18	<b>Brandeis</b> 299:16	97:12 124:12	284:9	<b>case</b> 23:12 29:12
286:19 289:10	<b>Brazil</b> 220:6,8	130:7 138:20	<b>bypassing</b> 180:5	39:14 48:3
<b>box-checking</b>	239:11	151:8 159:16	<b>Byron</b> 140:10	55:2 60:6
203:1	<b>break</b> 6:20	166:11 219:17		64:17 74:3
<b>Brad</b> 2:19 22:3	113:4 209:2	230:22 249:9	<b>C</b>	77:8 79:16
27:2 32:10	<b>breaks</b> 169:5	278:19 282:7	<b>C</b> 3:16	115:11 116:6,8
35:16 39:2	<b>Brennan</b> 3:10	289:17	<b>call</b> 4:16 90:6	137:22 139:22
72:6,22 80:8	113:16 140:20	<b>broadly</b> 15:1	138:2 159:6	140:10 141:9
146:14	<b>Brian</b> 5:5	68:15 122:16	163:18 174:17	141:14 144:16
<b>Brad's</b> 30:20	<b>brief</b> 7:6 8:13	158:20 208:3	177:9 189:1,2	147:8 149:10
<b>Bradford</b> 5:4	21:8 34:13	<b>brought</b> 141:9	189:12 197:6,7	155:19,21
<b>branch</b> 20:8	113:17 132:11	141:18	<b>called</b> 61:6	157:4 196:12
68:20,21 84:4	208:11 209:19	<b>Brownell</b> 140:3	118:2 124:15	197:21 198:4

198:21 204:19 225:2,18 226:15 227:5 234:1 237:19 249:8 262:22 263:14 269:5 278:18 290:6 294:7 304:14 <b>cases</b> 6:7 17:18 43:11 73:19,19 74:6 77:21 137:20 139:19 142:7 143:1 150:2,9,18,19 150:19 160:4,5 160:6 184:12 184:15 185:7 186:21,22 198:6,8,15 199:13,16 200:7,8,10,12 205:12,13,21 206:1 235:17 249:11 302:16 304:4,15 <b>catch</b> 227:8 <b>categories</b> 9:2 81:8 <b>category</b> 32:9 32:20 105:6 207:6 285:20 288:19 <b>cause</b> 116:5 118:6 124:7 141:11,20 150:20 155:19 156:9 157:19 160:8 172:10 172:16 173:1,8 173:16,17,19 174:3,5 180:8 193:6 227:22 <b>caution</b> 149:22 <b>cede</b> 100:15	290:22 <b>celebrating</b> 219:19 <b>cell</b> 73:10,13 <b>Center</b> 3:10 113:16 <b>central</b> 114:1 <b>centralized</b> 106:14 107:2 <b>CEO</b> 3:16 209:12 <b>certain</b> 66:19 85:11 95:19 102:7 104:2 106:7 134:5 177:17 195:13 216:4 233:8,13 236:19 237:14 238:12 239:15 245:20 257:12 306:22 <b>certainly</b> 44:14 83:9,14 102:7 112:6 118:12 126:19 135:6 135:14 137:6 186:18 190:13 192:2 196:16 197:18 203:16 216:11 217:9 246:2 247:8 250:1,9 251:9 254:22 264:18 284:16 287:4 290:7 <b>certainty</b> 200:1 <b>certification</b> 22:7,8,18 62:15 313:1 <b>certifications</b> 8:22 9:7 59:10 59:11 279:12 294:22 <b>certify</b> 313:6,9	<b>chair</b> 21:5 <b>chair's</b> 26:21 <b>chairman</b> 2:3 4:5,11 238:2,3 269:17 <b>challenged</b> 77:19 <b>challenges</b> 185:4 218:20 287:1,1 <b>chance</b> 35:9 45:9 132:12 142:20 160:15 182:17 266:1 284:5,22 305:2 <b>change</b> 23:6 157:16 158:2,9 205:14 213:7 230:9 245:7,10 251:16 279:3 <b>changed</b> 76:11 144:9,10 229:16 257:2 <b>changes</b> 79:19 139:11 157:12 201:5 230:8 <b>changing</b> 137:18 220:3 303:17 <b>characterized</b> 167:7 <b>charge</b> 92:22 <b>charges</b> 141:18 142:5 <b>charities</b> 153:15 <b>Charter</b> 231:4 264:20 265:1 265:15,16 290:16 304:21 305:11 <b>Charter's</b> 264:14 305:7 <b>chats</b> 191:9 <b>chatting</b> 171:21 <b>cheapest</b> 228:22	<b>check</b> 114:17 178:5,8,9 259:16 <b>checked</b> 259:8 <b>checking</b> 41:17 <b>checks</b> 62:8 255:12,15 <b>Chicago</b> 73:12 <b>chief</b> 127:10 140:14 <b>choose</b> 6:5 <b>Chris</b> 209:18 254:22 298:6 299:14 <b>Christopher</b> 3:22 274:1 <b>CIA</b> 18:4,15 78:22 119:7,9 119:10 140:1 <b>circuit</b> 130:4 <b>circuits</b> 15:22 <b>circular</b> 105:8 105:12 <b>circumscribed</b> 115:2 <b>circumstance</b> 23:9 88:19 178:17 <b>circumstances</b> 41:8 42:5 85:11 94:16 106:8,11 107:13 111:17 112:7 126:22 178:12 186:18 236:13 258:15 <b>cited</b> 255:1 277:10 <b>citing</b> 147:5 <b>citizen</b> 8:3 128:9 130:2 131:8 138:2 278:4 <b>citizen's</b> 125:4 <b>citizens</b> 126:9	129:7,12,13,19 183:22 184:2 215:18 230:3 230:20 232:19 233:5,6 236:22 259:2 277:20 278:4 <b>civil</b> 1:3 3:7 4:3 93:2 211:1 218:10 222:7,8 223:17 233:21 255:16 267:8 286:14 <b>claim</b> 165:21 304:8 <b>claimed</b> 127:21 128:6 <b>claiming</b> 121:20 145:1 <b>claims</b> 127:4 238:11 239:1 275:18 <b>clandestine</b> 285:7 <b>clarified</b> 185:7 <b>clarify</b> 30:14 78:20 183:10 202:10,11 306:14 <b>clarifying</b> 57:5 <b>clarity</b> 40:12 194:22 <b>class</b> 133:15 <b>classic</b> 137:21 144:16 <b>classified</b> 6:2,3 6:7 13:11 84:18 85:3 135:9 <b>clause</b> 100:12 152:11 224:7 224:12 248:9 270:12 <b>clauses</b> 69:3
---	--	---	---	---

<b>clear</b> 11:16 12:8 14:2 36:13 37:9 39:2 49:15 69:16 90:11 129:6 133:22 152:21 155:1 179:11 213:1,11 225:12 275:2 279:3 289:3 301:16 302:5 303:12,19 304:17	<b>colleague</b> 30:9 215:10 <b>colleagues</b> 13:17 29:1 36:3 54:4 68:9 100:14 <b>collect</b> 8:18 16:3 16:10 26:16 29:13,21 38:2 39:3 51:10 53:5 59:2 60:4 80:18 147:22 148:11,16 159:17,17 167:9 180:20 189:21 196:2 242:2 246:13 254:14 256:16 294:18 <b>collected</b> 9:3 13:3,5 15:12 16:20 17:11 19:12,19 27:16 28:5 29:9,15 29:19 30:21,22 31:3 32:15,17 37:14 38:21 43:18 72:19 95:5 100:20 101:2 102:20 106:20 133:20 134:6 136:15 146:4,6 163:6 170:10 176:8 176:18 177:14 179:12,19,21 180:3,7,12 199:18 200:3 243:19,20 245:6 254:3,7 254:15 269:11 308:18 309:1,2 <b>collecting</b> 13:13 51:15,19 58:19 73:14 85:22	89:4 94:13 95:20 142:12 159:21 161:5 162:10,18 167:19 177:17 181:10 198:22 288:18 302:14 303:11 <b>collection</b> 7:14 10:6,6,7,12 11:2,4,8 12:5 12:10,14 13:9 14:1,13,20,22 15:3,5,17 16:7 16:18 17:4,22 21:3,12,18 23:18,20 24:3 24:7,7,9,17,17 25:4,5,7,16,20 25:22 26:4,5,6 26:6,12,14,15 26:18,20 27:2 27:14,22 29:3 29:4,5 30:13 30:15 31:17 32:22 33:22 36:22 37:1,9 37:22 38:8,12 38:15,16 40:17 42:16 47:8,12 47:13,16 48:8 48:9 49:14,20 53:6 54:11 55:6 56:5 57:5 57:6,7,11,19 57:20 58:17 59:5,7 60:12 63:3,6,8 64:12 64:14 65:1,4 65:15,18 66:14 66:15 67:18 68:13 70:14 71:4,7 77:18 81:4 82:3,7,13	86:14 88:8 93:6,8,9,16,21 93:22 94:3 95:16 96:6,8 97:1 98:11 100:18 101:8 101:18 102:2 102:10 103:19 109:2,7 132:21 133:4,21 134:3 134:17,19 145:18,20 146:1,10 148:4 148:8,19 150:11 157:7 157:11 158:14 159:6,8 160:10 161:4 162:22 163:7 170:8,17 170:22 177:11 178:1 186:13 186:14 187:6 188:4,8,12,15 188:16 189:2 189:13 190:18 196:19 197:6 199:8,10,11,12 200:2 208:15 208:16,20 227:2 228:17 229:10,12,14 236:14 245:8 248:14 262:11 262:12 274:9 274:15 282:12 286:1 287:13 <b>collections</b> 30:18 54:14 56:8 59:17 94:10 137:5,8 157:9 <b>collects</b> 38:4 <b>Collins</b> 2:7 4:14 27:7 28:13	35:5 63:1,5,9 67:5 97:11 98:3,15,18 100:13 111:13 116:14,22 152:13 155:3 155:10,12 156:6,17 157:1 157:15 189:18 191:14 192:5 192:12,19 193:16 207:12 207:15 260:14 261:8 264:6 288:12 291:12 292:19 293:7 294:4,15 311:8 <b>collision</b> 143:19 <b>colloquial</b> 38:4 <b>combed</b> 166:12 <b>come</b> 25:19 33:3 34:11 41:3 65:3 99:14 118:3 136:17 160:16 169:1 176:16 184:1 198:6 221:18 226:22 260:7 260:12,16 263:10 266:2 278:8 298:12 310:1 <b>comes</b> 32:14,16 72:9 181:5 227:11 280:19 299:5 <b>comfort</b> 94:21 272:21 <b>coming</b> 27:7 126:14 152:14 182:19 183:15 194:10 204:19 207:2 258:15 258:16 259:18
---	---	--	--	--

260:15 261:15 286:22 299:1 311:9,21 <b>commencing</b> 1:17 <b>commend</b> 242:7 <b>comment</b> 14:16 40:5 63:22 82:18 83:14 86:3 111:1 195:22 196:3,8 196:15 234:2 249:20 276:16 307:16 <b>commented</b> 87:9 307:12 <b>comments</b> 7:10 19:15 32:7 132:12,13 182:16,17 210:5 272:18 307:9,13 312:8 312:10,11 <b>Commerce</b> 277:9 <b>commercial</b> 300:10 <b>commercializ...</b> 219:20 <b>commission</b> 172:8 257:17 257:18,22 313:17 <b>commission's</b> 172:15 <b>commissioners</b> 276:21 <b>commissions</b> 34:16,19 35:4 <b>commit</b> 155:20 172:17,18 <b>commitment</b> 310:20 <b>commitments</b>	267:20 <b>committed</b> 76:14 136:8 155:20 231:19 235:16 <b>committee</b> 211:22 212:4 213:9,16 214:7 214:8,22 215:5 226:12 234:1 244:22 249:21 250:4,6,18,22 268:10 290:11 290:13 304:17 307:9 <b>Committee's</b> 213:19 <b>committees</b> 84:11 98:21 99:11,18 100:3 100:6,9 <b>committing</b> 155:20 <b>common</b> 257:12 <b>commonly</b> 10:5 29:10 <b>communicate</b> 298:19 <b>communicating</b> 92:9 <b>communication</b> 7:15 12:12 25:15 50:9 52:10 87:21,22 90:14 91:20 94:13 95:5,20 103:16 108:14 108:18 120:4 123:8,12 134:16 138:13 138:14 139:12 175:8 197:3,8 221:3 288:8 <b>communicatio...</b>	9:14 12:2,10 12:17,19 13:3 14:8 15:11 19:17 24:7,12 25:22 26:17 37:4 40:17 51:19 52:14 54:16 55:5,7 55:16 73:15 82:8 86:15,18 87:3 91:9 92:3 92:7 94:14 95:22 101:3 115:14,18 118:19,22 119:1 121:5,5 122:3,6,12,14 122:19,21 123:6,16,21 124:1,4 125:5 131:9 132:1 133:4,13,19 134:5,7 135:20 136:5 137:11 138:6 144:10 144:11 148:1,2 151:21 152:4,7 152:9 155:16 159:17,22 161:4 162:10 163:6 164:1,21 165:16,22 166:4 167:9 170:18 174:19 175:11 180:20 188:17 189:10 189:11,12 190:3 192:6,14 195:6 197:14 199:1 201:18 201:18 226:3 227:13 229:22 234:19 271:6 287:8 293:5	<b>community</b> 46:19 64:21 99:15 241:11 <b>compact</b> 265:11 <b>companies</b> 53:18 70:5 218:7 221:16 228:17 240:20 272:10 273:7 273:13 282:9 282:10 283:2 300:22 <b>company</b> 52:1 53:10,14,21 69:21 70:8,16 107:1 272:14 <b>comparative</b> 237:21 <b>compare</b> 257:14 <b>compared</b> 184:4 <b>compatibility</b> 241:13 <b>competing</b> 282:10,17 <b>competition</b> 241:15 <b>competitiveness</b> 283:1 <b>complementary</b> 66:3 <b>complete</b> 130:21 302:11 304:2 312:5 <b>completely</b> 12:8 64:10 69:8 129:14 172:4 195:5 291:3 <b>complexity</b> 34:2 <b>compliance</b> 11:12,19 23:10 62:7,12 72:13 73:7,16 94:21 152:10 212:1 250:7 251:12	306:22 307:7,9 <b>complicated</b> 97:14 <b>complies</b> 21:4 132:21 <b>comply</b> 21:6 53:19,22 290:17,19 <b>comprehensive</b> 62:7 <b>compromise</b> 131:12 132:4 <b>compulsory</b> 25:13 70:15 <b>computer</b> 12:19 147:18 197:15 226:9 231:8 294:2 <b>computers</b> 198:7,9 <b>concede</b> 277:18 <b>concentrate</b> 233:20 <b>concentration</b> 225:9 <b>concept</b> 167:11 236:4 309:14 <b>concepts</b> 102:1 189:16 196:6 218:12 <b>concern</b> 18:9 36:18 45:13 92:19 94:2 95:17 118:16 119:22 120:9 157:17 181:5 205:19 269:22 282:18 291:17 <b>concerned</b> 114:4 114:22 199:13 254:6 <b>concerning</b> 63:11 <b>concerns</b> 14:10
---	---	---	---	---

15:2 23:11 94:5 114:2 118:1,11 119:16 120:16 152:20 153:5,7 153:9,11,16,19 200:4 217:11 236:18 239:22 254:17 272:11 282:17 <b>concise</b> 309:6 <b>conclude</b> 128:17 130:20 131:10 166:1 <b>concluded</b> 16:5 53:11 55:9 60:3 127:12 <b>concluding</b> 151:12 166:2 <b>conclusion</b> 29:21 55:2 120:12 164:14 166:5 276:2 302:20 <b>conclusions</b> 235:3 <b>conclusively</b> 178:20 <b>concrete</b> 103:9 189:7 <b>condemn</b> 132:7 <b>conditions</b> 212:14 <b>conduct</b> 12:15 22:11 121:3 123:15 124:4 126:1,16 127:1 127:8,14 128:1 128:6,14 131:13 182:21 183:13 195:17 216:5 240:15 246:6 270:9 275:12 277:4	285:12 290:1 305:9 <b>conducted</b> 21:19 25:14 37:19 62:19 75:22 129:21 130:3 139:1 179:4 282:13 <b>conducting</b> 20:9 29:11 75:19 130:12,14 134:16 168:22 262:6 277:1 <b>confers</b> 229:20 <b>confess</b> 261:15 <b>confidence</b> 42:10 292:9 <b>confine</b> 113:22 <b>confirm</b> 6:9 114:12 <b>confirmed</b> 129:9 129:16 134:12 214:2 <b>confirms</b> 212:18 <b>conflate</b> 49:16 <b>conflated</b> 133:21 <b>conflating</b> 162:12 <b>conflation</b> 182:14 <b>conflict</b> 140:21 262:21 264:1 <b>conflicting</b> 264:4 <b>conflicts</b> 260:1 <b>conform</b> 109:21 <b>confused</b> 147:16 171:8,13 191:2 <b>congratulate</b> 260:15 <b>Congress</b> 5:9 11:14 12:9 62:13 68:22	69:6 72:16 83:22 85:10 98:16 100:7,11 131:14,18 164:15,19 166:16 177:8 180:1 185:19 293:18 294:9 307:2 308:20 <b>congressional</b> 84:10 <b>connect</b> 46:20 <b>connected</b> 299:2 <b>Connecticut</b> 1:16 4:8 <b>connection</b> 33:18 100:3 <b>Conrad</b> 212:3 212:11 213:9 <b>consensus</b> 220:21 <b>consent</b> 4:21 312:19 <b>consequence</b> 77:5 94:18 <b>consider</b> 27:18 92:10 144:15 171:2 255:22 <b>considerably</b> 48:22 <b>consideration</b> 252:11 <b>considerations</b> 232:5 <b>considered</b> 19:17 69:12 75:16 140:15 141:6 145:8 216:6 251:14 <b>considering</b> 127:11 241:22 263:5,7 <b>consist</b> 6:12,16 6:21	<b>consistent</b> 9:19 12:22 22:15 43:4 74:21 86:7 104:19 128:20 169:13 211:16 214:12 <b>Consistently</b> 34:19 <b>conspiring</b> 140:1 <b>constitutes</b> 216:12 269:19 <b>constitution</b> 10:16 126:1,20 127:7,11 169:13 183:15 198:21 258:4 <b>constitutional</b> 5:18 6:18 11:1 71:12 74:18 82:14 109:20 109:22 114:2 125:14 126:10 127:4,14 128:1 128:6 131:17 136:10 137:14 194:2,8 197:9 197:11 235:5 237:19 256:7 258:6,21 260:1 263:20 <b>constitutional...</b> 75:16 76:4 78:3 121:19 170:14,21 <b>constitutionally</b> 194:11 256:21 <b>constrained</b> 256:20 274:17 <b>constraints</b> 128:13,18,19 128:19,22 183:7 <b>construction</b>	118:2,13 <b>consult</b> 88:17 <b>consulting</b> 87:7 <b>consumption</b> 106:10 <b>contain</b> 122:15 134:8 136:7 <b>contained</b> 313:6 <b>contemplate</b> 165:14 <b>contemplated</b> 80:5 163:22 164:15 166:8 <b>contemplates</b> 165:20 <b>contemplating</b> 164:20 166:17 <b>contend</b> 242:4 <b>content</b> 48:12 49:18,20 115:17 118:20 133:12,13 141:22 147:21 148:2 <b>contents</b> 155:15 165:3 <b>context</b> 39:13 46:17 47:2 48:15,16 50:21 62:2,19 65:22 83:20 86:19 88:16,21,22 96:15 107:9 118:20 138:19 146:15 154:19 154:21 156:5 158:17 160:5 165:19 179:4 197:18,20,21 206:7 225:1,2 225:20 226:5 252:12,18 270:14 293:3 295:14 298:11
--	---	--	--	--

307:17 308:2	<b>controlled</b> 246:8	156:6,17 157:1	252:16	304:19 305:6
<b>contexts</b> 12:15	<b>controlling</b> 15:7	157:15 189:17	<b>count</b> 38:15	306:8
28:10 29:13	249:15 259:6	189:18 191:14	<b>counterparts</b>	<b>country's</b>
105:9,13 124:6	<b>controls</b> 239:17	192:5,12,19	240:10 242:10	124:16 265:20
160:6 308:2	241:20 255:12	193:16 207:12	<b>counterterror...</b>	275:8 276:17
<b>continue</b> 20:6	255:16 275:22	207:15 260:6	5:10 59:12	277:20 284:1
50:6 110:14	<b>controversial</b>	260:14 261:8	68:14,16 69:12	286:11
195:11,18,18	175:10,11	264:6 288:12	69:15 83:18	<b>country-specific</b>
224:2 252:2	<b>controversially</b>	291:12 292:19	<b>countries</b> 71:3	220:13
<b>continued</b> 289:2	232:14	293:7 294:4,15	128:7 213:17	<b>County</b> 313:5
<b>continues</b>	<b>controversy</b>	311:8	214:20 228:16	<b>couple</b> 10:2
118:16 184:18	36:18	<b>Cook's</b> 82:22	229:3 230:2	27:11 30:8
214:9	<b>convention</b>	93:3	232:15 233:8	32:7 33:3
<b>continuing</b>	231:21 232:9	<b>cooperation</b>	241:21 244:8	63:17 86:13
131:13 220:10	246:16,17	132:4	250:10 254:22	88:5 207:9
232:11	249:5 251:6,20	<b>copies</b> 231:7	258:17 265:11	244:11 249:10
<b>contours</b> 236:3	260:10 303:21	<b>copying</b> 174:17	265:12 269:8	274:7 284:20
261:2,9	304:3,5,9,16	<b>core</b> 301:22	274:5 275:11	284:21
<b>contracting</b>	308:5,7	302:5	276:22 277:2	<b>course</b> 74:15
213:4	<b>conventional</b>	<b>corners</b> 283:8	277:19 278:18	81:18 132:11
<b>contradict</b> 266:4	159:7	<b>correct</b> 37:6,7	282:5,6,11	132:19 134:12
<b>contrary</b> 35:3	<b>conventions</b>	39:11 41:13	283:4 284:10	134:16 136:15
41:12 122:9	234:10	42:3 44:20	285:16 286:7	180:1 258:13
133:22 134:19	<b>conversation</b>	46:12 56:2	289:12,17	283:10 301:21
166:18 178:7	98:9 124:21	63:7 70:1,11	290:3,18	302:8 304:7
<b>contrast</b> 19:2	189:20 288:14	71:3,10,10	291:19 292:9	<b>court</b> 7:16,19
<b>contributes</b>	<b>conversations</b>	75:4 101:14	301:18,19	8:21 9:8 11:13
74:13,15	14:4 124:17	204:7 274:20	303:16 304:6	11:14,17,20
<b>contributions</b>	142:1 156:13	<b>correctly</b> 79:18	305:17 306:2,4	12:22 14:18,21
134:22	279:7	101:1 179:17	306:9 309:15	15:8,15 16:12
<b>control</b> 192:8	<b>converse</b> 247:14	261:20	<b>country</b> 11:2	18:14 20:9,13
215:3,3,8	<b>convey</b> 108:15	<b>correspondence</b>	123:12 138:4	20:17,18 21:3
224:14 225:19	<b>conviction</b> 263:2	120:4 211:6	191:22 213:21	21:9 22:4,15
226:1 227:13	<b>convincingly</b>	298:16 299:4	229:2 235:11	22:18 23:12,12
232:19 234:13	234:9	<b>costs</b> 34:7 68:4	255:7,11	28:17 29:6,16
234:18,18,22	<b>Cook</b> 2:7 4:14	<b>Council</b> 3:17	258:11,12	29:18 30:1
241:9 244:16	27:7 28:13	209:13 210:11	261:22,22	43:3 44:22
244:20 245:4	35:5 63:1,5,9	<b>counsel</b> 2:13,15	262:7,10,16	45:4 48:1 49:2
245:14 246:21	67:5 97:11	2:17 3:9 35:13	264:13,17,21	49:7 55:9
256:18 257:15	98:3,15,18	35:14,15 87:15	265:2,19	74:19 75:13,15
269:19,21	100:13 111:13	88:17 113:15	268:20 283:8	75:17 76:3,15
270:19 271:7	116:14,22	119:8 277:9	289:19 291:10	83:8 94:8,17
296:8,11,12	152:12,13	313:10	296:20 297:5	94:20 98:13
297:16 308:10	155:3,10,12	<b>counselor</b>	297:14 303:12	112:14 115:16

116:2,16	286:13	205:16 209:17	<b>cycle</b> 46:2	178:9,9 192:3
127:11,16	<b>covenant's</b>	210:13 297:19	<b>cynical</b> 278:12	201:14
129:9,22	214:13	<b>criminality</b>		<b>datas</b> 257:12
139:21 140:2,4	<b>cover</b> 165:5	149:12,13	<b>D</b>	<b>dating</b> 233:11
141:4,6,10,16	<b>covered</b> 10:20	<b>criteria</b> 49:8	<b>D.C</b> 1:17 4:8	<b>David</b> 2:3 4:5
142:6,8,9	<b>covers</b> 118:9	78:9,12 81:20	<b>dangerous</b>	311:17
151:5 167:6	<b>create</b> 33:11,21	107:6 109:11	170:12	<b>David's</b> 58:1
171:12 173:4	118:5 183:3	275:10 278:9	<b>dangers</b> 259:18	97:12
186:9 204:19	217:5 220:7,14	<b>critierias</b> 106:13	259:19	<b>day</b> 42:18 62:8
205:4 206:5,12	233:16 247:14	<b>critical</b> 112:11	<b>data</b> 31:9 34:10	260:21 261:6
207:8 222:9	302:11	261:12	37:17,20 38:14	309:13 313:13
226:17 233:22	<b>created</b> 139:4,9	<b>critically</b> 221:4	45:2 47:7 58:9	<b>days</b> 36:1 59:22
235:5,6 240:5	<b>creates</b> 183:6	<b>criticizing</b>	70:19 79:21	61:20 181:12
240:12 246:15	226:5 308:8	239:15	95:18 115:11	214:5
249:11 256:7	<b>creating</b> 32:9,20	<b>critics</b> 126:16	117:7,20	<b>De</b> 2:15 22:2,15
257:19 259:6	174:18 301:11	276:15	120:15 172:11	23:5 25:2 30:8
259:18 260:1	<b>creation</b> 174:22	<b>cross</b> 241:22	172:22 189:3,4	35:13 37:7
263:20 274:12	<b>credibility</b> 42:7	300:9	189:5 196:11	38:11 39:5,11
294:9,22 310:4	<b>credible</b> 244:21	<b>cross-border</b>	196:13 198:16	40:6 44:8,14
<b>court's</b> 20:10	<b>credit</b> 153:13	238:22 300:18	220:7 223:6	44:20 45:18,21
76:9	<b>crime</b> 17:16	<b>crucial</b> 206:20	228:17,18,21	46:7,12 49:12
<b>court-approved</b>	19:6 29:12	207:5	229:2,5,10,11	54:5 56:3,22
86:8	32:2 108:1,2	<b>cruelties</b> 256:9	229:13,19	57:3,11,17
<b>courtroom</b>	109:4 136:7,13	<b>CT</b> 83:20	230:3,3 231:8	58:20 62:1
142:4	148:16 155:21	<b>current</b> 74:14	231:9 233:8	63:4,7 65:19
<b>courts</b> 15:14,21	172:18 232:7	<b>currently</b> 84:12	235:10 236:14	68:17 70:12,20
17:21 85:10	303:21 304:3,4	178:1	238:9,13,20	71:4,10 72:6
118:2 121:14	304:9,15	<b>curtain</b> 203:10	240:20 241:1,5	74:8 76:20
126:7 127:21	<b>crimes</b> 257:6	<b>custody</b> 28:9,12	241:20 248:12	78:18 79:2,14
129:16 130:4,9	<b>criminal</b> 3:21	30:3,6 271:2	269:11 273:8	82:2 83:13
132:1 138:21	12:15 19:5	296:14	276:14 283:7	87:8 88:13
139:18 150:3	29:8 77:19	<b>customary</b>	283:13 300:10	90:7,18 93:11
150:10,12	86:20,21 88:11	231:16 262:1	300:14,18	94:7 95:7,11
154:13 184:1	88:13,16,19,22	262:14 263:1	302:15 303:11	97:5 98:1,14
186:18 199:13	115:10,15,21	289:11 304:22	308:18 309:2	98:17 99:20
234:3 236:12	115:21 117:22	<b>customer</b>	<b>databank</b> 47:22	103:17 106:16
307:22	118:7 141:18	228:18	<b>database</b> 37:4	108:1 109:1,18
<b>covenant</b> 211:1	142:3,4,15	<b>customs</b> 198:10	38:5 39:10	110:5,10,14,21
213:2 214:10	144:4 145:3	<b>cut</b> 269:15	48:4,22 175:1	112:2 178:11
223:16 224:7	146:10 148:7	<b>cyber</b> 53:13	199:21 200:2	<b>de-task</b> 73:13
224:11,17,18	148:20 149:5	60:19 108:10	201:2	<b>de-tasked</b> 73:3
233:21 248:1	149:11 174:4	108:10 223:2	<b>databases</b> 62:6	<b>deadline</b> 312:10
250:19 267:8	176:9 181:2	232:7 303:21	86:5 114:17	<b>deal</b> 222:4 235:4
271:11,12	198:14 201:13	304:2,4,9,15	119:7 123:22	<b>dealing</b> 235:18

259:10 307:20	<b>decoupling</b>	295:22 296:22	102:15,21	<b>described</b> 30:15
<b>dealings</b> 272:4	300:8	297:1,7 298:3	103:3 104:4	<b>describing</b>
<b>deals</b> 49:17,18	<b>dedicated</b> 36:11	298:11,12,21	105:7 160:18	158:18
49:22 252:8	<b>dedication</b> 36:6	299:7,14	162:16 163:13	<b>description</b>
<b>dealt</b> 249:3	<b>deepening</b>	301:17 302:18	164:4,17 165:4	108:21 187:13
300:16	235:15	<b>definitions</b>	165:9 195:21	<b>designations</b>
<b>Dean</b> 3:16	<b>deeper</b> 236:1	50:15 173:22	195:22 197:10	200:21
209:11 301:3	<b>deeply</b> 36:4	296:18 297:2	197:13 199:5	<b>designed</b> 13:2
<b>debate</b> 70:4	99:16	301:20	199:17 200:6	16:22 17:10
77:13 224:4	<b>default</b> 46:3	<b>definitive</b>	200:11 254:19	60:11 104:16
252:1 273:18	47:5,6,8 96:2	250:11	254:20 255:10	<b>desirability/n...</b>
276:18	202:10	<b>degree</b> 80:9	255:20 260:7	204:12
<b>debated</b> 220:6	<b>defendants</b>	185:1 194:14	283:18,22	<b>desire</b> 191:15
<b>decade</b> 34:14,15	77:19	242:13 261:1,4	284:19 286:4	<b>desk</b> 294:3
<b>deceiving</b> 283:6	<b>defending</b> 167:5	261:9 269:8	286:15 287:12	<b>despite</b> 216:22
<b>December</b> 236:6	<b>defends</b> 158:22	<b>degrees</b> 6:13	287:19 288:5,9	252:2 257:12
313:17	<b>Defense</b> 188:11	<b>delay</b> 33:4,9	309:8	282:6
<b>decide</b> 107:6	<b>defenses</b> 159:1	<b>delegation</b>	<b>Dempsey's</b>	<b>destroy</b> 122:11
110:2 111:21	<b>defer</b> 72:6	212:21	176:22	152:4
275:16	<b>deference</b> 249:6	<b>delete</b> 104:9,11	<b>denied</b> 205:4	<b>destroyed</b>
<b>decided</b> 74:4	<b>deficiencies</b>	<b>deleted</b> 101:8,13	<b>deny</b> 226:12	201:21
<b>decides</b> 78:11	241:19	108:16	<b>Department</b>	<b>destruction</b>
<b>decision</b> 44:5	<b>define</b> 143:9	<b>delve</b> 23:19	2:20 11:9	59:13 201:17
45:7 78:9,15	236:3	<b>delving</b> 36:4	35:18 42:19	201:22 285:7
110:13 129:10	<b>defined</b> 117:13	<b>democracies</b>	59:20 61:13	<b>detached</b> 141:3
140:11 259:6	117:15 122:16	240:3 255:2	62:9 167:7	<b>detail</b> 11:7
259:17	161:12 215:1	<b>democracy</b>	210:9,13 234:7	25:10 87:11
<b>decisions</b> 61:21	299:5,13	175:12	252:17 272:19	120:13 159:5
62:17 77:22	<b>defines</b> 212:7	<b>democratic</b>	273:3 277:10	241:16 272:21
79:1 217:13	216:19	125:1 221:8	<b>Department's</b>	273:6
226:20 290:12	<b>definitely</b> 37:7	237:6	188:11	<b>detailed</b> 95:15
290:20 294:12	68:17 97:22	<b>democratically</b>	<b>depend</b> 64:15	281:2
294:16 307:19	156:9 258:22	292:2	190:7	<b>details</b> 112:5
<b>decisive</b> 235:2	279:20	<b>demonstrate</b>	<b>depending</b>	130:8 237:21
<b>declaration</b>	<b>definition</b> 24:5	302:14	105:2,5 143:9	292:21
300:12	82:3,12 87:5	<b>Dempsey</b> 2:6	<b>depends</b> 66:7	<b>detained</b> 270:18
<b>declassification</b>	96:7,11,12	4:14 35:20	<b>deprived</b> 233:6	270:20
75:6,8,12	104:14 105:8	38:1,22 39:8	<b>deprives</b> 232:19	<b>detainees</b>
<b>declassified</b>	165:1,10,17	39:14,18 69:16	<b>Deputy</b> 2:19 3:6	307:21
5:22 11:16	173:21 196:1	70:4,18 71:1,8	35:16 113:12	<b>detention</b>
76:16 93:13	279:5 282:7	71:11 74:17	<b>derivative</b>	225:20 270:14
134:14	285:1 286:5	75:5,9,15	109:20	270:17
<b>declassifying</b>	289:9,17	77:14 100:16	<b>derived</b> 65:14	<b>determination</b>
292:13	295:16,19,20	101:15 102:5	<b>describe</b> 153:3	14:19 40:8

41:4,5,15	25:3 26:20	<b>digital</b> 236:7	<b>disallow</b> 307:20	273:17 311:11
42:11,13,18,21	27:2,3,4 30:16	<b>dignity</b> 217:17	<b>disclose</b> 111:7,7	<b>disinclination</b>
45:22 47:1	30:18 34:9	259:2	241:1	33:13
48:19 58:22	38:18 50:8	<b>diligence</b> 114:16	<b>disclosed</b> 111:10	<b>disinterested</b>
59:15 61:12,22	55:6,18 57:20	<b>diminishing</b>	269:7	140:5 141:3
71:16 73:17	58:3 66:8,9,10	219:6,7 225:5	<b>disclosure</b> 84:9	155:22
74:7,9,12,14	68:8 73:6	<b>Diplomatic</b>	197:21	<b>disparate</b> 46:21
74:16 156:9	86:12 102:1	231:22	<b>disclosures</b>	<b>disposal</b> 31:11
163:1,10,17	103:22 104:7	<b>direct</b> 79:19	218:18 219:1	<b>dispute</b> 127:6,22
192:22 193:6	104:12,21	105:22 117:12	238:11 272:14	158:12 232:15
242:15	105:2,4,8,9,12	<b>directed</b> 49:20	<b>discourse</b>	<b>disseminate</b>
<b>determinations</b>	105:13 106:12	80:21 110:16	157:13,17	17:13 31:21
42:15 43:8,13	106:13 107:5	168:11,14	<b>discover</b> 71:18	80:19 104:1,10
52:18	125:10 132:4,5	295:8	71:22,22 101:5	107:19
<b>determine</b> 42:20	138:14 139:16	<b>directing</b> 66:18	101:6	<b>disseminated</b>
46:17 64:20	144:13,15	<b>direction</b> 256:10	<b>discovery</b> 66:13	81:10 106:6
74:20 76:15	146:5 154:8	<b>directions</b> 66:19	<b>discriminant</b>	110:7
88:1 102:13	160:6,10	84:20	24:8 274:9	<b>disseminating</b>
140:6 178:20	162:13 176:4	<b>directive</b> 24:5	<b>discriminators</b>	110:11
267:1 288:17	180:10,15	47:20 50:18	147:20	<b>dissemination</b>
<b>determined</b> 44:9	182:5 188:6	54:8 79:18	<b>discuss</b> 95:16	9:22 17:8 81:5
44:15 65:6	192:20 199:12	217:15 229:9	121:12 166:18	103:20 104:17
74:19 75:1	224:1 230:16	237:13 252:14	166:19,21	111:17 117:7
162:17	233:7 236:10	<b>directives</b> 7:20	200:19	117:21 120:15
<b>develop</b> 301:21	236:13,13	26:3 53:16,17	<b>discussed</b> 58:5	174:14 229:10
<b>developed</b>	258:14,18	<b>directly</b> 35:3	94:11	<b>distances</b> 260:17
222:21 236:11	259:1 263:10	97:19 302:3	<b>discussing</b> 6:8	<b>distinction</b>
<b>developing</b> 68:2	277:18 280:18	<b>Director</b> 2:18	37:13,18 38:19	14:17 38:7
222:9	301:18 305:17	3:6,20 7:21 9:1	54:17 55:21	50:1 94:1
<b>device</b> 189:9	309:15,16,17	11:10 35:15	57:6 113:2	137:14 139:3
<b>dialogue</b> 27:9	309:19	42:20 59:21	155:15 190:17	145:18 146:9
301:8,12	<b>differentiation</b>	64:18 85:20,21	<b>discussion</b> 5:18	148:6 158:7
305:15,16	257:7	113:13 161:22	5:21 6:1,4 14:1	187:16 188:7,9
<b>Diane</b> 5:5	<b>differentiations</b>	209:15	20:7 36:18	188:13 196:18
<b>difference</b> 48:5	236:16	<b>Disabilities</b>	50:7,12 58:9	196:18 219:3
48:7 101:21	<b>differently</b>	251:7,20	58:21 113:21	266:16
182:2 192:10	20:17 34:4	<b>disaggregation</b>	209:2 235:6	<b>distinctions</b>
279:15	175:9 268:3	273:8	236:1,8 237:3	196:2
<b>differences</b> 19:8	<b>difficult</b> 30:4	<b>disagree</b> 76:18	237:22 243:17	<b>distinguish</b> 73:6
238:8 256:2,11	46:16 125:1	127:5 223:19	260:18 266:9	266:10
258:13 280:13	302:8	<b>disagreed</b>	284:12 300:3,7	<b>distinguishing</b>
280:14	<b>difficulty</b>	223:21	301:10 305:14	281:17
<b>different</b> 15:22	137:17	<b>disagreement</b>	<b>discussions</b>	<b>District</b> 139:21
18:16,17 19:3	<b>dig</b> 99:15 178:15	245:17	55:21 166:13	142:9

<b>diverse</b> 264:3	40:17 42:1	<b>drawer</b> 226:8	250:21 301:14	<b>electronic</b> 7:15
<b>diverts</b> 189:9	94:14 95:5,20	<b>drawing</b> 188:7	307:3	25:15 126:1
<b>division</b> 2:20	95:22 122:5,11	<b>drawn</b> 207:6	<b>effective</b> 67:8,10	133:14,16
35:18 139:10	134:16 136:4	<b>draws</b> 188:13	67:14 68:18	137:11 140:16
210:13	139:20 142:6	191:7	69:9 85:17	165:1,4,6,9,11
<b>DNI</b> 62:10 85:20	163:8 184:5,8	<b>drive</b> 170:21	215:3,3,8	171:17 188:13
99:16 110:16	184:18 185:9	<b>drug</b> 29:12	224:13 225:22	188:18 210:6
<b>doctrine</b> 179:7	185:11 265:8	<b>dual</b> 212:12	233:16 234:13	244:19 246:6
200:10	269:9	<b>due</b> 114:16	241:9 271:7	246:10,18
<b>document</b> 59:17	<b>domestically</b>	240:1 251:12	<b>effectively</b> 64:20	264:16 265:7
59:19 61:5	114:15 138:22	<b>duty</b> 114:16	221:2 225:5	289:21 290:1
62:5 76:2	139:6 184:14	226:4 248:1,3	<b>effectiveness</b>	291:11 296:14
267:14	271:14	248:6,17	66:5 68:22	303:17 306:7
<b>documentation</b>	<b>Donohue</b> 3:4	<b>dynamic</b> 218:7	69:7	<b>element</b> 32:4
42:17 60:22	113:10,19		<b>effectual</b> 230:19	79:8 95:1
<b>documented</b>	116:19 117:3	<b>E</b>	<b>effectuate</b> 57:20	103:21 149:12
42:16 59:18	120:19 139:13	<b>earlier</b> 26:22	59:16	155:18 179:20
<b>documenting</b>	145:13 146:2	55:19 58:20	<b>effectuated</b> 54:9	204:13 221:21
61:8	146:13 149:1	61:20 74:5	109:5	245:11
<b>documents</b> 6:2,5	152:16,17	80:8 85:5	<b>efficacy</b> 63:13	<b>elements</b> 309:19
6:10 11:15	153:21 155:7	93:20 96:7	63:18,19 64:2	309:22
75:11,14 119:2	155:11,17	147:16 186:6	64:6,8 83:2,3	<b>eleven</b> 113:5
119:10 147:17	156:2,15,22	187:4 191:2	92:22	<b>eliminate</b> 34:20
178:8 188:2,9	157:3 160:17	195:4 196:17	<b>efficient</b> 228:22	<b>eliminating</b>
292:14 310:14	168:10 171:7	220:19 243:17	<b>efficiently</b> 31:5	203:17
<b>doing</b> 28:17	176:5,15	249:1 271:22	<b>efforts</b> 5:6 11:21	<b>Elisebeth</b> 4:14
86:9 89:22	177:16 190:22	272:8 274:15	213:7 218:9,15	<b>Elizabeth</b> 2:7
96:21 150:13	193:14 198:5	279:11 296:11	237:10	<b>email</b> 9:5 10:8
162:9,10 175:8	200:7,9 201:9	301:6	<b>either</b> 10:4 14:4	14:5 25:12
181:21 204:11	204:22 205:13	<b>early</b> 45:7 46:1	33:13 64:5	50:13 51:4
215:19 226:9	<b>door</b> 123:15	70:4	66:18 91:16	52:6,10 54:8
257:19 262:8	<b>dots</b> 46:20	<b>easier</b> 182:3	107:20 114:11	54:14,18,20
263:16 267:2	<b>Douglas</b> 140:20	<b>easily</b> 207:3	117:13 149:9	71:6 73:21
275:5 282:19	<b>download</b>	<b>East</b> 263:17	154:3 158:2	167:20 174:17
284:15 285:17	303:16	<b>echo</b> 170:4	173:5 189:9	191:9
286:9,16,18	<b>draft</b> 213:2	<b>economic</b>	245:10 254:8	<b>emailing</b> 56:19
291:19 292:8	276:12	117:17 218:22	262:10 266:13	<b>emails</b> 26:2,10
292:14 297:5	<b>drafters</b> 225:3	219:12,17	306:6	26:11 120:4
304:6 307:10	<b>dragnets</b> 253:6	240:16 241:14	<b>elaborate</b> 23:2	190:15
<b>DOJ</b> 43:7	<b>dramatic</b> 301:14	282:8 301:8	23:21 94:4	<b>embassies</b>
<b>dollars</b> 219:15	<b>draw</b> 169:12	<b>education</b> 58:1	95:14 127:3	231:20
<b>domain</b> 93:7	187:15 188:9	311:12	170:5	<b>embedded</b> 104:5
227:1	261:13 275:11	<b>effect</b> 83:11	<b>Eleanor</b> 212:21	<b>emergency</b> 33:7
<b>domestic</b> 9:13	288:16	192:15 213:20	247:12	<b>emerging</b>

301:21	<b>endpoint</b> 124:19	<b>entirely</b> 159:9	179:9,10	<b>everybody</b>
<b>emphasis</b>	<b>ends</b> 82:8	167:11 197:12	<b>established</b>	35:22 169:21
220:22 237:10	<b>enforceable</b>	<b>entities</b> 240:22	116:5 141:11	188:5 215:6
<b>emphasize</b>	307:14	<b>envision</b> 176:3	141:20 200:1	286:16,17
69:10 105:16	<b>enforcement</b>	<b>envisioning</b>	<b>establishes</b>	289:12
121:18 144:18	13:6 19:7	207:21	212:13	<b>everybody's</b>
151:12	118:5 136:5	<b>equal</b> 253:18	<b>estimate</b> 93:14	174:18 252:1
<b>emphasized</b>	143:19 144:20	<b>equality</b> 231:5	<b>estimating</b>	<b>everything's</b>
183:20	156:1 203:18	264:16,22	65:17	185:3
<b>emphasizing</b>	277:13 306:16	<b>equally</b> 186:12	<b>estimations</b>	<b>evidence</b> 17:15
13:8 143:14	<b>engage</b> 127:19	<b>equates</b> 43:10	263:4	19:6 21:18
<b>employed</b> 129:3	175:10 196:22	<b>equivalent</b>	<b>etcetera</b> 109:16	32:1 108:1,2
<b>employee</b> 111:7	197:1 262:12	205:15	120:4 161:5	109:4 122:9
<b>empowering</b>	264:10	<b>eroded</b> 222:13	171:6,6 173:7	136:7 142:3
84:10 225:4	<b>engaged</b> 16:6	<b>erroneous</b> 43:12	179:7 196:2	146:20 148:16
<b>en</b> 227:5	115:14 156:2	73:17 178:2,4	307:21 309:20	169:1,6 186:15
<b>enables</b> 8:17	158:11,14	<b>erroneously</b>	<b>EU</b> 238:12,13	<b>evident</b> 204:18
<b>enabling</b> 222:10	194:12 196:21	74:7	239:15 241:8,9	<b>evolution</b>
<b>enact</b> 228:16	<b>engagement</b>	<b>error</b> 43:9	241:14,15	193:22
271:14	113:12 221:3	<b>especially</b>	275:21	<b>evolving</b> 305:15
<b>enacted</b> 15:20	284:13	119:19 126:3	<b>Europe</b> 220:9	310:12
<b>enactment</b>	<b>engaging</b> 233:12	129:20 163:4	220:12 275:19	<b>ex</b> 20:18 21:19
127:20 128:4	242:7 262:10	170:15 233:7	276:15 310:18	21:20 42:16
130:18 194:13	<b>England</b> 307:18	236:20 259:3	<b>European</b>	59:19 82:10
194:18 195:20	<b>enjoy</b> 15:7	269:5 303:20	226:17 239:14	206:8
<b>encompasses</b>	<b>enlightening</b>	304:15	241:6 246:9,15	<b>exact</b> 93:17
87:19 279:7	209:1	<b>espionage</b>	246:16 276:10	222:6
<b>encounter</b> 87:16	<b>Enlightenment</b>	231:18,19	276:13 301:19	<b>exactly</b> 13:12
<b>encountering</b>	233:11	241:14 262:19	308:5,7,9	44:1 185:8
59:12	<b>enormous</b>	263:3,16	<b>evaluate</b> 64:2,12	248:14 291:22
<b>encourage</b> 64:8	270:10 302:14	305:10	64:14 66:4	293:11,17
<b>encouraged</b>	<b>ensure</b> 9:10,18	<b>espouse</b> 278:19	84:14 186:22	<b>examination</b>
46:20	16:22 24:8	<b>essential</b> 245:10	205:10	205:16
<b>encourages</b>	44:22 61:2	<b>essentially</b> 24:6	<b>evaluated</b> 22:22	<b>examine</b> 110:16
312:6	212:8 224:9	43:10 61:6	65:22 94:17	<b>examining</b>
<b>encroach</b> 126:22	243:14 248:1	91:7 104:15	<b>evaluating</b>	238:7
202:11,12,13	254:1,3 271:10	108:20 118:9	110:22 243:3	<b>example</b> 17:12
<b>encrypted</b>	271:16	130:15 144:11	<b>evaluation</b>	17:18 19:2
118:21 119:1	<b>ensuring</b> 58:18	145:5 198:2	63:12 69:7	26:14 32:16
135:20,21	<b>entails</b> 106:11	224:16 229:7	72:11 83:16,19	47:7,13 59:12
<b>encryption</b>	299:12	269:20 297:20	84:6 94:18	66:10 71:9
222:18,20	<b>entire</b> 71:3,9	305:9	<b>event</b> 5:7 141:8	73:7 81:7
<b>endorse</b> 123:8	98:8 105:6	<b>establish</b> 40:18	<b>eventually</b>	83:17 99:22
280:10,11	110:10 165:13	42:2 177:20	294:13	109:10 153:8

165:18 167:1	85:12 125:22	56:13 283:18	214:4,18	95:8 103:12
169:19 186:16	126:16 127:21	<b>expires</b> 313:17	225:17 227:17	134:14 135:22
188:10 190:11	128:5,14 140:2	<b>explain</b> 11:6	229:5 234:12	139:7 143:18
207:1 222:16	140:4 142:13	20:7 44:1	244:14 245:12	150:1,15
225:8 256:13	142:14 182:20	50:11,19 58:2	270:13 271:12	155:13 158:10
259:5,17 265:6	183:1 187:17	58:12 82:7	271:18,19	158:13 159:9
268:20 281:6	188:12 229:15	129:5 193:8	289:18	160:11 163:4
290:16 298:16	256:14 291:4	262:13 311:17	<b>extraterritorial</b>	166:1 172:14
300:12 302:2	291:22 292:1	<b>explained</b> 21:5	216:5 224:3	173:7 177:22
<b>exasperation</b>	293:11,17	28:2 212:3,22	234:4,9,15	180:18 200:16
291:17	<b>exempted</b>	213:10	256:1 268:18	214:5 215:16
<b>exceedingly</b>	229:13	<b>explaining</b> 21:8	268:21 291:9	218:13 219:13
69:14	<b>exercised</b> 127:7	39:2 91:14	303:1	221:10 244:12
<b>exception</b> 14:11	234:20	<b>explanation</b>	<b>extreme</b> 168:3	245:5,7 246:14
15:19 16:1	<b>exercising</b>	56:21 76:4	169:19 242:3	251:14,15
115:7 117:12	121:20	<b>explicate</b> 76:8	<b>extremely</b> 49:2	252:13 253:3
130:7 139:14	<b>exist</b> 102:8	<b>explicates</b> 87:11	251:5 254:6,16	258:20,22
143:6 149:18	160:13 184:18	<b>explicitly</b> 164:10	<b>eye</b> 99:5	274:22 275:3
150:2,4,5,15	227:6 240:7	164:11 165:5		284:8 290:21
150:17 151:6,9	287:6 301:8	<b>explosives</b> 56:20	<b>F</b>	294:6 302:19
183:3,6 184:16	<b>existence</b> 156:12	<b>exposes</b> 229:5	<b>FAA</b> 123:17	<b>fact-specific</b>
185:14 186:5,8	<b>existing</b> 128:19	<b>expository</b>	165:14,19	41:15
186:20 259:21	310:14	275:14	166:16	<b>factor</b> 33:8
262:1,15	<b>expanded</b> 87:4	<b>expression</b>	<b>fable</b> 221:10	157:1 235:2
<b>exceptions</b>	<b>expect</b> 5:20	124:12 299:3	<b>face</b> 142:4	<b>factors</b> 23:6
95:13 102:7	46:22 58:15	<b>expunged</b>	187:22	<b>facts</b> 33:14
117:9 152:6	77:22 83:19	117:10	<b>Facebook</b> 191:7	41:16 187:10
202:2,4 299:20	169:2,7	<b>extended</b> 110:17	<b>faces</b> 130:21	<b>failed</b> 213:7
300:1	<b>expectation</b>	<b>extensive</b> 11:5,7	<b>facetious</b> 167:20	<b>failure</b> 229:4
<b>exchange</b> 7:7	121:6 190:9,13	44:20 45:16	<b>facial</b> 154:17	230:4
84:3 166:15	227:9	210:14 235:1	<b>facilitate</b> 229:14	<b>fair</b> 54:3 102:21
233:8 257:4	<b>expeditiously</b>	241:7 297:17	<b>facilities</b> 281:11	108:21 113:1
<b>excited</b> 283:3	32:19	<b>extent</b> 20:13	<b>facility</b> 162:15	158:6,7 159:6
<b>excitement</b> 35:8	<b>experience</b> 45:6	45:1 65:4 81:3	168:4	164:12 193:18
<b>exclude</b> 86:18	99:2,14 187:1	88:8 112:14	<b>facing</b> 218:21	208:19 260:20
<b>excluded</b> 195:5	210:14 219:5	163:11 170:4	<b>fact</b> 10:19 12:1	260:22 261:3
<b>exclusive</b> 218:13	284:9	207:22 221:11	16:21 27:15	262:10 308:6
<b>Excuse</b> 162:16	<b>experiencing</b>	274:3 275:3	32:8 40:9,19	<b>fairly</b> 84:3 97:14
<b>execute</b> 256:15	218:17 219:6	308:7	45:2 46:19	99:13 102:9
<b>executed</b> 85:15	<b>expert</b> 252:7	<b>external</b> 84:22	47:6 52:20	158:4 180:7
<b>execution</b> 292:3	<b>experts</b> 261:11	258:19	59:4 64:17	<b>faith</b> 71:19
<b>executive</b> 20:8	290:14 291:2	<b>extra</b> 33:15	66:15 74:14	250:21 267:21
68:20,21 81:7	<b>expire</b> 69:4	297:10	77:2 84:16	<b>faithfully</b> 85:15
81:11 84:3	<b>expired</b> 50:5	<b>extra-territori...</b>	87:22 92:8	<b>fall</b> 94:9 104:13

229:22 302:17	<b>filing</b> 77:21	<b>first</b> 6:12,19 8:7	48:1 49:7	7:1,13 66:20
<b>falling</b> 9:6	<b>fill</b> 8:15 67:1	10:3 20:2 24:3	74:19 75:13,15	86:16 132:16
<b>falls</b> 144:14	<b>fills</b> 26:15	25:19 27:12	76:15 83:8,9	174:13 201:4
<b>false</b> 284:14	<b>filter</b> 192:15	31:11 32:7	98:13 109:2	210:4 218:16
<b>familiar</b> 35:11	<b>filtering</b> 192:17	33:3 38:22	111:3 112:13	261:15 292:20
219:2,21	<b>final</b> 6:21	39:3 59:3 75:1	112:21 117:15	<b>focused</b> 56:3
<b>family</b> 211:5	120:15 124:9	76:3,12 80:6	118:10 121:16	57:12 68:11
<b>far</b> 48:15 88:19	208:21 303:9	114:3,5 119:16	125:19 126:12	85:22 92:19
97:6 117:2	<b>finally</b> 13:7	119:18,22	127:20 130:18	124:10 145:20
144:3 151:9	31:20 42:22	120:10,16	139:4,5,9	253:10 261:16
245:1 272:20	44:4 119:15	121:22 125:18	141:7,10 149:2	276:4,12
292:10	123:13 136:3	129:6 132:14	150:4,6,8	<b>focusing</b> 51:11
<b>far-reaching</b>	216:2 222:11	132:19 133:5	158:3 165:14	55:20 254:1
205:20	<b>find</b> 12:19 32:16	135:2,16 147:9	173:4 184:22	<b>folks</b> 76:21 77:6
<b>farthest</b> 260:16	90:13 114:17	152:2,20 153:1	184:22 185:4,5	98:5,6 127:5
<b>fashion</b> 66:3	115:20 152:14	153:4,6,9,10	185:6,17	128:20 219:2,4
243:5	153:2 154:15	153:16,17	186:21 187:2	<b>follow</b> 14:15
<b>faulty</b> 239:1	164:1 172:3	154:12,14,18	194:1 195:4,6	27:11 81:16
<b>favor</b> 4:17	178:16 266:8	155:8 156:4,14	200:20 202:9	98:4 120:10
130:11 258:5	281:15 287:3	156:20 157:14	204:13 207:8	192:20 206:13
312:15	295:22 298:12	157:18,21,22	208:2,7,14	247:1 282:17
<b>FBI</b> 18:4,15	303:2	158:4,15	222:8 288:20	288:14
19:2,3 30:6	<b>finding</b> 21:11	161:14 164:7	308:20	<b>follow-up</b> 56:16
35:13 61:19	43:12 124:7	165:1 169:11	<b>FISC</b> 22:10	152:18 207:13
78:22 85:21	135:22 153:19	171:15 179:12	59:10 62:12,13	291:13 311:5
86:4 105:17	153:20 193:12	180:17 182:15	62:16 72:14	311:12
108:3 257:9	<b>findings</b> 239:9	187:9,15	112:10 115:1	<b>following</b> 28:13
<b>FBI's</b> 106:1	241:18 242:18	201:20 205:3,5	134:13 202:18	56:15 93:2
<b>federal</b> 2:13	293:12	210:2 211:14	202:21 222:8	97:11 117:4
4:10 5:10	<b>finds</b> 123:1	211:21 218:22	294:22	196:9 235:10
86:21 111:6	169:6	221:5 223:10	<b>five</b> 4:12 17:18	238:15 239:18
<b>feel</b> 136:22	<b>fine</b> 102:16	232:4 235:8	47:8 69:5 99:9	266:18
137:2 154:3	289:5 295:9	236:3 247:16	101:8,10,11,12	<b>follows</b> 66:16
<b>fellow</b> 240:3	<b>finger</b> 288:13	248:21 256:13	104:8 172:5	166:7
<b>field</b> 233:19	<b>fingers</b> 116:17	258:7 272:12	214:5 301:8	<b>force</b> 265:6,18
<b>fifty</b> 214:14	<b>fingertips</b> 112:5	273:2 285:19	<b>flavor</b> 37:10	<b>forces</b> 215:4
<b>fifty-six</b> 218:6	<b>finish</b> 85:4	288:16 292:12	<b>flip</b> 182:3	308:9
<b>fighting</b> 303:21	<b>firm</b> 107:1	294:5,6,11	<b>flipping</b> 192:5	<b>forecloses</b>
<b>figure</b> 24:15	218:11 222:19	297:9 305:12	<b>flowing</b> 248:12	164:10
29:12 32:18	238:4	<b>FISA</b> 5:12,16	<b>flows</b> 85:19	<b>foreign</b> 1:7 2:10
67:4 172:1	<b>firm's</b> 238:5	7:19 8:21 9:8	127:9 228:21	3:3,21 7:14,17
<b>figuring</b> 24:13	<b>firmly</b> 221:1,9	12:16,22 15:15	229:20 300:10	7:22 8:4,18 9:2
<b>filed</b> 223:12	<b>firms</b> 272:4,19	15:20 16:12	300:18	9:5,19 10:10
<b>files</b> 45:15	272:22	20:16 29:4,6	<b>focus</b> 5:15 6:17	11:12,16 12:3

12:12 13:5	147:2 148:6,9	303:12,13,15	17:21 18:15	186:12 190:4
14:11 15:22	148:11,14	304:6 309:12	34:20 43:9,20	191:18 192:1,4
16:3,6,17	149:2,3,4,5,7,9	<b>foreigner</b>	63:11 82:21	192:8,17 193:7
17:14,15 29:7	149:10,14,18	281:17	99:1,6,9	200:4
31:18 32:1	150:1,12,15,21	<b>foreigners</b> 10:20	166:15 184:17	<b>frame</b> 125:15
43:2,21 44:15	151:2,6,9,15	109:11 180:18	240:9,20 246:9	126:11 145:9
44:21 45:3,22	162:3,7,19,22	181:21 229:10	254:6 295:15	<b>framework</b>
46:7,8,17 47:2	163:8,10,17	254:7 258:3	<b>foundation</b>	216:19 222:6,9
49:1 51:10	164:3 167:11	259:1 269:1	221:8,10	226:19 227:18
58:10,16 59:6	167:11,12	<b>foreignness</b> 41:4	<b>founded</b> 256:22	293:14 301:11
59:9,15 60:10	169:20 171:11	42:2,12 43:8	<b>four</b> 41:20 42:1	<b>frameworks</b>
60:14,18 61:1	173:19,22,22	43:12 52:18	113:22 114:4	239:7
61:8,21 67:19	174:1,2 176:9	58:21 61:12,22	178:13 283:7,8	<b>France</b> 239:7
67:21 68:12	179:22 180:14	74:12	<b>fourth</b> 10:16	240:11,14,21
73:11 79:10	181:1,11,14,21	<b>foreseeable</b>	12:1 13:1 14:9	<b>Franklin</b> 5:4
80:1,16,19	183:13 184:9	159:9	14:11 15:2,7,9	<b>frankly</b> 246:3
81:18,19 82:1	184:17 185:9	<b>foreshadowed</b>	15:12,14,17	251:4 297:8
82:2 85:6 92:6	185:14 186:4,8	239:14	16:2,9 17:4,22	<b>Frazelle</b> 5:5
95:9 102:13	186:13,19	<b>forge</b> 220:20	20:6,9,11,12	<b>free</b> 136:22
103:1 104:20	195:10 202:13	<b>forgive</b> 93:15	21:4,7,9,11,13	137:2 199:3
106:6 107:21	204:2,2,3	145:15	22:4,11,13,19	<b>freedom</b> 125:1
107:22 108:6	207:17,18	<b>form</b> 10:5 17:4	27:13,19 28:7	299:2,3
109:4 110:3,7	208:1,3,8,17	76:16	28:15 39:4,6	<b>Freiburg</b> 209:17
111:18,22	209:16 210:6	<b>forma</b> 99:2,6,12	39:15 43:4	<b>frequently</b>
112:1 115:6	210:18 215:12	99:19	74:21 75:19,21	144:3 154:15
116:2,6,7	215:16,17,21	<b>format</b> 144:15	80:13 94:22	<b>fresh</b> 74:14
117:11,17	231:9,10 232:6	<b>former</b> 234:6	116:10 117:22	<b>friendly</b> 244:7
122:9,15 126:2	232:17 233:1,2	<b>forms</b> 238:22	119:15,18	<b>froms</b> 163:14,16
126:2,6 127:1	235:18 236:22	<b>Fort</b> 34:17	121:2 126:5	168:7
127:2,8,10,14	239:3 240:6	<b>forth</b> 52:11	129:2,6,14,17	<b>front</b> 24:6 58:12
127:19 128:2,7	245:2 253:9	67:22 94:19	130:10 131:5,6	<b>front-end</b>
128:8,14 129:3	255:2 257:21	104:3 288:20	131:20 137:4	160:12 193:10
129:12,13,21	258:8 262:11	<b>forthright</b>	137:19,21	<b>frustrating</b>
130:3,7,15	262:12 264:10	159:14	138:8,16,17	63:11 266:8
131:13 133:10	274:12,16	<b>forum</b> 260:19	142:17 144:16	295:16
133:15 134:3,8	279:5,8 281:19	277:2 306:16	144:19 146:18	<b>frustration</b>
138:3,3,11	281:19 283:2	307:5	148:3 154:10	96:14
139:1,5,8,15	285:1,5,11,11	<b>forward</b> 32:19	154:15 160:4	<b>full</b> 12:9 69:21
141:5,13,13,15	285:12,15,16	113:21 242:19	172:21 175:22	75:19
141:21,21	285:17,21	247:18 273:4	180:19 182:9	<b>full-up</b> 21:14
142:12 143:3,4	286:4,6 287:13	274:8 310:17	182:11 183:2,3	<b>fuller</b> 87:11
143:7,15,22	287:17,21	310:20	183:4,6,8,19	<b>fully</b> 33:1 84:12
144:5,12,21	288:4,18,19	<b>foster</b> 5:17	184:11 185:1,8	<b>fulsome</b> 76:4
145:7,18 146:9	290:2 294:18	<b>found</b> 11:21	185:20 186:5	<b>function</b> 57:22

58:1 204:16,21 205:1 303:18 <b>functions</b> 230:20 232:18 257:20 <b>Fund</b> 277:11 <b>fundamental</b> 87:13 256:8 257:3 259:12 <b>fundamentally</b> 182:4,8 251:16 <b>funneled</b> 185:3 <b>further</b> 128:22 130:8 171:12 175:22 202:11 205:16 235:12 257:14 302:7 310:10 311:5 313:9 <b>further</b> 284:14 <b>future</b> 229:17 291:1	130:16 131:14 139:6,15 143:21 144:5 144:22 145:8 149:14 183:18 184:9 186:14 195:11 235:18 259:7 276:13 302:3 <b>general</b> 2:13,15 2:17,19 7:21 9:1 11:9 28:10 29:3 35:13,14 35:15,17 62:14 80:17 81:2 85:20 87:15 112:20 119:8 119:22 126:12 140:15 141:1 151:1 161:21 167:6 231:3 234:2 236:5 249:20 253:2 255:14,15 258:10 259:20 263:11,20 266:9 277:9 280:5 285:21 <b>General's</b> 106:15 <b>generality</b> 206:11 304:11 <b>generalize</b> 259:10 <b>generally</b> 106:17 107:17 107:19 130:9 149:14,19 163:3 167:7 187:5 216:18 219:19 273:21 279:8 <b>generated</b> 65:2 <b>generic</b> 57:14	106:19 <b>generis</b> 207:22 <b>generous</b> 137:7 138:21 <b>generously</b> 130:11 <b>Geneva</b> 214:5 <b>gentlemen</b> 36:2 <b>geographic</b> 91:6 133:7 162:8 <b>geography</b> 138:10 228:21 <b>Georgetown</b> 3:4 113:11 <b>German</b> 235:4 237:19 246:14 247:17 256:2,5 258:5 259:5 263:14 277:10 279:15 309:16 <b>Germany</b> 3:21 209:17 225:8 226:7 239:7 240:11,21 246:19 256:6 256:12,14,21 257:16 263:15 263:17 279:17 287:22 288:1 306:1,1 308:11 309:19 310:4,8 <b>getting</b> 24:11,21 35:8 51:16 62:3 99:9 103:13 125:11 154:6 264:3 298:20 301:9 310:20 <b>give</b> 8:13 60:17 61:3 63:22 110:3 122:4,18 142:19 159:16 160:15 197:16 213:21 250:9	250:20 256:1 263:6 266:1 268:20 272:21 280:20 282:5 282:15 284:4 305:2 <b>given</b> 26:19 42:1 54:1 123:19 128:11 131:14 200:16 249:7 252:3,21 277:17 282:17 306:2 <b>gives</b> 121:21 143:10 190:2 309:6 <b>giving</b> 259:1 299:11 <b>glad</b> 8:14 56:14 58:3 <b>global</b> 220:19,22 221:3 233:5,16 238:5 264:2 276:3 283:14 300:7 310:22 311:1 <b>globally</b> 232:8 300:4 <b>globally-integ...</b> 220:4 <b>go</b> 29:17 30:1,4 33:6,15 51:13 51:14 52:19 53:14,18 58:18 78:14 80:22 93:5 100:4 115:15 131:19 142:2 143:1 149:20,20 159:4 164:4 171:4,16 172:9 175:9,16 178:15 241:16 245:1 250:16	257:14 259:13 265:22 275:5 278:9,20 280:1 280:9 281:1 302:7,21 303:15 <b>goal</b> 261:6 <b>goals</b> 67:15,17 143:20 <b>goes</b> 46:14 53:20 78:21 97:12 143:12 158:20 183:11 272:20 275:21 276:9 299:16 305:13 <b>going</b> 21:10 34:3 36:3 48:14 50:4 51:15 52:15 53:4 60:15,17 61:9 64:15 71:11 74:17 83:1 84:7 92:16 100:16 104:15 104:21 105:1,4 132:16 136:21 143:1,18 145:9 149:17 167:3 170:8 173:3 178:1 179:16 180:2,9 181:21 182:10,14 183:18 195:11 196:1 209:2 210:4 213:15 223:13,19 226:6 227:2 228:8 244:2 250:14 261:6 264:11 265:13 281:18 286:22 287:3 295:5 296:9 302:12 305:16,17
<b>G</b>				
<b>G-10</b> 257:18 <b>gap</b> 26:16 33:11 33:20 <b>gaps</b> 33:12 <b>gardens</b> 220:7 <b>Garfield</b> 3:16 209:11 218:4,5 271:21 273:1 274:20 284:2,7 301:5 308:14 309:3 <b>Garfield's</b> 310:21 <b>gather</b> 142:15 145:3 151:2 181:1 186:15 <b>gathered</b> 144:11 <b>gathering</b> 14:8 54:16 89:16 115:7 128:15				

309:14,15	174:16,21	267:19 268:16	228:8 290:13	34:10 168:8
<b>good</b> 4:2 56:17	175:5,6,19	282:11 283:2	291:2	<b>handling</b> 217:20
68:2,7 71:19	183:12 187:19	286:6 290:7,14	<b>groups</b> 45:13	<b>hands</b> 174:15
75:5,7 145:11	187:21 189:4,8	300:17 303:5	213:16 215:19	291:3
209:6 250:21	190:20 194:12	<b>grabbed</b> 284:21	251:12 290:6	<b>hanging</b> 24:12
267:20 275:9	194:17 196:4	<b>grade</b> 277:6	290:18	<b>happen</b> 21:21
299:20,21	196:16,20	282:15	<b>growth</b> 118:12	254:5
<b>Google</b> 191:7	197:16,17,19	<b>grand</b> 4:7	<b>guaranteed</b>	<b>happened</b>
<b>Google.com</b>	198:22 199:20	153:12 156:7	304:20	115:13 171:3
51:7 55:4	201:19 206:22	156:18 194:6	<b>guarantees</b>	292:18 300:14
60:17 167:2	207:1,7 211:16	<b>grandmother</b>	237:11 242:10	307:11
207:2	215:12 222:14	81:22 167:21	258:6,21	<b>happening</b>
<b>gotten</b> 29:6,16	222:22 225:18	167:22	<b>guards</b> 298:13	68:20 137:10
29:21 251:5	228:10 234:17	<b>grandmothers</b>	<b>guess</b> 15:1 29:1	185:3 248:11
<b>govern</b> 111:20	239:3 241:1,2	171:20	33:12 54:12	<b>happens</b> 62:4,4
229:11	242:5 246:3,4	<b>grandson</b> 168:1	61:21 83:5	72:8 73:13
<b>governing</b> 105:3	246:9,14	<b>granted</b> 183:14	146:8 171:22	120:7
<b>government</b>	248:22 250:3	<b>granting</b> 228:9	176:11 186:11	<b>happy</b> 27:9
2:10 6:12 8:1	251:10 267:2	<b>granular</b> 62:18	189:22 193:8	50:10 116:1
11:6 16:3	267:12 268:3,6	<b>granularity</b>	203:12 207:21	120:12 198:8
20:19 30:22	270:20 271:2,7	273:10	208:2 209:22	200:9
31:6 38:4,14	272:15 273:14	<b>grave</b> 285:4	243:7,11,22	<b>harbor</b> 220:11
40:14 54:10	274:13 290:8	<b>gray</b> 172:2	254:20 264:6	300:11
64:4 66:19,20	291:16 294:17	<b>great</b> 13:20	272:17 274:10	<b>hard</b> 33:14 39:2
67:4 70:13,21	295:11,21	52:19 58:2	282:2 292:7	191:10 301:2
94:19 97:17	300:6 308:17	80:11 136:20	295:7,18	<b>harder</b> 138:8
108:6 109:13	<b>government's</b>	137:16 201:15	<b>guidance</b> 226:18	266:17
110:4 111:18	7:14 28:9	222:4 251:12	249:14 309:10	<b>harms</b> 228:14
121:3,20 122:4	31:11 37:15	252:21 253:8	<b>guideline</b> 104:6	<b>Harold</b> 223:20
122:11,18,21	122:2,19	254:8 296:2	<b>guy</b> 55:3,8 60:16	234:6 252:6
123:7,10,15	125:16 159:1	<b>greater</b> 47:16	73:10 137:22	<b>Harper</b> 212:3
124:20 125:3	159:21 169:10	48:15 94:2,11	167:2 207:2,2	212:11 213:9
126:8 130:12	174:15 187:10	221:12,14,21		<b>head</b> 87:12
130:21 131:7	188:2 189:5	240:1 252:11	<b>H</b>	95:12 101:20
132:5 142:1	192:7 241:4	272:13 273:10	<b>hacker</b> 108:10	210:12 212:20
143:12,21	303:3	273:15,19	<b>half</b> 34:15 98:6	<b>headed</b> 292:2
145:1 151:14	<b>governmental</b>	301:11	<b>halves</b> 162:6	<b>hear</b> 76:6 171:8
151:17,20	238:9,20 239:1	<b>greatest</b> 7:6	<b>hand</b> 41:16	215:9 294:10
152:8 158:11	<b>governments</b>	<b>grievances</b>	119:19,19	<b>heard</b> 70:7,8
158:13,22	106:7 112:1	200:17	188:14 191:3,4	115:4 172:12
159:16 160:3	126:2 215:17	<b>ground</b> 5:20	206:3 247:22	186:6 193:17
162:17 163:2	215:21 234:3	<b>grounds</b> 205:3,4	313:12	274:15 279:10
166:6,22 167:8	240:22 242:2	<b>group</b> 8:12	<b>handed</b> 139:22	289:16
169:5 171:3	246:5,20 250:8	203:20 211:22	<b>handle</b> 19:9	<b>hearing</b> 1:5,15

4:4,9,16,17 5:1 5:17 7:13 117:5 206:13 312:4,13,15,15 312:21 <b>hearings</b> 57:22 <b>heart</b> 305:13 <b>heartening</b> 276:10 <b>heeds</b> 269:2 <b>held</b> 1:15 15:21 16:12 129:22 130:5 142:6 147:13 150:3 186:19 201:10 201:14 213:5 307:6 <b>help</b> 20:14 66:13 135:11,12 146:11 194:8 194:10 202:14 218:19 292:8 296:1 <b>helpful</b> 24:2,18 50:16 58:6 88:1 117:16 152:15 153:2 192:19 221:15 221:20 222:15 223:8 260:18 272:10 273:5 273:11 275:5 311:6,22 <b>helping</b> 66:20 <b>high</b> 32:6 34:11 103:16 124:22 178:22 179:10 180:7 221:2 261:1,4,8 <b>higher</b> 95:21 <b>highly</b> 129:17 234:22 <b>hill</b> 222:3 <b>historic</b> 51:19	<b>historical</b> 128:21 233:10 <b>historically</b> 10:21 82:14 88:7 97:7 183:10,12 <b>history</b> 12:8 123:3 125:20 128:11 130:13 166:12,15 167:12 181:20 185:16 214:13 <b>hits</b> 299:22 <b>Hofstra</b> 3:8 113:14 <b>Hogan</b> 3:22 209:18 238:4,6 <b>hold</b> 93:3 97:9 <b>holding</b> 297:13 <b>holistic</b> 83:3 <b>home</b> 169:5 211:5 232:22 235:11 <b>homeland</b> 236:14 <b>homework</b> 311:11 <b>honest</b> 268:19 <b>honestly</b> 41:2 203:22 <b>honor</b> 219:9 267:20 <b>honored</b> 262:15 <b>Hood</b> 34:18 <b>hope</b> 46:22 132:12 136:16 173:20 276:14 <b>host</b> 100:6 136:9 <b>hostile</b> 285:4 <b>Hotel</b> 1:16 4:7 <b>hours</b> 98:6 <b>house</b> 138:1 217:10 226:7 <b>huge</b> 36:5 175:1	180:20 198:22 <b>human</b> 3:19 207:4 209:14 210:17,22 211:22 213:9 213:15,16,18 214:6,22 215:5 215:19 226:12 226:17 227:20 231:1 233:14 233:17,19 234:1 235:22 236:2 237:5,9 244:22 246:15 246:17 249:21 250:4,6,17,22 251:4,8,10 259:3 268:9 290:5,11,12,18 307:8 308:5,8 <b>humanly</b> 45:1 <b>humans</b> 233:14 <b>humility</b> 222:4 <b>Humor</b> 299:8 <b>hundred</b> 36:13 168:20 <b>hunting</b> 45:9 <b>hurting</b> 261:5 <b>hypothetical</b> 174:11 190:1 190:17 191:20 <b>hypotheticals</b> 167:17 170:6 170:15,19	226:13 234:4,8 234:12,16 236:21 242:21 244:13 246:8 246:12 248:8 249:1 252:7 261:16 268:21 278:15,20 280:10 289:18 289:20 290:4 291:10,11 295:10 296:4 297:15 298:11 306:6,15 307:7 307:19 308:1 <b>ICCPR's</b> 282:7 <b>ICJ</b> 290:17 <b>idea</b> 256:17 <b>ideas</b> 252:17 <b>identifiable</b> 81:14 179:3 <b>identification</b> 154:16,18 <b>identifier</b> 28:18 193:5 <b>identifiers</b> 37:3 37:19 295:1 <b>identifies</b> 163:2 <b>identify</b> 9:2 65:5 87:14 123:6 178:20 <b>identifying</b> 53:9 104:10 <b>identity</b> 60:8 <b>idiosyncrasies</b> 97:15 <b>ignore</b> 41:12 168:7 169:3,7 <b>ignored</b> 46:4 <b>ignoring</b> 172:4 <b>IGs</b> 308:20 <b>II</b> 3:1 142:14 144:6 194:1,4 <b>III</b> 3:13 29:10	121:16 155:21 197:18 206:7 <b>illegal</b> 263:8 <b>illegitimacy</b> 159:20 <b>illegitimate</b> 163:18 <b>illustrating</b> 302:16 <b>imagine</b> 30:3 76:17 204:22 297:8 <b>immediately</b> 101:19 201:21 265:1 <b>impact</b> 28:20 29:2 87:4 184:4 218:22 219:12,14,18 272:3 280:15 293:4 <b>impacting</b> 287:10 <b>impacts</b> 232:3 299:3 <b>impair</b> 280:14 <b>impermissible</b> 89:5 288:18 <b>implement</b> 58:13 268:8 <b>implementation</b> 69:19,20 188:11 310:6 <b>implemented</b> 69:20 74:21 306:21 <b>implementing</b> 187:19,21 196:6 267:15 306:19 <b>implicate</b> 192:17 <b>implicated</b> 115:20 153:4
--	---	--	--	---

171:16 191:19 248:18 <b>implicates</b> 14:9 <b>implicating</b> 94:12 155:8 <b>implication</b> 47:17 157:22 256:1 <b>implications</b> 27:14 33:2 114:20 120:10 123:4 138:15 170:22 171:10 175:1,22 198:12 205:20 205:21 219:18 220:16 <b>implicitly</b> 162:5 162:5 165:19 310:22 <b>import</b> 42:7 88:20 <b>importance</b> 247:20 273:19 274:8 292:15 301:10 <b>important</b> 10:2 12:13 13:13 19:8 36:12,17 49:19 60:1,10 65:13 69:9,14 80:7 82:5 119:12 124:10 125:18 139:11 143:5 151:11 187:15 198:19 199:15 201:5 221:4 222:10 223:4 236:9 248:7 251:1,3 254:14,18 273:13 275:17 289:1 311:10 <b>importantly</b>	305:12 <b>impose</b> 216:4 <b>imposed</b> 128:15 129:4 131:18 <b>imposes</b> 129:2 212:4 215:14 229:5 <b>imposing</b> 194:16 <b>impossible</b> 260:4 <b>imprecise</b> 208:10 <b>impression</b> 77:6 98:20 100:8 307:22 <b>impressionistic</b> 65:11 <b>in-country</b> 282:13 <b>inadvertent</b> 97:2 101:1,6 101:18,22 102:2 <b>inadvertently</b> 94:13 100:20 122:12 201:17 <b>inaudible</b> 259:14 303:12 <b>incident</b> 72:13 73:16 88:4 <b>incidental</b> 12:10 12:14 14:1 15:3 43:19 45:14 81:17 82:6,13 94:12 96:6,7,8,15,19 96:22 97:2 100:18 101:4,7 101:18,22 102:4,10 103:12 115:13 158:21 159:7 160:2,4,10 201:1	<b>incidentally</b> 12:2 13:3 15:12 16:10,20 17:11 43:18 52:13 79:21 80:1 92:9 106:4 108:13 159:3 160:13 180:3 <b>incidents</b> 11:12 11:20 34:17 <b>include</b> 75:13 109:11 117:16 117:17,18,19 124:1 135:13 151:4 215:2 270:6 276:21 <b>included</b> 128:9 200:18 308:22 <b>includes</b> 11:7,11 11:13 84:17 239:10 273:20 <b>including</b> 6:18 21:12 121:16 172:14 187:7 203:11 222:2 233:6 250:8 251:4,18 273:7 282:5 308:18 <b>inclusion</b> 114:5 <b>inconvenience</b> 49:6,10 <b>incorrect</b> 38:16 72:11 211:8 <b>increasing</b> 118:11 <b>increasingly</b> 219:9 220:2 <b>incredibly</b> 152:14 221:20 223:4,8 <b>incrementally</b> 228:10 <b>increments</b>	42:18 <b>independent</b> 240:2 308:16 308:21 <b>indicated</b> 271:22 <b>indicates</b> 84:2 171:15 <b>indication</b> 118:7 282:16 <b>indicator</b> 172:11 <b>indicators</b> 48:4 172:22 <b>indicia</b> 121:14 <b>indictment</b> 86:20,21 88:11 118:18 <b>indifferent</b> 198:22 <b>indiscriminate</b> 223:7 274:14 274:22 275:4 <b>individual</b> 29:13 64:11 73:18 106:22 114:10 114:18 116:8 123:5 141:12 149:8 154:7 170:1 177:20 178:6 205:12 205:13,21,22 212:14 225:19 225:22 227:12 228:12 237:17 281:16 294:1 310:6,6 <b>individual's</b> 254:11 298:15 298:17 <b>individualized</b> 10:17 158:7,17 160:7 199:2 206:4 <b>individuals</b>	115:20 118:3 120:1 140:1 141:17 212:9 214:11 217:11 229:22 237:15 237:16 242:5 244:15 245:13 248:4 253:7,10 271:17 281:7,9 281:10 292:2 <b>industry</b> 3:17 209:13 232:12 237:7 275:19 310:21 <b>ineffectual</b> 126:15 <b>inevitable</b> 83:5 <b>inevitably</b> 6:1 <b>informally</b> 24:11 <b>information</b> 3:16 5:22 6:3,6 6:10 7:15,19 8:1 9:21 10:1 13:4,14 14:13 15:11 16:10 17:8,11,13,19 18:9,22 19:3,5 19:10,12,16,19 19:22 27:16 28:1,6,7,8,11 29:9,14,17,18 30:2,5,21,21 31:2,4,10,16 31:19,21 32:10 32:11,21 33:16 34:21 35:3 36:4 37:15 38:20 41:11,12 41:21,22 42:8 43:17,17,20 44:9,14 45:14 46:13,18,21 47:3,4 48:22
---	---	---	--	--

51:8,11,15,16 52:2 53:5,15 57:7,8,12 58:11,16,19 60:17,18 65:9 67:20 68:6 69:22 70:9 72:9,18 73:3 77:20 79:11 80:20,20 81:9 81:14,17 83:18 86:1,2,14 89:4 89:16 93:12 95:10 100:19 103:12 104:1 104:10,12,18 104:20 105:5 106:4 107:20 108:9,11,15 109:12 110:3,6 110:11 111:8,9 111:22 112:8 112:21 114:5 115:5,9 117:10 117:11,16,18 117:19 118:3 119:5 120:5 122:15 133:11 134:8 136:2,14 139:17 141:7 142:2 143:21 144:1,2 145:3 146:3 147:4,12 147:13,19 148:10,17 151:3 154:3,7 154:9 157:10 157:12 158:15 159:2,8,17 162:3,18 167:19 169:21 170:9 171:4,14 173:8,9 174:1 174:15 175:20	176:6,6,7,17 177:13,18 178:16 179:3 179:11,18 180:2,6,10,12 181:1 191:10 193:1,2 198:1 198:11,17 199:14,18 200:3 201:1,3 201:10,12 203:17 209:12 217:21 226:22 237:16 239:10 240:6 242:2 243:18 244:5 254:2,7,10,15 256:17 257:4 273:14,15 279:6 281:18 285:2,10,16,20 286:1 287:13 287:20 293:1 294:18 311:15 <b>information's</b> 146:16 <b>informative</b> 67:19 152:15 <b>informed</b> 84:12 226:22 <b>infringe</b> 304:14 <b>infringed</b> 234:21 302:2 <b>infringement</b> 231:17 232:12 302:5 303:19 304:18 <b>infringements</b> 232:1,5 235:15 304:7 <b>infringes</b> 235:8 235:9 <b>infringing</b> 264:9 303:13	<b>inherent</b> 10:22 125:22 127:13 131:17 182:20 183:1 <b>initial</b> 64:3 74:9 78:9 114:1 118:7 <b>initially</b> 79:13 118:10 <b>initiate</b> 231:9 237:1 <b>injury</b> 172:17 <b>innocent</b> 171:21 <b>innovative</b> 218:7 <b>inquiry</b> 56:17 <b>insensitive</b> 217:8 <b>insert</b> 205:14 <b>inserting</b> 201:11 <b>inside</b> 9:16 20:8 91:10 97:20 128:2 159:19 212:5 245:6 282:10 283:3 306:1 <b>insight</b> 308:22 <b>insights</b> 194:6 <b>insist</b> 282:12 <b>insofar</b> 249:6 <b>inspect</b> 123:8 189:21 <b>inspecting</b> 197:2 <b>inspectors</b> 11:9 62:14 <b>installed</b> 190:2 <b>installs</b> 189:8,8 <b>instance</b> 31:12 111:20 114:11 119:21 120:2 136:13 253:13 <b>instances</b> 277:14 <b>Institute</b> 3:20 209:16	<b>institutional</b> 99:10 257:10 <b>institutions</b> 257:8,9,12 <b>instrument</b> 267:4 <b>integrated</b> 220:15 <b>integrity</b> 219:10 223:2,3 231:5 232:2,6,11 264:15,22 265:5 305:8 <b>intel</b> 98:21 <b>intelligence</b> 1:7 2:11,18 3:3 7:14,17,22,22 8:4,18 9:2,3,6 9:19 10:10,19 11:11,12,17 12:4 13:5 14:11 16:1,4,7 16:18 17:14,15 31:18 32:1 33:22 35:16 42:20 43:3,21 44:15,22 45:4 45:11,22 46:8 46:8,15,17,19 47:2 49:1 51:11 58:10,16 59:2,7,9,15,21 60:10,14,18 61:1,8,22 64:18,21 65:13 65:21 66:2,8 67:20 68:12 72:10 79:10 80:2,16,18,19 81:2 82:1,3 83:16 84:10,12 84:16 85:6 86:1 92:6 95:10 99:11	100:3,6,9 102:13 103:2,5 104:11,20 107:21,22 109:4 110:7 111:22 115:6,8 116:2 117:11 118:4,8 122:15 127:2,8 128:2 128:8,15 129:3 129:21 130:3,7 130:15 131:14 133:11,15 134:4,8 139:1 139:5,8,15 141:5,16 142:12,15 143:3,4,7,15 143:20,22 144:5,12,22 145:7,19 146:9 147:3 148:6,10 148:12,15 149:8,14,18 150:1,12,15 151:2,6,9 161:22 162:3,7 162:19,22 163:8,11,17 164:3 169:20 171:11 173:19 174:1,2 176:9 179:22 180:14 181:1,11 183:18 184:9 184:17 185:9 185:14 186:5,8 186:13,19 188:12 195:10 195:12 202:14 204:2,3 208:1 208:3,17 210:15 217:15 235:18 240:6
--	---	---	--	---

240:14,18	103:16 140:21	231:13,17	137:19 184:12	<b>involved</b> 70:6
241:10 253:4	148:21 159:21	232:6 233:17	224:13,22	88:1 132:2
253:12 255:2	237:20 253:12	233:19,21,22	270:13	141:3 149:11
256:14,19	261:20	235:22 236:2,4	<b>interpreters</b>	150:19 160:5
257:1,21	<b>interested</b> 91:15	236:12 237:3,9	249:7 252:5	198:13
258:19 259:7	92:7 132:20	252:2 260:10	<b>interpreting</b>	<b>involvement</b>
262:11,12	251:5 269:18	261:10 262:2	246:16 249:12	141:20 202:18
274:12,16	276:19 312:7	262:14,20	249:13	202:21
276:9,13 279:5	313:11	263:11,21	<b>interpretive</b>	<b>involves</b> 188:16
281:19,20	<b>interesting</b>	264:8 265:6,10	226:13	190:18
285:1,7,15	147:15 263:14	265:21 267:4,8	<b>interprets</b> 268:3	<b>involving</b>
288:19 294:18	<b>interests</b> 16:5	272:3 276:7	<b>interrelated</b>	199:14
302:3 309:12	27:4,4 47:17	278:6 285:5,6	230:18	<b>invulnerability</b>
<b>intend</b> 100:22	131:12 143:12	286:13 289:4,4	<b>interrupting</b>	239:3
223:1 239:12	145:5 217:20	289:7,8,9	48:11	<b>IP</b> 120:1,6,7
<b>intended</b> 77:9	218:1 224:2	298:5 301:17	<b>intervene</b> 205:2	<b>irrelevant</b>
97:7 122:1,17	230:6,17,17	305:21 306:5	205:6	165:10
274:21	240:17 260:3	306:10,11,20	<b>intervention</b>	<b>irrespective</b>
<b>intensively</b>	261:18 264:9	<b>internationally</b>	297:22	183:2 258:10
276:5	278:14	138:22 139:7	<b>interviews</b>	<b>islands</b> 220:14
<b>intent</b> 89:15	<b>interfere</b> 254:11	238:20 273:22	297:17	<b>isolate</b> 66:4
286:6	300:17	275:6 276:8	<b>introduce</b> 35:9	<b>isolation</b> 66:5
<b>intention</b> 134:3	<b>interference</b>	289:11 305:18	37:8 209:8	<b>ISPs</b> 26:2
<b>intentional</b>	211:5 216:9,12	<b>Internet</b> 26:7,8	<b>introducing</b>	<b>Israel</b> 225:13
11:21 40:16	298:14	191:9 219:19	33:9	<b>issue</b> 21:8 37:16
96:16 130:22	<b>interfering</b>	219:21 220:4	<b>intrusions</b>	37:17 49:15
<b>intentionally</b>	230:2	220:15	131:22	56:11 57:4
9:13 97:18	<b>internal</b> 41:18	<b>interpret</b> 107:6	<b>invaded</b> 190:8	69:17 91:6
131:8	54:10 70:12	225:7 244:1,3	<b>invasion</b> 190:12	106:18 110:21
<b>intentions</b> 67:21	236:10 241:15	268:4	<b>investigate</b>	138:9 223:20
<b>interact</b> 175:3,4	257:16 258:18	<b>interpretation</b>	34:16 302:10	225:10 226:18
<b>interaction</b>	259:22 274:13	87:1,2 202:15	<b>investigation</b>	240:18 269:4
99:19	<b>international</b>	212:19 213:18	116:9 141:19	276:7 295:13
<b>interactions</b>	3:21 121:5	214:10 225:14	<b>investigations</b>	295:18 296:15
99:10,11,17	122:2 123:21	247:22 249:5,9	2:14 124:5	300:21 301:9
<b>intercept</b> 9:13	138:14 147:4	250:11,19	<b>investment</b>	301:13 303:8
12:17	148:1 209:17	268:1,6 269:2	300:13	<b>issued</b> 5:13
<b>intercepted</b> 12:3	210:5,15,20,22	269:12,18,22	<b>inviolate</b> 261:21	21:10 75:2,18
<b>intercepting</b>	211:10,11,11	278:19 291:1,5	<b>invitation</b>	156:18
51:18 233:2	215:14 216:1	296:12 299:1	230:13 309:9	<b>issues</b> 3:2,14
<b>interception</b>	216:13,16,19	<b>interpretations</b>	<b>inviting</b> 218:8	5:19 6:18,19
118:20 161:4	217:3,5 218:1	243:8 249:14	<b>involve</b> 21:18	7:2 20:22
233:4 235:7	223:16 227:10	<b>interpreted</b>	86:15 150:19	21:10,22 34:6
<b>interest</b> 102:22	230:14 231:3	125:20 130:10	286:9	36:15 73:7

74:18 113:3	<b>Jim</b> 32:5 35:12	307:19 310:3,9	273:3	166:13,19
132:17 136:10	69:10 96:3	<b>judicially</b>	<b>justices</b> 140:10	168:4 173:13
136:11 144:19	160:15 306:13	307:13	140:18 249:11	174:11,22
197:9,11 198:6	<b>job</b> 64:19 80:18	<b>judiciary</b> 293:12	<b>justifiably</b> 175:8	177:10 180:5,8
198:7 209:9	99:8 257:19	293:13,13	<b>justification</b>	180:9 188:22
221:2 227:3	284:2	<b>Julian</b> 3:8	54:15 187:13	189:1,2 190:17
243:1,7,15	<b>Joe</b> 108:5,7,12	113:13	<b>justified</b> 259:16	199:12,12
261:12 300:16	287:21	<b>jump</b> 137:2	259:20	202:8 216:20
311:14	<b>John</b> 3:15	264:11 284:3,4	<b>justify</b> 159:13	226:5 230:13
<b>It'll</b> 76:18	209:10 266:15	295:9	186:9	242:13 253:19
<b>Italy</b> 239:11	286:15 295:8	<b>juris</b> 263:2		310:20
240:11	305:2 306:14	<b>jurisdiction</b>	<b>K</b>	<b>kinds</b> 20:12
<b>item</b> 73:3	307:17	22:16 83:21	<b>Katz</b> 140:9	158:18 180:17
	<b>joined</b> 113:10	212:10,15	<b>keep</b> 6:6 7:5	<b>Kingdom</b> 239:8
<b>J</b>	209:10	213:3 214:12	72:8 84:11	240:11
<b>Jaffer</b> 3:6	<b>joining</b> 209:1	214:21 215:2	101:10,11	<b>knew</b> 12:9 70:10
113:12 120:18	<b>jointly</b> 162:1	216:7 224:10	102:18,22	177:8 180:1
120:20 149:17	<b>journalist</b> 207:4	224:12 230:1	103:7,11,15	<b>know</b> 16:14
149:21 158:6	<b>judge</b> 43:14	243:10 244:2,4	104:8 116:15	20:16 22:6
164:7,18 165:7	77:13,16 78:7	244:4,5 247:3	119:4 126:13	32:18 33:20
165:12 168:18	82:6 106:2	247:5,11 248:2	128:12 138:10	34:6 36:9 40:1
168:20 173:10	111:14 117:8	263:18 270:2,3	171:5 283:3,7	41:2 51:6,7
173:15,18	163:4 167:14	270:4 296:6,7	<b>Keeping</b> 54:5	55:3 70:18
180:16 186:7	171:11 200:14	297:12	<b>kept</b> 45:8 106:5	76:1 78:15
186:17 187:14	248:19 252:20	<b>jurisdictional</b>	135:9 207:1	81:21 82:10,10
190:6 192:2,9	265:11 277:15	224:7 243:1,6	254:3 293:6	83:10,11 84:13
192:16 193:13	283:17 289:1	243:15,16	<b>Kerry</b> 277:10	84:20 85:5
196:15 198:18	289:15 300:5	245:11 246:21	<b>key</b> 26:14 56:4,6	90:5,14 91:19
199:9,22	307:15	248:9 270:12	57:13 108:6,11	92:13,22 93:17
201:16 202:2	<b>Judge's</b> 50:5	<b>jurisdictions</b>	135:15	99:15 104:5
205:18	<b>judged</b> 185:19	226:16	<b>kick</b> 102:12	105:16 106:10
<b>Jameel</b> 3:6	<b>judgement</b> 76:9	<b>jurisprudence</b>	154:1	108:11 110:9
113:11 149:16	76:12 97:7	308:6	<b>kid</b> 128:18	114:12 120:1
153:22 160:20	140:13	<b>jury</b> 153:12	<b>killing</b> 224:19	120:22 131:3
164:4,5 186:2	<b>judgements</b>	156:7,18	<b>kind</b> 11:2 12:14	132:19 134:2,6
196:10	275:15	<b>justice</b> 2:20 3:11	18:21 21:14	135:5,7 136:12
<b>Jameel's</b> 170:4	<b>judicial</b> 11:3	11:9 35:18	33:7 35:1	139:14 151:16
<b>James</b> 2:6,13	14:18 119:18	42:19 59:20	53:20 65:4	154:18 155:15
4:14	124:6 156:16	61:13 62:9	73:20 76:2	157:21 158:21
<b>Janosek</b> 5:5	156:20 157:19	66:6 67:3 74:4	86:1 92:18	159:4 163:4
<b>January</b> 5:13	160:11 201:11	106:14 113:17	124:5 138:5	167:2,10
47:19 221:7	205:19 206:9	140:3,10,19,20	157:7 159:6	168:22 169:3,4
237:14 276:12	237:1 241:4	167:7 210:13	160:12 162:8	169:17 170:15
<b>Jazeera</b> 120:6	292:4 293:2,20	233:22 272:19	162:11,11	172:8 173:3,6

174:9,9,12	265:12	283:21	280:13 287:2	252:7
175:13 177:3,4	<b>Koh</b> 234:6,8	<b>Laura</b> 3:4,18	289:4,4,7,8,9	<b>leads</b> 164:14
179:1,2,2,3	252:6	113:10 136:4	296:20 298:5	<b>leak</b> 297:20
184:11 186:22	<b>Koh's</b> 223:21	209:13 213:14	299:20 301:19	<b>leaked</b> 6:1
187:20 188:3	247:21	245:17 251:19	301:19 304:22	<b>leaking</b> 144:3
188:19 190:7	<b>Ku</b> 3:8 113:13	254:21 266:18	305:21 306:21	<b>leaks</b> 70:13
194:6 197:15	125:6,7 137:3	284:19 298:6	309:14	<b>learn</b> 134:14
198:18,20	137:16 139:14	305:20	<b>lawful</b> 21:4	<b>leave</b> 76:20
199:15 200:21	142:20,22	<b>law</b> 3:4,5,8,21	32:12 53:19	100:8
202:4,13 206:1	145:12 149:15	8:1 13:6 19:7	111:8,10 193:2	<b>leaving</b> 121:18
206:9,12	181:6,7 182:15	85:14 102:3,11	199:8 227:21	<b>led</b> 249:17
208:12,15,19	183:5 184:10	104:6 113:10	<b>lawfully</b> 13:5	<b>left</b> 204:9 270:1
210:8,16	193:17 194:5	113:11,14	28:5 29:19	299:17 301:9
213:14 217:10	202:6,7	118:5 125:14	30:20 31:3	<b>legal</b> 3:2,6 5:18
220:9,15 222:5	<b>Ku's</b> 147:1	127:4 136:5	34:21 37:14,20	6:17 10:13
222:5 240:4		143:19 144:20	38:21 102:20	20:22 21:15,22
243:17 244:17	<b>L</b>	155:22 182:11	175:20 177:14	25:13 29:21
245:21 247:21	<b>lack</b> 26:7 180:19	182:12,12	179:11,19,21	53:21 54:8
249:6,8 251:8	193:9 194:22	196:12 197:21	180:12 181:16	70:15,21 72:12
252:4 254:13	198:13 200:20	198:4,21	193:2 196:11	72:20 106:21
265:9,12	239:16 241:8	203:17 209:17	196:13 197:14	113:12 126:11
266:21 267:18	256:18 284:12	210:5,15,20	197:17,19,22	140:14 145:6
270:12 271:6	293:19 294:19	211:10,11	198:9 199:14	210:8,10
271:14,15	295:15	215:14 216:1	199:19	211:12 212:3
272:12 279:7	<b>lacking</b> 99:3	216:16,19	<b>lawless</b> 126:16	213:20 214:7
279:10,18,21	<b>lacks</b> 121:13	217:3,5 218:2	<b>laws</b> 85:15	215:20 218:2
281:2,14 282:3	291:18	224:21 226:15	198:10 226:19	230:14 232:20
286:13,20	<b>laid</b> 94:8	227:8,10 230:8	228:16 239:11	234:6 237:21
287:10,16,16	<b>language</b> 123:2	231:3,13,17	241:15 242:11	238:8,21 267:3
290:15,22	161:18 214:13	232:7 234:1	275:8,10 284:1	289:13 301:20
291:6,8,10,14	224:21 290:15	237:5,19 238:4	286:12 306:1,3	303:13 304:8
292:21 293:3	<b>large</b> 47:6 57:21	240:9 255:3,12	306:22 311:2	306:5,10,11
295:3 296:9,19	121:3 150:10	258:9,9 259:20	<b>lawyer</b> 87:21	307:3
297:3,20 299:4	187:6,12 188:4	259:22 260:22	88:1 156:12	<b>legally</b> 176:12
300:2,5	189:3,10,11	261:10 262:2	<b>lawyer's</b> 299:15	250:5,12
<b>knowing</b> 229:3	232:2 292:13	262:14,20	<b>lawyers</b> 87:6,19	268:12 299:13
<b>knowledge</b>	295:17	263:1,5,9,11	153:14	299:13 307:14
69:21	<b>largely</b> 75:18	263:21 264:8	<b>lead</b> 34:6 195:1	<b>legislation</b> 220:5
<b>known</b> 25:20	144:7	265:7,8,10,20	201:12 236:12	229:16 271:14
27:15 29:10	<b>larger</b> 49:1	265:21 266:11	238:5 262:6	284:17 306:19
89:12 123:18	138:9 144:17	266:14,19	302:20	<b>legislative</b> 12:8
133:6 254:9	277:13	267:4,14 269:5	<b>leader</b> 254:8	84:4 123:3
273:21	<b>latitude</b> 19:4	269:8,9 277:12	<b>leaders</b> 217:12	166:12,15
<b>knows</b> 87:20	<b>Laughter</b> 261:7	279:15,16	<b>leading</b> 237:4	167:12 291:21

292:6	3:9 113:15	<b>limiting</b> 197:22	<b>little</b> 19:4 20:17	<b>longer</b> 73:14
<b>legislators</b>	132:9,10 161:8	198:4 200:12	23:19,21 24:20	<b>look</b> 16:16 24:4
166:19	162:20 163:20	201:9 203:16	25:1 28:19	29:20 30:2,5
<b>legitimacy</b>	168:19 170:3	<b>limits</b> 31:9	30:7 39:18	32:14,15,17
163:14	179:13,15	79:20 169:10	41:17 45:6	33:18 49:13
<b>legitimate</b> 91:8	202:16 203:5	169:12 185:8	61:2 80:3 82:7	65:1,16 68:5
92:12 106:5	203:12 204:6	203:8 207:6	89:1 93:6	68:13,14,15
143:11 151:15	207:16,20	214:19 246:12	98:20 104:15	80:22 81:19,20
172:20 206:13	<b>libertarian</b>	255:13 289:22	105:7 147:16	83:2 92:17
206:14 217:19	222:7	291:11 306:7	149:2 159:4	93:1 111:2
227:22 228:1,5	<b>liberties</b> 1:3 3:7	<b>line</b> 56:17 79:22	171:7,13	119:12 130:20
<b>legitimately</b>	4:3 93:2	119:20 138:12	181:19 185:2	140:22 142:2
95:4 167:18	218:10 222:8	201:15 216:22	189:7 191:1	158:2 159:11
169:22 207:7	255:16	229:18 282:16	195:3 204:18	165:17 173:4
296:10	<b>liberty</b> 3:9	288:16	223:13 253:1	178:14,19
<b>length</b> 121:12	113:15 228:13	<b>lines</b> 41:20	257:2 266:17	188:10 193:21
<b>lengths</b> 52:20	242:16	57:15 58:8	291:16 293:8	194:20 198:16
<b>lengthy</b> 84:17	<b>license</b> 199:17	168:1	<b>live</b> 263:10,22	242:19 249:13
223:12	199:18,20	<b>link</b> 154:14	<b>lived</b> 99:22	256:5 257:15
<b>lesser</b> 254:8	200:3	<b>linking</b> 235:11	<b>lives</b> 220:1	258:2 271:5,8
256:19 282:3,4	<b>life</b> 297:18 302:4	<b>list</b> 81:11 208:13	<b>Livingston</b> 1:22	291:20 292:18
<b>lessons</b> 275:10	302:12	309:22	313:4,15	293:22 294:1
<b>let's</b> 29:11 32:16	<b>lift</b> 204:1 207:16	<b>listen</b> 115:17	<b>local</b> 239:4	299:10 308:4
73:9 78:11	<b>light</b> 16:2,13,21	<b>literally</b> 123:10	<b>localize</b> 228:17	<b>looked</b> 121:15
91:7 108:9	130:13 135:3	161:18,20	<b>located</b> 4:7 8:3	141:10 239:6
120:7 156:6,17	135:12 275:18	162:14	37:11 40:10,20	255:1
157:6 160:15	<b>likelihood</b> 40:2	<b>Litt</b> 2:17 8:8,10	40:22 41:6	<b>looking</b> 50:12
176:7 197:15	94:12	21:16 24:1,22	49:21 52:17,21	65:8 113:21
265:22 266:5	<b>limit</b> 17:19	34:13 35:14	73:21 114:15	161:18,20
282:21 297:11	196:12 206:22	39:12,17 48:6	176:19 231:8	200:6 202:8
297:12 305:2	213:12 238:9	48:13 49:9	231:10	242:9 266:22
310:14	246:18	53:7 63:15	<b>location</b> 60:8	292:14 304:15
<b>letter</b> 87:8,10	<b>limitation</b>	64:9 69:8	114:10	<b>looks</b> 144:16
132:21 181:13	123:20 196:14	70:11 75:7,10	<b>logical</b> 124:19	149:16 206:6
181:15,17,18	<b>limitations</b> 81:4	80:6 84:7	<b>long</b> 17:19	<b>loop</b> 192:21
273:9	126:5,19 129:2	96:22 97:22	124:17 125:2	<b>loopholes</b> 97:15
<b>letters</b> 226:7	131:18 185:22	98:2 99:8	127:6 130:13	<b>loose</b> 204:4
<b>level</b> 32:6 34:11	240:9 245:22	101:14,21	181:20 185:16	<b>loosely</b> 126:4
72:22 206:11	<b>limited</b> 63:5	102:6,20 103:1	230:5 233:10	<b>losers</b> 275:16
221:3 272:9	68:16,21 137:4	103:4 104:13	272:16 280:1	<b>losing</b> 233:9
273:6,10 278:5	184:3 191:3,13	105:11 107:8	<b>long-lasting</b>	<b>loss</b> 219:17
<b>LEVINSON-...</b>	220:8 225:7	107:15 112:11	235:12	<b>lost</b> 71:13 192:9
202:20	234:16 240:5	112:18,20	<b>long-standing</b>	273:16
<b>Levinson-Wal...</b>	257:5	<b>Litt's</b> 14:15	213:18	<b>lot</b> 36:14 43:2

44:6 68:8 75:7 75:11 76:7 94:7 99:14 105:20 143:21 184:21 195:8 213:16 222:16 226:22 252:22 277:1 279:14 279:16,18 291:14 310:3	88:6 124:20 145:17 165:8 214:6 222:6 266:15 <b>malicious</b> 108:10 <b>managed</b> 84:8 <b>Manfred</b> 252:6 <b>mangle</b> 104:15 <b>manipulates</b> 231:7 <b>mankind</b> 233:10 <b>manner</b> 223:7 224:3 <b>manufacturer's</b> 179:6 <b>March</b> 1:10 4:6 4:10 7:12 312:10 <b>Marco</b> 225:9 <b>market</b> 241:15 <b>marketplace</b> 218:18 <b>Marshall</b> 277:11 <b>Mary</b> 214:8 <b>Maryland</b> 313:5 <b>mask</b> 109:11 <b>masked</b> 106:8 106:12 107:7 107:13 <b>masking</b> 106:10 106:13,17 109:16,18 <b>mass</b> 59:13 270:10 285:7 302:8,15 <b>massive</b> 175:1 241:13 <b>match</b> 208:4 <b>matching</b> 208:6 <b>material</b> 33:19 33:19 62:6 88:9,21 <b>materials</b> 32:15	32:17 41:18 <b>matter</b> 28:15,16 72:14 78:5 118:12 174:8 176:15 194:2 215:19 226:14 254:17 262:9 266:14 298:4 300:7 306:20 <b>mattered</b> 139:8 <b>matters</b> 21:17 23:11 119:20 138:11 141:1 286:9 <b>Max</b> 3:20 209:16 <b>Mayflower</b> 1:16 4:7 <b>McLeod</b> 214:8 <b>mean</b> 24:21 38:3 41:9 44:2 48:5 49:9 50:3 51:21 61:2 67:13 68:14 74:19 76:6,13 78:4,11 85:9 85:19 87:21 91:5 96:8,9,19 102:15 104:5 107:1,12 109:13 125:18 137:17 142:22 146:7 151:13 151:15 152:11 158:12,19 161:8 168:5,8 180:16 181:7 182:10 183:10 186:10 193:4 199:21 202:1,5 202:7 207:20 224:13 227:5 227:17 229:2 246:5,5 248:12	248:16 250:20 254:4 267:6 268:15 269:12 270:17 279:2 279:17 285:14 286:11 292:12 292:17 295:13 295:18 296:4 297:8 298:10 298:22 299:5,9 305:9 306:15 <b>meaning</b> 39:9 55:19 58:2 134:20 270:1 289:11 <b>meaningful</b> 123:19 308:16 308:22 <b>meaningless</b> 270:5,7 <b>meanings</b> 39:1 <b>means</b> 20:19 25:9,11 38:19 41:9,11,14 44:2,17 51:14 52:8 53:5 55:21 73:14 78:21 102:17 103:3 104:7,8 104:9,11 105:8 105:9,12 106:22 133:12 151:19 152:1 171:3 179:1 181:15 217:7 224:16 227:15 229:1 249:1 265:10 270:4 285:2 306:18 <b>measures</b> 151:20 232:21 256:20 <b>mechanism</b> 201:11	<b>mechanisms</b> 98:7 131:3 240:7 <b>medal</b> 263:6 <b>media</b> 6:2 64:5 120:8 <b>Medine</b> 2:3 4:2 4:5,20 13:20 17:2 18:2,8,19 19:11 20:1 35:7 43:14 50:4 53:2,16 54:12 55:18 56:12 77:10,16 78:7 85:4 86:11 88:10 89:1,19 90:3 90:10,19 91:1 91:12,17,19 92:1,15,21 106:2 112:22 113:8 116:16 120:17 125:6 132:8 136:20 142:19 152:12 160:15 167:14 168:13,16 175:16 177:6 179:13 181:6 182:6 189:17 195:21 200:14 207:9,14 208:21 209:6 218:4 223:9 230:10 238:1,3 242:20 247:1 247:15 248:19 254:19 255:7 255:15 260:6 260:12 265:22 271:21 274:6 275:7 276:22 277:15 283:17 295:5 301:3
<hr/> <b>M</b> <hr/>				
<b>magistrate</b> 141:1,4 155:22 <b>magistrate's</b> 140:13 <b>magnitude</b> 93:17 <b>mail</b> 7:12 <b>main</b> 133:2 134:22 226:13 260:3 281:16 <b>mainstream</b> 291:19 <b>maintain</b> 237:4 <b>major</b> 254:22 255:1 <b>majority</b> 42:4 150:5 <b>makers</b> 65:14 103:5 269:7 <b>making</b> 5:6 8:8 20:4 22:17 34:20 43:12				

305:2 306:12 307:5,15 309:6 312:2,18 <b>meet</b> 142:16 <b>meeting</b> 180:7 198:3 <b>meets</b> 21:13 274:18 <b>member</b> 7:5 100:5,5 239:16 241:8,10,13 <b>members</b> 2:1 4:12,13 6:8 7:3 7:10 36:9 100:11 207:10 210:4 218:6 220:20 312:7 <b>memo</b> 223:21 <b>memorandum</b> 234:6 <b>mention</b> 110:6 134:5,21 202:17 277:7 <b>mentioned</b> 43:1 49:17 57:13 60:16 61:20 62:15 68:19 73:8 74:5 83:22 102:6 109:7 118:15 118:22 136:4 146:14 152:18 161:11 236:5 259:18 261:14 272:7 304:4 <b>merely</b> 122:22 124:11 134:5 288:3 307:3 <b>merit</b> 76:11 <b>message</b> 48:12 <b>messages</b> 190:19 <b>met</b> 72:11,19 104:2 116:11 215:10 278:17	<b>metadata</b> 47:22 49:17,22 66:11 66:12 157:7 190:12 227:10 <b>methods</b> 98:11 206:14 277:3 <b>metric</b> 68:3 <b>microphone</b> 266:6 <b>Microsoft</b> 191:7 <b>midway</b> 288:13 <b>Milanovic</b> 225:10 <b>military</b> 308:10 <b>millions</b> 124:1 <b>mind</b> 6:6 33:3 34:12 126:13 128:12 138:10 196:5 299:11 308:20 <b>mine</b> 261:15 <b>minimization</b> 9:9,18 12:7,21 15:16 16:13 17:3,5 18:2,4 18:10,13,20 19:13,18,20,22 21:6,12 22:8 26:20 30:17 45:3 79:5 86:8 86:17 94:17 95:13 100:17 101:4 103:3,18 104:7,8,9,10 104:14,22 105:2,4,6,18 105:22 107:9 107:18 109:5 109:21 112:12 112:16 114:13 117:14 119:11 119:14 122:3 135:19 178:21 180:4 186:1	203:14 205:8 <b>minimize</b> 9:20 88:8 104:16 131:22 <b>minimizing</b> 87:3 <b>minimum</b> 23:15 136:12 310:2 <b>Minneapolis</b> 103:15 <b>minute</b> 204:9 295:13 <b>minutes</b> 116:20 172:6 207:10 <b>mischaracteri...</b> 10:4 <b>misconception</b> 10:4 41:2 <b>misimpression</b> 76:21 <b>misleading</b> 242:3 <b>misperception</b> 56:4 282:20 <b>mission</b> 18:14 19:7 27:4 <b>missions</b> 105:1 <b>mistake</b> 100:21 <b>mistaken</b> 111:2 <b>misunderstan...</b> 36:14 <b>mix</b> 6:21 <b>mobster</b> 115:12 <b>model</b> 255:4,8 255:11 <b>moment</b> 25:21 44:9 106:18 115:5 146:15 146:19 147:3 192:3,4 242:22 267:1 <b>money</b> 84:21 85:16 <b>monitor</b> 250:7 <b>monitoring</b>	171:12 197:4 290:18 <b>monitors</b> 307:9 <b>Monroe</b> 179:7 <b>month</b> 124:17 <b>months</b> 210:16 <b>morning</b> 4:2 20:3 27:8 167:1 182:16 188:6 <b>morphing</b> 162:12 <b>motion</b> 205:3 <b>move</b> 32:18 182:10 196:4,7 310:17,20 311:4 312:14 <b>movement</b> 73:18 175:7 <b>movements</b> 125:4 174:19 <b>moves</b> 128:21 <b>moving</b> 29:8 266:18 <b>multinational</b> 284:13 301:12 <b>multiple</b> 119:7 <b>multipurpose</b> 257:9 <b>mutual</b> 238:21 <b>mutually</b> 218:12 218:13 <b>mysterious</b> 76:21 77:7 <b>MYSTIC</b> 124:15,19 190:16	<b>narrow</b> 36:17 86:19,22 102:9 152:6 186:18 279:20 <b>narrowing</b> 208:3,9 <b>narrowly</b> 228:5 <b>nation</b> 13:16 34:22 103:6 <b>national</b> 2:15,18 2:20 3:10,18 7:21 9:1 11:10 35:15,17 42:20 59:21 64:18 65:10 93:1 113:16 119:19 139:19 140:16 141:2 161:22 209:14 210:10 210:12 218:10 228:4 230:5 232:7 234:3 235:19 236:12 236:22 237:10 240:12,16 241:20 242:12 245:2 253:9,10 253:14,15 254:13 255:17 258:6 272:11 272:16 273:9 275:20 277:12 286:2 287:9 300:2,9,14 301:19 305:15 306:3 <b>nationality</b> 133:7 162:8 217:18 233:15 237:15 <b>nationally</b> 305:16 <b>nationals</b> 210:7 210:18 290:2
<b>N</b>				
<b>name</b> 57:14 106:19 108:5 108:12 179:1,6 179:6 <b>names</b> 198:8				

<b>nations</b> 284:15 289:10	308:15 311:1	109:15	<b>notion</b> 40:1 204:14 293:8	270:15 272:5 272:19 273:20 292:14 293:5				
<b>natural</b> 203:15	<b>needs</b> 9:19 16:3 18:17 23:16	<b>non-U.S</b> 8:2 9:11 14:3 15:6	<b>novel</b> 21:22 158:5 204:19	<b>numbers</b> 9:4 10:8 25:11 26:1,10,11 48:18 52:6,11 52:12 71:6 219:14 221:20				
<b>naturally</b> 41:14	31:1,10 59:14	16:11 17:1	226:11 227:3	<b>numerous</b> 100:4				
<b>nature</b> 26:19 46:15 47:12,15 47:15 49:14 65:9 94:10 105:3,5 144:9 191:13 234:20	72:20 79:9 100:10 145:8 151:18,20 262:21 276:7 279:3,4 300:3	37:11 40:9,19 40:22 41:6 43:19 49:21 52:17,21 53:12 55:11,13 58:14 60:2,4,12,13 71:16 72:4 74:1 79:20 80:11 81:15 82:13 90:13 91:10,20 92:2 92:5 96:10 103:14 109:12 110:17 111:6 129:7 148:8 176:19 177:7 177:18,20 178:2 182:22 237:11 243:21 252:12 253:16 253:19 278:2,4 278:14 280:7 295:11	244:17 269:4 269:12,13 <b>Nowak</b> 252:6 <b>NSA</b> 17:18 18:3 18:15 19:2,6 28:3 30:6 31:16 35:14 41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>Nazi</b> 225:6,8 256:9	<b>negotiated</b> 211:19	<b>noting</b> 126:7		<b>observer</b> 140:5
<b>necessarily</b> 55:7 55:15 98:19 151:18 153:1 157:18 185:21 227:4,12 228:21 271:13 271:16 274:4 286:2 287:8	<b>negotiating</b> 212:17 214:13	<b>nonsensical</b> 166:5	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>NW</b> 1:16 4:8				
<b>necessary</b> 17:14 25:5 29:16 31:22 50:1 79:3 107:21 108:5 109:3 175:11 183:17 227:22 236:16 279:22	<b>neither</b> 6:8 12:4 114:14 140:22 211:10 250:9	<b>norm</b> 216:13,17	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>O</b>				
<b>necessity</b> 28:15	<b>networks</b> 138:3	<b>normal</b> 32:22 197:19 264:2	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>O 140:20</b>				
<b>need</b> 16:6 23:6 23:20 34:20 67:4 84:9 85:2 85:3 94:14 103:5 104:19 108:4 109:21 125:19 127:17 128:17 131:13 142:16 147:2 169:9,12 170:19 171:18 173:11 185:15 185:20 193:5 217:10 239:22 254:15 300:16	<b>neutral</b> 140:5 141:4 155:22 241:3	<b>normally</b> 32:13 33:18 87:5	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>o'clock</b> 113:5 <b>Obama</b> 214:1 214:16 223:22 253:22 254:1 291:7 <b>Obama's</b> 217:14 <b>object</b> 225:1 <b>obligated</b> 293:18 <b>obligation</b> 21:2 42:12 53:22 74:11 85:13 87:14 178:5,10 179:9 215:14 224:8 227:16 229:21 248:8 250:20 271:8 271:10 289:14 290:3 <b>obligations</b> 98:22 212:4,13 213:12 216:4 218:2 223:16 227:5,20 230:14 231:20 251:16 308:8 <b>obliges</b> 178:15 <b>observations</b> 126:11 277:21				
	<b>never</b> 11:20 35:9 70:7 101:5,6,7 161:3 205:5 251:17 260:5,5 290:22 299:11	<b>norms</b> 215:20 231:12	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3	<b>observer</b> 140:5				
	<b>new</b> 32:9,20 72:9 161:16 198:16 245:19 303:2 310:13	<b>notarial</b> 313:12	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>news</b> 120:8	<b>Notary</b> 313:4,16	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>nexus</b> 147:4,6 198:13	<b>note</b> 12:13 239:13 282:8	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>NIST</b> 222:19	<b>noted</b> 8:17 238:20	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non</b> 300:15	<b>notes</b> 145:15	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non-arbitrary</b> 227:22	<b>noting</b> 126:7	41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non-citizens</b> 215:15 217:9		41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non-intelligence</b> 44:6		41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non-public</b> 9:21 231:8		41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					
	<b>non-targeted</b>		41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2 <b>NSA's</b> 45:1 79:7 122:3,7,20 123:14,20,22 124:3					

<b>observers</b> 277:17	<b>offer</b> 220:18 222:6 228:18 309:9 311:3,5	30:21 37:15 42:13 60:3 74:10 141:22 146:4	<b>opinions</b> 20:12 21:10,10 75:13 76:7,14,15,19 77:2 78:4 206:10 287:17 287:20	<b>outnumbers</b> 135:7
<b>obtain</b> 29:17 67:18 115:16 122:21 136:1	<b>offered</b> 222:3	<b>one's</b> 53:10	<b>opportunity</b> 8:11 50:6 84:14 113:20 120:20 125:8 136:18 223:11 242:17	<b>outset</b> 149:12 164:9 238:3
<b>obtained</b> 7:19 69:22 70:9,10 70:19 115:5 122:12 141:7 142:1 146:16 171:14 175:20 180:13 181:16	<b>office</b> 2:17 11:10 42:19 64:18 87:15 88:6	<b>onerous</b> 172:13 185:2	<b>oral</b> 239:8 252:9	<b>outside</b> 8:4,19 9:12,15 10:15 10:21 39:20 40:4 45:13 69:14 71:17,17 72:2 73:11 83:10,11 88:19 88:21 89:10,11 89:15,21 90:1 90:9,12,15 97:21 129:8,13 129:19 131:1 137:13 151:17 159:18 162:2 162:17 176:19 180:18 210:7 211:17 215:4 216:6 219:4 224:5,18,19 233:3 235:19 241:21 245:9 245:12 246:7 246:13,19,22 248:4,10 258:11 277:14 278:16 281:9 291:18 308:10
<b>obtaining</b> 8:5 146:20	<b>official</b> 249:7 252:5 254:14 278:5,19	<b>open</b> 200:5 206:12 220:3 220:15 259:11 260:18 284:12 311:17	<b>order</b> 4:16 6:4 31:20 34:22 53:20 67:14 70:21 81:7,12 93:17 95:17 123:6 136:14 145:2 151:16 179:9 180:20 188:12 206:5 221:1 229:16 237:3 284:22 299:21	<b>over-collection</b> 170:16
<b>obtains</b> 38:5	<b>officials</b> 6:12 85:13 159:12	<b>opened</b> 161:15	<b>orders</b> 53:18	<b>overall</b> 22:14 276:2
<b>obviously</b> 33:4 43:5 68:7 82:8 82:15 85:11 106:22 135:8 159:20 161:9 174:4 187:20 203:18 208:6 223:19 238:15 239:22 242:14 268:2 275:20 276:4,20,22	<b>oh</b> 40:2 56:12 71:12 155:7 156:1 171:9	<b>operating</b> 4:17 8:9 136:21 152:19 209:20	<b>ordinary</b> 175:2 262:22	<b>overarching</b> 53:20 72:7
<b>occasionally</b> 99:16	<b>okay</b> 23:17 29:20 39:1 47:18 50:22 51:21 53:4,21 54:12 57:16,21 60:3 62:21 65:1 78:8 79:16 82:20 85:1 92:10,21 93:19 96:5,13 97:4,9,9 142:22 154:12 156:17 157:15 160:17 177:13 179:18 186:2 187:3 193:16 201:15 202:5 204:8 247:15 250:13 251:21 281:21 295:7 308:12 309:4	<b>operate</b> 79:4 175:2 177:5 183:1	<b>organization</b> 308:15	<b>overbroad</b> 286:12 287:10 287:14
<b>occur</b> 12:11 72:5	<b>old</b> 181:12	<b>operated</b> 1:6 183:12	<b>organizations</b> 251:11 278:6	<b>overbroadness</b> 287:5
<b>occurred</b> 84:6 138:2 139:6 147:7	<b>older</b> 137:20	<b>operates</b> 20:17 183:7 200:17	<b>organize</b> 31:13	<b>overhear</b> 115:13
<b>occurring</b> 131:16	<b>once</b> 22:14 23:1 23:3,15,16 28:5 29:15	<b>operating</b> 86:7	<b>organized</b> 29:12	
<b>occurs</b> 12:14 25:6 27:22 28:1,4 39:3 42:17 146:16 155:18 170:16 242:14		<b>operation</b> 45:17	<b>original</b> 50:3 195:6	
<b>October</b> 93:12		<b>operational</b> 18:17 28:20 29:2 32:4 48:14 54:7	<b>originally</b> 183:21	
<b>off-cycle</b> 23:13		<b>operative</b> 51:2 224:7	<b>ought</b> 206:11 217:8	
<b>off-limits</b> 32:21		<b>opinio</b> 263:2	<b>outcome</b> 313:11	
		<b>opinion</b> 75:2,18 76:3 77:7 93:13 94:8 116:3 134:13 140:8 163:5 234:11 268:15 288:6 293:4	<b>outlier</b> 225:12	

160:4	<b>Paltalk</b> 191:8	<b>parcel</b> 280:17	89:12 95:13	<b>party's</b> 213:12
<b>overheard</b> 159:2	<b>panel</b> 2:9 3:1,13	<b>pardon</b> 116:19	98:21 104:22	215:1
160:13	6:16,21 7:4 8:7	<b>parliament</b>	116:8 117:4	<b>pass</b> 108:12
<b>overhears</b>	8:9 14:7 113:1	220:10 239:15	119:21 120:3,9	243:2 307:2
158:21	113:6,9 115:4	241:7,16	123:18 154:7	<b>passed</b> 12:9
<b>overlooked</b>	117:8 118:15	257:18 276:11	154:21 174:4	84:16 118:4
166:14	119:1,9 132:14	<b>parliamentary</b>	178:16 179:5	<b>passing</b> 108:6
<b>overseas</b> 15:6	132:15 135:2	257:22	197:8 220:11	229:2
52:17,22 53:12	135:16 146:14	<b>parsing</b> 38:6,11	246:1 272:17	<b>Pat's</b> 58:9
55:11,13 60:4	147:10,16	<b>part</b> 10:22 22:7	291:20 305:20	<b>Patricia</b> 2:5
60:13 73:21	161:14 166:22	22:12,17 27:9	306:2,3 308:21	4:15
89:3 91:8,15	171:8 173:20	36:6 57:21	<b>particularity</b>	<b>PATRIOT</b> 5:11
91:21 92:5,10	175:19 178:11	64:15,19 69:2	14:19 193:10	<b>pause</b> 223:8
103:9,14 126:3	182:9 187:10	77:12 107:8,9	199:2	<b>pay</b> 131:21
126:9 128:10	191:2,16	112:12 135:1	<b>particularized</b>	277:5 282:15
128:14 130:2,6	196:17 209:3,8	138:13 143:5	37:5 157:19	<b>payments</b>
130:12 131:8	260:16 279:10	145:6 150:10	193:11 200:21	153:14,14
131:15 132:1	292:12 294:5,6	161:10 192:12	<b>particularly</b>	<b>PCLOB</b> 5:8
137:5,22 138:1	294:11	203:15 205:4	86:16 100:10	66:18 136:1
147:7 183:22	<b>panelist</b> 136:22	211:11 267:10	114:4,22	218:6 221:6
184:3 206:22	207:1	270:1 273:12	132:20 219:6	284:18 301:13
272:22	<b>panelists</b> 4:22	280:16,17	221:12,19	<b>PCLOB's</b> 4:5
<b>overseeing</b>	7:5 35:10	297:9,19	226:16 254:2	<b>PCLOB.gov</b> 7:9
150:11	125:10 167:1	311:16	272:2 273:22	312:13
<b>oversees</b> 212:1	176:14 188:6	<b>parte</b> 20:18	275:19 276:8	<b>Peace</b> 305:1
292:3	191:18 208:22	21:19,21 206:8	311:14	<b>pen</b> 156:7,8,10
<b>oversight</b> 1:3	209:19 244:1	<b>participate</b>	<b>parties</b> 132:5	157:9
4:3 11:5,6 61:1	312:7	260:17	249:15 313:10	<b>penalties</b> 142:16
85:1,2,10 86:7	<b>panels</b> 6:11,19	<b>participating</b>	<b>partly</b> 36:19	<b>people</b> 15:13
98:7,22 132:2	152:14	5:1	<b>partner</b> 3:15,22	33:13 52:5
160:11 222:1	<b>paper</b> 238:7,19	<b>participation</b>	209:11,18	60:2,14 83:7
240:2,6 241:9	239:5,10,13,19	69:17	238:4	89:9 133:16
274:8,9,11	240:8 241:17	<b>particular</b> 14:19	<b>partners</b> 112:4	159:18,19
292:4,5,10,17	242:18 275:14	23:11 24:9	112:9 272:22	160:13 163:15
292:22 293:1,3	277:8 282:19	26:10,16 28:2	<b>partnership</b>	166:18 168:6
293:9,21 294:7	310:21	29:7 41:16	300:13	168:17 171:15
295:3 308:16	<b>paradigmatic...</b>	46:18 50:13	<b>parts</b> 162:13	175:2,6 195:8
309:1 310:4	161:6	51:20 54:11,20	176:11 208:14	207:6 215:2
<b>overview</b> 8:13	<b>paragraph</b>	54:20 55:16	263:15	216:6,14,17
10:3	252:8	59:2 61:10	<b>party</b> 20:20 21:1	225:4 245:20
<hr/>	<b>parallel</b> 118:2,6	63:18,20 64:16	106:18 112:4,8	246:7,22 247:9
<b>P</b>	118:13	65:17 66:4	180:21 212:7	247:10 249:2
<b>p.m</b> 312:21	<b>parameters</b>	67:16 78:19	215:4 234:14	252:4 263:2,16
<b>page</b> 96:18	109:1,22	79:16 88:3	264:19 307:4	266:13 270:11

270:15 279:19	106:7 124:6	176:5 177:3,7	176:19 178:2	227:13 234:15
280:10 291:8	<b>person</b> 9:15	177:8,10,17,18	182:22 213:2	271:2
296:19 302:8	14:3,5,6 17:8	177:21 178:6	214:19 217:16	<b>physically</b>
307:21 311:13	17:13 19:5,21	179:4,5 180:2	217:19 229:11	128:10 138:1
<b>peoples</b> 50:12	28:18 30:12,14	181:13,14	230:17 237:11	296:13
283:2	31:21 36:21	193:5 244:6	243:21 245:8	<b>pick</b> 13:22
<b>percent</b> 36:13	37:2,19 40:9	254:9 271:1	252:12 253:16	167:15 255:20
39:19 40:2,3	40:20,22 41:6	278:3,5 297:15	253:19 278:14	275:15 295:6
40:21,22 43:9	41:13,21,22	297:17 302:15	280:7,7 295:12	<b>picked</b> 133:13
93:16 168:21	43:19 48:3	<b>person's</b> 40:4	<b>perspective</b> 2:10	170:1
<b>perception</b>	51:9 52:17,21	51:12,17 55:4	15:18 43:7	<b>picture</b> 40:7
97:13 157:16	53:12,13 55:11	92:2 109:12	48:7 138:15	88:5 302:12
284:14	55:13 56:6	297:18,22	144:5 194:21	<b>piece</b> 46:18
<b>perfectly</b> 217:22	58:14 60:4,8,9	<b>personal</b> 81:8	195:1 218:11	170:9 189:19
<b>period</b> 37:1	60:13 71:16,16	81:14 217:21	<b>persuade</b> 21:3	<b>pieces</b> 41:20,22
44:18 47:9,11	71:19,20,20	228:12 242:15	<b>persuasive</b>	46:21
47:14 93:22	72:4 73:11,12	242:16 298:17	176:1,2 268:13	<b>pillaging</b> 224:19
94:20 95:21	74:1,2 78:10	298:18	<b>pertain</b> 94:5	<b>pioneers</b> 303:4
103:7	81:18,19 82:16	<b>personally</b>	<b>pertains</b> 237:16	<b>piqued</b> 148:20
<b>periodic</b> 11:13	89:4,12,14	150:22 179:3	295:18	<b>Pitter</b> 3:18
74:12 84:1	90:1,12,14,15	254:4,5	<b>pertinent</b>	209:13 213:15
214:6	90:22,22 91:9	<b>personnel</b> 86:5	108:14	223:9,10
<b>periodically</b>	91:10,14,20,20	<b>persons</b> 8:2 9:11	<b>Peter</b> 5:5	245:17 247:15
42:12 64:7	92:2,5,8,9	9:22 10:14,14	<b>phenomenon</b>	247:16 250:14
<b>periods</b> 47:7	94:12 96:8,9	12:2,11,17,19	283:14	250:17 254:21
<b>permanent</b> 8:3	96:10,10 101:3	13:2 14:9,13	<b>philosophy</b>	267:6,17 268:9
125:3 174:18	101:8,19	15:6,10 16:5	124:12	268:15 269:3
<b>permissible</b>	103:11,13,14	16:10,11,20	<b>phone</b> 25:11	270:7 271:5
14:14 54:21	106:3,19,20,21	17:1,10 37:11	26:1,10,11	277:17 278:22
56:20 90:16	107:20 108:16	39:19 40:13	51:5 52:3,3,6	279:2 280:12
98:2 285:21	108:19 109:15	43:17,20 49:21	52:11 54:8,15	281:1,5,22
300:1	111:5,6 114:8	54:16,17 60:2	54:18,20 71:5	284:20 285:19
<b>permissibly</b>	114:14,18	60:12 79:20,22	73:10,13,21	286:11,20
175:21	131:1 137:1	80:11,12,12	96:9 115:17	287:15 288:3,6
<b>permission</b>	138:11 142:7	81:6,9,15	124:16 138:2,6	291:13 292:10
262:19	148:8 149:3	82:13,14 89:16	156:11 174:17	292:21 293:20
<b>permit</b> 7:6	161:7 162:17	89:21 90:9	177:9 191:21	294:10,21
89:14 107:19	162:19 164:1	97:19 102:12	<b>phonetic</b> 140:3	298:8,13,22
122:13,20	164:21 165:15	104:19 109:17	<b>phrase</b> 26:7	299:9
231:13 260:8	165:15,18,19	109:19,22	106:19 122:16	<b>place</b> 15:16
<b>permits</b> 8:1	165:20,21,21	110:17 112:17	212:19 215:1	16:14 31:15
121:3 231:17	166:3 167:18	133:6,6 142:18	270:2,5	59:3 94:18
<b>permitted</b> 40:5	172:11,16,21	152:5 161:3	<b>phrases</b> 147:20	98:7 124:18
59:5 96:1	173:8 175:17	162:1 176:18	<b>physical</b> 225:19	152:2 160:1

166:20 169:11 171:15 179:12 201:20 214:19 218:2 220:22 221:13 227:19 233:4,15 248:15 273:18 275:3 278:2 281:13 284:11 306:17 <b>placed</b> 128:13 211:11 237:10 <b>places</b> 210:5 222:2 <b>Planck</b> 3:20 209:16 <b>plans</b> 67:21 <b>plate</b> 199:17,19 199:21 200:3 <b>play</b> 205:11 <b>please</b> 4:17 63:22 311:6 312:16 <b>pleased</b> 113:9 <b>pleasure</b> 230:13 237:20 <b>plenty</b> 280:2 <b>plot</b> 169:2,7,19 <b>plots</b> 66:22 <b>plotting</b> 168:3,4 <b>plus</b> 232:7 <b>point</b> 10:13 22:2 22:16 30:11,20 34:14 42:10 44:5 46:14 47:4 48:13 49:12,19 60:2 68:18 69:10 72:8 80:7 82:5 85:5 88:14 89:7 97:13 99:20 102:11 103:17 110:10 110:15 112:12	115:10 121:17 124:9 129:1 132:13 138:20 142:5 144:17 146:14,19,21 147:1,9 148:4 153:22 154:1,2 154:6,9 157:6 157:21,22 165:8,12 166:11 183:9 183:11 192:1 195:4,14 207:13 214:15 216:13 221:7 227:5 239:18 244:14 255:4 258:2 262:5 274:1 277:8 284:5,7 289:1 303:9 305:5 306:14 <b>pointed</b> 140:20 225:11 <b>pointing</b> 180:18 180:22 <b>points</b> 8:15 10:3 27:12 30:9 85:7 88:6 110:5 117:4 125:14 170:4 251:3 289:15 311:7 <b>Poland</b> 225:9 <b>police</b> 257:1 303:18 304:5 <b>policies</b> 220:3 239:20 282:16 <b>policy</b> 3:14 5:18 7:2 24:5 28:16 28:16 31:9 65:14 103:5 209:9 215:19 217:12,15	229:8 232:4 236:20 237:18 245:21 252:10 254:17 266:14 266:22,22 269:7 289:5 <b>political</b> 117:18 119:20 132:3 157:12,17 211:1 223:17 233:21 267:8 286:14 303:7 <b>Porter</b> 3:15 209:11 <b>portion</b> 188:2 189:10,11 <b>pose</b> 7:3 167:16 199:6 232:10 253:10 <b>posed</b> 155:4 309:11 <b>poses</b> 282:14 <b>position</b> 6:9 126:21 135:11 140:6 152:20 190:10,14 193:3,14 211:16,18 212:17 214:3 224:1 229:19 237:18 244:13 247:17 249:1 252:3,16 267:7 278:15 283:5 303:3 <b>positively</b> 178:20 <b>possessed</b> 127:22 <b>possesses</b> 127:13 <b>possession</b> 31:6 34:22 37:16 192:7 <b>possibility</b> 45:15	<b>possible</b> 5:7 32:19 45:1 46:1 81:3 88:8 166:14 257:4 312:4 <b>possibly</b> 181:19 <b>post</b> 114:21 118:17 124:13 173:5 174:10 <b>post-targeting</b> 120:14 <b>post-World</b> 225:2 <b>posted</b> 7:9 312:13 <b>pot</b> 33:16 <b>potential</b> 103:1 156:11 261:17 285:4 <b>potentially</b> 33:11 87:16 89:3 94:2,11 132:13 153:10 156:13 203:16 208:19 <b>power</b> 29:7 116:6,7 125:22 126:6 127:7 128:1,6 131:17 141:13,13,21 141:21 149:2,4 149:4,5,9,10 173:22 183:1 183:14 195:2 204:2 207:17 207:18 208:8 215:2,7 224:13 234:13 244:15 244:20 245:3 245:13 285:5 285:11 287:21 296:8,11,12 297:16 <b>powers</b> 67:21	127:1 256:15 256:22 <b>PPD</b> 110:16 <b>practicability</b> 49:11 <b>practical</b> 136:11 262:9 280:19 281:8 <b>practicality</b> 170:14 <b>practice</b> 19:11 104:6 123:1,4 123:9 128:21 150:8 214:15 238:5 <b>practices</b> 125:16 239:15,20 242:8,9 260:22 276:13,16,17 277:18 278:10 280:9 <b>pre</b> 173:5 <b>pre-FISA</b> 150:18 <b>precedent</b> 15:8 <b>precise</b> 93:15 193:19 <b>precisely</b> 150:13 285:14 288:17 <b>predate</b> 150:4,6 186:21 <b>predecessor</b> 75:17 212:2,11 <b>predecessors</b> 128:5,13 <b>predicate</b> 25:5 25:18 79:3 <b>prefer</b> 37:8 202:9 <b>preference</b> 208:9 <b>premise</b> 87:13 149:22 297:9 <b>premises</b> 231:20
--	---	--	--	--

<b>prepare</b> 312:1	222:5	172:22 187:7	88:12 118:14	18:3,5,13,20
<b>prepared</b> 63:16	<b>pretty</b> 163:21	<b>privacy</b> 1:3 4:3	<b>privileged</b> 87:17	19:13,22 21:6
<b>prerequisite</b> 116:10	<b>prevailing</b> 234:11	8:20 13:2 16:4	87:22 88:9,21	21:9,13 22:9
<b>prescriptive</b> 84:18	<b>prevent</b> 174:16	17:21 27:4	<b>pro</b> 99:2,6,12,18	22:12,20 23:7
<b>presence</b> 243:10	236:20	47:17 93:2	<b>probable</b> 116:5	26:21 27:1
<b>present</b> 4:12	<b>prevented</b> 256:10	94:2,5 114:20	118:6 124:7	30:17,17 32:3
21:21 154:22	<b>previous</b> 117:8	121:7 123:5	141:11,19	43:1 45:3,21
242:18 293:12	146:13 152:21	131:12,22	150:20 155:19	79:5,7 80:22
<b>presented</b> 234:6	171:8 178:11	185:18 190:9	156:9 157:19	86:9,17 87:12
307:11	191:16 195:16	190:13 198:12	160:8 172:10	88:15 94:17,21
<b>President</b> 3:16	206:17 238:19	210:19 211:5	172:16 173:1	95:1,14,15
5:9 47:18	<b>price</b> 131:21	215:15 216:10	173:16,17,19	98:11,12
79:17 80:21	<b>primary</b> 132:17	217:6,20 218:1	174:3,4 180:8	100:17 101:4,5
81:12 85:12,19	143:8 151:1	225:16 226:4	193:6	104:16 105:18
110:15 127:12	208:17	227:10,14	<b>probably</b> 24:2	107:10 109:6
127:13,18	<b>principle</b> 80:17	228:12 229:4	24:22 66:5	109:16,19,21
140:13,22	236:11,17	229:21 232:13	74:8 87:11,19	111:20 112:2,3
150:22 195:2	239:18 259:15	233:1 234:19	116:17 160:2	112:9,13,16
195:11,16	262:14,20	235:8,15 236:2	171:20,21	117:14 119:11
209:12 217:14	265:4 281:17	236:4,7,19	185:19 200:15	119:13 122:4,7
229:7 252:13	<b>principles</b> 109:3	238:5 239:21	208:10 252:2	122:10,20
254:1	220:19 221:9	242:15 247:20	280:2,3 286:16	123:14 124:3
<b>President's</b>	279:22 289:5,6	248:10,17	<b>problem</b> 36:20	135:20 148:17
10:22 24:4	304:22	253:8 254:12	147:8 181:3,4	174:7,12
125:22 127:1,9	<b>prior</b> 62:8 72:10	254:17 255:16	188:5 226:2	178:21 180:4,6
131:16 172:8	118:19 127:20	259:3 271:17	247:12 252:10	203:14 205:9
172:14 202:13	128:4,16	276:20,21	263:13 267:10	205:10 281:13
203:19	130:17 139:4	278:13 280:16	276:3 292:12	293:22 295:2
<b>presidential</b>	156:15 157:18	282:6,8 289:22	295:3	<b>proceed</b> 4:21,21
126:6 217:14	194:13,18	295:13,16,20	<b>problematic</b>	209:20
229:8 237:13	195:19 198:2	295:20 296:17	294:20	<b>proceeding</b> 21:1
<b>presidents</b> 127:6	201:13 204:10	296:22 297:6	<b>problems</b>	204:16 297:19
<b>presiding</b> 4:11	<b>priorities</b> 65:1,3	298:1,3,10,15	172:20	<b>proceedings</b> 4:1
<b>press</b> 86:13 88:5	65:11	299:2,12,15,17	<b>procedural</b>	21:19 204:13
<b>presumably</b>	<b>PRISM</b> 25:20	300:19 302:1,2	131:2 171:10	237:1 313:6,8
82:9 170:6	26:13,17 31:17	302:6 304:7	185:22	<b>proceeds</b> 236:8
283:7	37:10 47:8	305:15	<b>procedure</b> 90:4	<b>process</b> 11:3
<b>presume</b> 23:14	48:4 56:10	<b>private</b> 6:22	140:12 176:3	20:8 22:6,8,12
122:8	57:18 63:3,7	58:5 155:15	176:13 199:21	22:18 25:14
<b>presumption</b>	70:7,8,12	156:12,13	203:1	32:12 33:5
280:6	78:11 93:9,22	240:22 254:3	<b>procedures</b> 9:9	35:2 45:7 54:9
<b>pretend</b> 33:1	101:12 109:15	297:18 302:12	9:10,18 12:7	62:3,15 63:12
		<b>privilege</b> 86:13	15:16 16:13,21	70:16,21 72:17
		87:1,6 88:10	17:3,6,6,9,20	72:18 78:15

100:2 103:18 103:22 106:10 107:3 136:18 167:19 174:4 180:3 206:2,16 222:9 240:2,19 292:13 294:7 304:2,9 311:12	68:3,13,16,18 69:1,1,5,9,11 69:12,13 70:6 70:15 71:7 74:20 75:17 76:5 79:2 83:2 97:6 100:10 113:16 157:8 170:11 187:12 190:16,18 191:4,13 216:15 243:3 243:19 274:11 274:18 293:21	225:10 <b>prominently</b> 234:21 <b>promise</b> 265:16 265:17 <b>promote</b> 6:4 235:22 300:6,8 <b>prompt</b> 23:7 <b>prong</b> 296:3 <b>proof</b> 114:7,10 176:16 177:19 <b>proper</b> 86:6 169:10 <b>properly</b> 135:9 <b>proportion</b> 190:21 <b>proportional</b> 228:1 <b>proportionality</b> 236:11,17 259:15 <b>proportionate</b> 279:22 <b>proposed</b> 128:20 213:1 272:4 <b>proposition</b> 196:13 197:22 200:13 <b>prosecution</b> 115:10,22 117:22 139:18 141:8 145:4,21 146:1,7 201:13 205:16 <b>prosecutions</b> 144:4 181:2 <b>prosecutor</b> 156:19 <b>protect</b> 13:2 17:10,21 34:22 230:3,3 232:22 240:15 281:14 285:3	<b>protected</b> 80:12 206:15 242:16 <b>protecting</b> 8:20 103:6 228:3 <b>protection</b> 60:11 160:12 184:13 230:18 232:20 233:7 236:2 258:3 264:15 276:14,20 304:20 305:7 <b>protections</b> 80:9 80:10 82:15 110:17 174:14 185:18 186:1 221:13 243:4 273:21 275:2 278:2,5,13 282:4 300:19 <b>protective</b> 230:19 232:21 233:9 <b>protects</b> 231:4 <b>protocol</b> 191:9 <b>provide</b> 5:8 81:3 111:22 132:2 136:1 226:18 237:11,20 239:4 242:4 273:15 308:22 309:10 <b>provided</b> 26:2 54:2 65:13 88:7 160:12 308:15 <b>provider</b> 51:16 52:2 53:21 137:11 238:14 <b>providers</b> 7:16 25:16 26:8 69:18,19 238:12 239:2 <b>provides</b> 81:8 211:3 272:21	<b>providing</b> 52:1 103:5 <b>provision</b> 88:15 89:21 90:8 106:15 136:2 215:13 217:3 <b>provisions</b> 69:4 112:3 <b>provocative</b> 82:22 <b>PRTT</b> 157:6 <b>pry</b> 297:5 <b>public</b> 1:5,15 5:9,17 7:10 57:22 70:14 75:3 77:12,14 77:21 78:3,6 79:8 83:16 84:2,9 87:10 87:10 93:7,10 94:8 95:2,15 106:9 112:7 113:3 135:6 154:17 221:17 227:1 228:13 231:12 243:18 258:9 279:12 293:16 294:16 311:16 312:8 312:12 313:4 313:16 <b>publicly</b> 32:2 93:11 112:3 <b>publish</b> 239:12 297:18 <b>published</b> 238:6 <b>pull</b> 192:14 280:9 <b>pulses</b> 303:17 <b>purely</b> 122:5,11 149:7 184:4,8 194:7 <b>purge</b> 45:2,6,7 45:18,18 82:1
---	---	---	---	---

101:19 102:14 102:19 <b>purged</b> 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5 <b>purging</b> 44:1,17 45:16 58:9 72:18 202:1 <b>purports</b> 229:9 <b>purpose</b> 5:17 10:10 59:16 61:1,8 89:12 90:21 92:5 111:8,10 133:9 134:10 143:4,4 143:7,8,8,15 145:20 146:1,7 146:9,10 148:7 148:10,15,20 149:8 151:1 159:10,15,15 179:22,22 180:14 181:1,9 181:9 184:8 186:13,15 190:4 193:20 204:3 208:17 208:18 212:22 225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5 <b>purposes</b> 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3	148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10 <b>pursuant</b> 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6 <b>pursue</b> 33:15 45:5 61:9 66:14 149:19 <b>push</b> 149:1 293:7 <b>pushing</b> 301:1,2 <b>put</b> 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22 <b>puts</b> 38:5 <b>putting</b> 73:19 188:20 278:1 <b>puzzled</b> 169:17	79:9 86:9 193:4 199:20 <b>querying</b> 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2 <b>question</b> 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10	228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11 <b>questioned</b> 241:12 <b>questioning</b> 35:8 93:20 163:14 209:21 220:10 <b>questions</b> 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13	<b>quick</b> 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16 <b>quickly</b> 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19 <b>quirk</b> 89:8 <b>quite</b> 30:3 99:5 154:4 159:14 203:22 221:14 222:14 <b>quorum</b> 4:13 <b>quote</b> 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8 <b>quoting</b> 140:2 148:12 160:21
<hr/> <b>Q</b> <hr/>				
225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5 <b>purposes</b> 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3	148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10 <b>pursuant</b> 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6 <b>pursue</b> 33:15 45:5 61:9 66:14 149:19 <b>push</b> 149:1 293:7 <b>pushing</b> 301:1,2 <b>put</b> 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22 <b>puts</b> 38:5 <b>putting</b> 73:19 188:20 278:1 <b>puzzled</b> 169:17	79:9 86:9 193:4 199:20 <b>querying</b> 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2 <b>question</b> 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10	228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11 <b>questioned</b> 241:12 <b>questioning</b> 35:8 93:20 163:14 209:21 220:10 <b>questions</b> 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13	<b>quick</b> 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16 <b>quickly</b> 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19 <b>quirk</b> 89:8 <b>quite</b> 30:3 99:5 154:4 159:14 203:22 221:14 222:14 <b>quorum</b> 4:13 <b>quote</b> 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8 <b>quoting</b> 140:2 148:12 160:21
<hr/> <b>R</b> <hr/>				
101:19 102:14 102:19 <b>purged</b> 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5 <b>purging</b> 44:1,17 45:16 58:9 72:18 202:1 <b>purports</b> 229:9 <b>purpose</b> 5:17 10:10 59:16 61:1,8 89:12 90:21 92:5 111:8,10 133:9 134:10 143:4,4 143:7,8,8,15 145:20 146:1,7 146:9,10 148:7 148:10,15,20 149:8 151:1 159:10,15,15 179:22,22 180:14 181:1,9 181:9 184:8 186:13,15 190:4 193:20 204:3 208:17 208:18 212:22 225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5 <b>purposes</b> 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3	148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10 <b>pursuant</b> 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6 <b>pursue</b> 33:15 45:5 61:9 66:14 149:19 <b>push</b> 149:1 293:7 <b>pushing</b> 301:1,2 <b>put</b> 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22 <b>puts</b> 38:5 <b>putting</b> 73:19 188:20 278:1 <b>puzzled</b> 169:17	79:9 86:9 193:4 199:20 <b>querying</b> 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2 <b>question</b> 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10	228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11 <b>questioned</b> 241:12 <b>questioning</b> 35:8 93:20 163:14 209:21 220:10 <b>questions</b> 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13	<b>quick</b> 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16 <b>quickly</b> 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19 <b>quirk</b> 89:8 <b>quite</b> 30:3 99:5 154:4 159:14 203:22 221:14 222:14 <b>quorum</b> 4:13 <b>quote</b> 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8 <b>quoting</b> 140:2 148:12 160:21
101:19 102:14 102:19 <b>purged</b> 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5 <b>purging</b> 44:1,17 45:16 58:9 72:18 202:1 <b>purports</b> 229:9 <b>purpose</b> 5:17 10:10 59:16 61:1,8 89:12 90:21 92:5 111:8,10 133:9 134:10 143:4,4 143:7,8,8,15 145:20 146:1,7 146:9,10 148:7 148:10,15,20 149:8 151:1 159:10,15,15 179:22,22 180:14 181:1,9 181:9 184:8 186:13,15 190:4 193:20 204:3 208:17 208:18 212:22 225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5 <b>purposes</b> 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3	148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10 <b>pursuant</b> 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6 <b>pursue</b> 33:15 45:5 61:9 66:14 149:19 <b>push</b> 149:1 293:7 <b>pushing</b> 301:1,2 <b>put</b> 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22 <b>puts</b> 38:5 <b>putting</b> 73:19 188:20 278:1 <b>puzzled</b> 169:17	79:9 86:9 193:4 199:20 <b>querying</b> 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2 <b>question</b> 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10	228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11 <b>questioned</b> 241:12 <b>questioning</b> 35:8 93:20 163:14 209:21 220:10 <b>questions</b> 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13	<b>quick</b> 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16 <b>quickly</b> 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19 <b>quirk</b> 89:8 <b>quite</b> 30:3 99:5 154:4 159:14 203:22 221:14 222:14 <b>quorum</b> 4:13 <b>quote</b> 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8 <b>quoting</b> 140:2 148:12 160:21
101:19 102:14 102:19 <b>purged</b> 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5 <b>purging</b> 44:1,17 45:16 58:9 72:18 202:1 <b>purports</b> 229:9 <b>purpose</b> 5:17 10:10 59:16 61:1,8 89:12 90:21 92:5 111:8,10 133:9 134:10 143:4,4 143:7,8,8,15 145:20 146:1,7 146:9,10 148:7 148:10,15,20 149:8 151:1 159:10,15,15 179:22,22 180:14 181:1,9 181:9 184:8 186:13,15 190:4 193:20 204:3 208:17 208:18 212:22 225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5 <b>purposes</b> 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3	148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10 <b>pursuant</b> 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6 <b>pursue</b> 33:15 45:5 61:9 66:14 149:19 <b>push</b> 149:1 293:7 <b>pushing</b> 301:1,2 <b>put</b> 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22 <b>puts</b> 38:5 <b>putting</b> 73:19 188:20 278:1 <b>puzzled</b> 169:17	79:9 86:9 193:4 199:20 <b>querying</b> 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2 <b>question</b> 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10	228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11 <b>questioned</b> 241:12 <b>questioning</b> 35:8 93:20 163:14 209:21 220:10 <b>questions</b> 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13	<b>quick</b> 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16 <b>quickly</b> 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19 <b>quirk</b> 89:8 <b>quite</b> 30:3 99:5 154:4 159:14 203:22 221:14 222:14 <b>quorum</b> 4:13 <b>quote</b> 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8 <b>quoting</b> 140:2 148:12 160:21
101:19 102:14 102:19 <b>purged</b> 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5 <b>purging</b> 44:1,17 45:16 58:9 72:18 202:1 <b>purports</b> 229:9 <b>purpose</b> 5:17 10:10 59:16 61:1,8 89:12 90:21 9				

<b>raising</b> 136:9 165:20 278:4	105:15 144:19 219:12 278:13 282:14,22,22	48:18 121:6 140:7,17 151:20 173:7 185:15 190:8 190:12 227:9 236:20	267:9,13 268:18 292:15 309:15	179:6
<b>Raj</b> 24:22 28:1 35:13 36:19 43:7 60:5 61:19 102:6 108:22	<b>reality</b> 33:8 <b>realize</b> 36:1 116:20 <b>realized</b> 101:7 <b>really</b> 27:8 28:10 36:10 45:17 52:5,6 60:5,7,11 62:2 63:21 67:13 68:1,2,10 69:10 91:8 158:3 161:3 169:2 175:18 177:18 182:4 185:17 191:17 194:15,16 196:3 206:21 214:14 224:20 228:13 242:22 261:5 265:9 275:14 277:6 278:21 284:7 289:3 296:3,9 299:22 300:22 305:13	<b>reasonableness</b> 16:19 121:14 130:9,10 137:7 143:11,13 <b>reasonably</b> 9:11 31:18 37:11 39:20 40:10,20 41:6 58:14 71:17 79:10,12 89:9,13 131:1 136:6 148:11 162:1 <b>reasoning</b> 249:17 <b>reasons</b> 30:16 106:5 121:22 129:5 134:18 172:13 211:9 280:19 <b>reassessed</b> 240:1 <b>reauthorization</b> 100:1 <b>rebuild</b> 222:12 <b>recall</b> 48:17 <b>received</b> 70:17 70:20 86:6 <b>receives</b> 38:14 <b>receiving</b> 4:20 312:18 <b>recipient</b> 70:16 <b>recipients</b> 235:13 <b>recite</b> 102:8 <b>recited</b> 282:3 <b>recognize</b> 226:3 227:9 230:4 233:3,13 236:9 236:17 248:22	<b>recognized</b> 66:18 151:9 154:13 210:20 229:8 241:7 299:18,19 <b>recognizes</b> 95:7 291:8 310:22 <b>recognizing</b> 47:14 88:20 <b>recommend</b> 68:11 221:22 272:13 278:1 283:16 <b>recommendat...</b> 172:15 203:21 <b>recommendat...</b> 35:4 274:7,21 277:22 280:3 284:17 301:14 <b>recommended</b> 173:2 274:6 <b>reconsider</b> 76:12 <b>record</b> 78:4,6 84:2 99:4 113:7 125:3 174:18 209:5 311:16 313:8 <b>recorded</b> 7:8 313:7 <b>recording</b> 124:15 174:17 235:9 <b>records</b> 153:13 205:17 <b>redacted</b> 75:18 76:16 <b>reevaluate</b> 84:1 <b>refer</b> 38:9 54:7 115:21 234:5 <b>reference</b> 6:5	<b>referred</b> 26:5 134:13 178:11 187:4 <b>referring</b> 41:5 187:4,5 207:18 208:10 <b>refers</b> 26:6 67:2 102:2 103:18 161:3 <b>reflect</b> 99:4 <b>reflected</b> 132:17 133:3 241:17 <b>reflects</b> 137:17 <b>reforming</b> 206:18 <b>refrain</b> 230:1 <b>regain</b> 237:4 <b>regard</b> 79:7 80:5 114:3,9 116:4 147:11 154:22 155:18 176:17 177:2 205:11 243:3 251:1 272:3 274:14,18 <b>regarding</b> 1:5 15:2 114:7,10 250:19 271:15 292:22 293:2 <b>regardless</b> 217:18 233:14 237:15 <b>regards</b> 271:17 <b>regime</b> 62:20 <b>regimes</b> 238:8 263:9 264:4 <b>regional</b> 238:17 239:2 242:4 <b>regions</b> 71:3 <b>register</b> 4:10 156:7,8,10 157:9 <b>regular</b> 20:18
<b>rate</b> 43:9 <b>ratified</b> 211:2 304:5 <b>rationale</b> 54:13 59:19 69:2 150:7,9 <b>re-articulated</b> 211:20 <b>reach</b> 94:20 275:15 <b>reached</b> 272:18 276:3 <b>reaching</b> 226:8 <b>reaction</b> 256:8 <b>read</b> 71:1 92:16 151:7 182:17 188:1 285:1 <b>reader</b> 200:3 <b>readers</b> 199:18 199:19 <b>ready</b> 13:18 113:8 284:3 <b>reaffirm</b> 74:11 275:4 <b>reaffirmance</b> 249:18 <b>reaffirmed</b> 214:15 244:12 248:22 <b>real</b> 51:18 73:2 85:8 90:21	<b>realm</b> 37:14 88:19 <b>reason</b> 10:9 27:1 44:19 47:6,10 51:9 59:1,7,9 60:15 80:15 88:16 94:1 143:14 171:22 178:3 183:11 237:12 256:10 258:17 296:4 302:5 <b>reasonable</b> 15:17 16:9,12 16:21 17:3,22 18:16 40:18	<b>reasonableness</b> 16:19 121:14 130:9,10 137:7 143:11,13 <b>reasonably</b> 9:11 31:18 37:11 39:20 40:10,20 41:6 58:14 71:17 79:10,12 89:9,13 131:1 136:6 148:11 162:1 <b>reasoning</b> 249:17 <b>reasons</b> 30:16 106:5 121:22 129:5 134:18 172:13 211:9 280:19 <b>reassessed</b> 240:1 <b>reauthorization</b> 100:1 <b>rebuild</b> 222:12 <b>recall</b> 48:17 <b>received</b> 70:17 70:20 86:6 <b>receives</b> 38:14 <b>receiving</b> 4:20 312:18 <b>recipient</b> 70:16 <b>recipients</b> 235:13 <b>recite</b> 102:8 <b>recited</b> 282:3 <b>recognize</b> 226:3 227:9 230:4 233:3,13 236:9 236:17 248:22	<b>referred</b> 26:5 134:13 178:11 187:4 <b>referring</b> 41:5 187:4,5 207:18 208:10 <b>refers</b> 26:6 67:2 102:2 103:18 161:3 <b>reflect</b> 99:4 <b>reflected</b> 132:17 133:3 241:17 <b>reflects</b> 137:17 <b>reforming</b> 206:18 <b>refrain</b> 230:1 <b>regain</b> 237:4 <b>regard</b> 79:7 80:5 114:3,9 116:4 147:11 154:22 155:18 176:17 177:2 205:11 243:3 251:1 272:3 274:14,18 <b>regarding</b> 1:5 15:2 114:7,10 250:19 271:15 292:22 293:2 <b>regardless</b> 217:18 233:14 237:15 <b>regards</b> 271:17 <b>regime</b> 62:20 <b>regimes</b> 238:8 263:9 264:4 <b>regional</b> 238:17 239:2 242:4 <b>regions</b> 71:3 <b>register</b> 4:10 156:7,8,10 157:9 <b>regular</b> 20:18	

21:1,14 29:5 61:13 294:8 <b>regulate</b> 126:15 165:11 <b>regulated</b> 133:14,17 <b>regulations.gov</b> 7:11 <b>rein</b> 199:3 <b>reined</b> 279:11 <b>reinforcing</b> 218:13 <b>Reingold</b> 5:4 <b>reining</b> 287:4 <b>reinserted</b> 36:20 <b>reiterate</b> 244:12 <b>reject</b> 166:6 259:12 <b>rejoining</b> 209:7 <b>relate</b> 242:9 288:3 <b>related</b> 51:16 179:5 239:21 <b>relates</b> 221:16 222:1 285:2,12 <b>relating</b> 5:19 102:12 147:14 152:5 <b>relation</b> 249:2 <b>Relations</b> 231:22 <b>relatively</b> 75:19 276:17 <b>released</b> 11:16 147:18 191:6 220:19 223:21 <b>relevance</b> 169:22 <b>relevant</b> 10:9 42:7 46:13 65:7 108:8 143:17 146:10 158:16,16 165:8 200:11	235:5 242:14 <b>reliable</b> 256:2 <b>relied</b> 130:6 307:18 308:1 <b>relying</b> 24:8 160:3 196:6,18 <b>remain</b> 6:7 13:11 85:3 262:18 304:13 311:17 <b>remaining</b> 16:8 280:21 <b>remains</b> 230:8 <b>remarks</b> 63:16 113:18,22 114:1 116:21 125:11 152:19 230:22 266:16 272:8 <b>remediate</b> 218:20 <b>remember</b> 100:4 125:19 204:10 249:6 284:3,5 <b>remind</b> 125:9,13 <b>reminder</b> 301:7 <b>remote</b> 154:16 <b>remotely</b> 226:10 227:15 <b>removed</b> 44:17 <b>Renaissance</b> 1:15 <b>render</b> 15:17 <b>renewed</b> 238:18 <b>repeat</b> 10:11 298:8 <b>repeated</b> 10:5 <b>repeatedly</b> 126:7 <b>repeating</b> 40:12 74:9 235:14 <b>report</b> 5:9,12 6:15 152:22	174:10 211:21 214:6 221:7 239:14 272:12 276:12 282:3 307:11 <b>reported</b> 1:22 72:14,15 73:17 124:13 <b>reporter</b> 116:17 <b>reporting</b> 11:11 65:2 222:17 294:8 <b>reports</b> 6:2 11:14 62:11,13 65:3,13 72:15 84:19 86:13 <b>representatives</b> 7:1 <b>request</b> 212:20 241:5 311:11 <b>requested</b> 306:13 <b>requests</b> 221:18 272:15 <b>require</b> 10:17 45:21 109:14 122:10 131:5,7 140:12 146:21 149:5 185:22 240:12 263:1 306:19 <b>required</b> 12:7 22:19 28:11 44:16 45:2 47:19,19 49:3 84:11 103:7 126:20 130:1,5 139:20 178:19 184:15 242:13 <b>requirement</b> 15:20 16:1,19 28:20 48:2 58:13,18 80:14 109:20 121:9	129:18 130:11 134:4,10 137:6 142:6 143:6 148:13 150:2 150:16 151:7 151:13 152:8 154:2,11 162:7 162:7 184:16 185:15 204:3 205:15 208:2 212:12 243:13 243:14 281:6,8 <b>requirements</b> 11:22 16:17 44:21 140:15 142:17 151:5 178:19 253:5 274:19 294:1,8 <b>requires</b> 22:7 52:16 84:19 126:19 131:20 148:7 224:21 240:5 <b>requiring</b> 35:1 <b>research</b> 241:18 275:14 <b>Researcher</b> 3:18 209:14 <b>reside</b> 217:19 <b>residence</b> 133:8 233:15 <b>resident</b> 8:3 <b>resides</b> 237:17 <b>resolution</b> 236:6 241:6,12,17 247:19 276:11 <b>resolved</b> 276:7 <b>resources</b> 64:20 <b>respect</b> 16:19 19:4 37:21 61:19 65:20 67:16 81:1,1 84:19 86:4 94:3 98:12,22	105:18,21 111:5 144:19 145:7 190:14 194:9 211:14 212:8 213:21 215:14 217:17 224:9 226:4 229:4,21 232:4 234:8 243:13 248:3,6,9,17 250:9 251:12 258:7 259:9 268:22 271:11 271:18 285:11 285:16 287:20 289:21 298:15 298:16 303:10 <b>respected</b> 185:16 <b>respectful</b> 217:11 <b>respecting</b> 247:20 <b>respective</b> 237:13 <b>respond</b> 132:13 142:20 149:16 305:3 <b>responded</b> 140:18 307:12 <b>responding</b> 225:5 <b>response</b> 8:16 64:3,4 83:14 99:5 102:16 111:15 154:12 238:11 284:8 <b>responses</b> 7:6 187:14 <b>responsibilities</b> 244:9 <b>responsibility</b> 6:13 291:1 <b>rest</b> 76:10
--	---	--	---	--

<b>restore</b> 208:14	<b>reunification</b>	<b>reviews</b> 18:14	304:10 305:22	282:8
<b>restraint</b> 187:17	263:14	22:4 62:9	306:5 307:17	<b>road</b> 300:1
<b>restricting</b>	<b>reveal</b> 153:14	68:22 310:5	311:4	<b>roamer</b> 73:7
194:16 242:12	155:13 156:11	<b>revised</b> 95:1	<b>rightly</b> 185:20	<b>roamings</b> 72:1
<b>restriction</b>	<b>revealed</b> 240:8	<b>revising</b> 206:19	<b>rights</b> 3:19 8:20	<b>robbery</b> 186:15
133:8,12,15	<b>revealing</b> 13:11	<b>revisit</b> 42:12	10:15 15:7,14	<b>Robert</b> 2:17
162:9 194:4	<b>revelations</b>	<b>rewind</b> 124:16	180:19 207:4	<b>robust</b> 6:4 84:3
195:15	226:21 238:16	<b>right</b> 18:7 32:10	209:15 210:17	184:13 185:5
<b>restrictions</b>	247:18 269:6	38:8 39:14,17	210:22 211:1	202:17,20
133:3,18	272:1 276:6	53:13 55:1,3	211:22 212:8	309:17,19
187:16 194:17	286:21	57:9,10 58:21	213:9,16,16,19	<b>robustly</b> 8:20
210:6 211:12	<b>reverse</b> 40:15	61:17 73:5	214:7,22 215:5	<b>role</b> 106:1 115:1
253:18	89:2,10 90:4,6	75:3 81:16,17	215:15,19	127:9 205:11
<b>restricts</b> 111:5	90:10 91:1,3,6	91:12,22 96:11	217:8 223:17	237:4
<b>result</b> 31:22	91:17 92:11	100:18 101:2	224:10 225:4	<b>rolls</b> 99:5
33:10 70:13	97:19 123:14	101:13 102:15	226:12,17	<b>Romania</b> 109:14
218:18 228:14	<b>review</b> 9:8 11:7	110:2 112:18	227:6,20	<b>room</b> 154:20
<b>resulting</b> 231:18	15:13 22:12	112:22 114:20	229:21 231:1	219:2,4 280:2
<b>results</b> 134:2	23:13 31:1,5,7	117:3 137:20	232:14 233:3	287:4
163:12 236:13	31:11 61:19	138:3 142:13	233:14,17,20	<b>Roosevelt</b>
263:10	68:19 72:7	143:4,20 144:6	233:22 234:1	212:21 247:12
<b>resume</b> 113:5	74:2,4,5 78:14	146:17 149:3	234:19 235:8	<b>Rosetta</b> 76:2
209:3	81:20 83:21	157:8 161:9	235:10,15,22	<b>rough</b> 93:14
<b>retain</b> 122:14	103:19 116:3	163:1,22 164:7	236:2,19 237:5	<b>round</b> 50:6 93:4
<b>retained</b> 17:20	124:17 135:1	170:1 180:1	237:9 244:22	93:20 97:10
44:4 81:10	141:6,14	181:9 183:5	246:16,17	100:14 142:21
93:21 119:1	156:16,20	184:15 189:19	248:1,3,9	175:14 283:22
120:5 135:21	157:19 172:8	192:16 194:5	249:21 250:4,6	288:10,10
146:4	172:14 192:14	196:16 203:12	250:18,21,22	290:10 306:13
<b>retains</b> 152:7	200:20 201:12	206:21 207:20	251:4,8,10	<b>rounds</b> 7:4
195:2	202:21,22	210:19 217:6	252:11 253:8	<b>route</b> 228:22
<b>retention</b> 9:20	203:1,9,20	225:16 226:4	256:8 258:3	<b>routed</b> 144:13
17:7,17,19	205:8,9 228:8	227:14 229:4	259:1,2,3,4	<b>rubber</b> 299:22
47:6,9,11,14	242:14 294:16	236:7 246:6	262:4 267:9	<b>rule</b> 40:21 41:1
79:21 81:4	312:12	247:20 248:17	268:9 271:10	96:2 100:19
94:19 95:21	<b>reviewed</b> 42:17	249:19 251:3	271:12,16,19	101:10,13,16
103:21 104:17	42:18 43:2,7	254:11 263:3	286:14 290:5	109:18 231:16
116:12 117:6	47:5 59:20	266:5 268:2,13	290:11,13,18	237:5
117:21 118:21	61:11 76:18,19	270:21 280:15	307:8 308:5,8	<b>ruled</b> 139:19
120:15 201:2	77:2 78:15	280:16 281:2	<b>ripe</b> 237:8	<b>rules</b> 5:20 12:21
229:9 253:19	116:22 117:1	282:1 283:19	<b>rise</b> 184:22	17:17 54:1
<b>return</b> 31:18	294:12	287:6 289:22	<b>risk</b> 95:19	56:15 81:14
79:10 113:12	<b>reviewing</b> 75:12	297:4,22 299:2	253:15 282:14	101:5 102:11
153:21 171:10	76:14 101:17	299:4,17,17	<b>risks</b> 258:15	104:22 105:2,4

105:6 107:18 112:20 229:9 259:12 309:14 <b>rulings</b> 205:19 290:17 <b>Rumanian</b> 109:15 <b>run</b> 225:8 <b>runs</b> 35:3 <b>rushing</b> 228:16 228:17 <b>Russia</b> 304:1	91:11 111:4 156:1 161:2,20 165:2 212:7 224:8 230:7 247:4 258:9 285:10 290:16 305:11 <b>scale</b> 121:3 160:9 187:6,12 188:4 189:3 232:2 270:10 <b>scan</b> 147:20 148:1 189:21 <b>scanned</b> 192:13 <b>scanning</b> 189:1 192:16 197:8 <b>scans</b> 189:11 <b>scenario</b> 247:2 <b>schedule</b> 311:20 <b>scheme</b> 145:2 165:14 183:16 <b>Schmoe</b> 287:21 <b>scholar</b> 225:10 <b>scholarly</b> 118:12 <b>scholars</b> 210:17 <b>school</b> 3:5 113:11 302:14 <b>scientific</b> 240:16 <b>scope</b> 9:6 173:21 203:8 212:7 232:14 236:1 244:8 <b>score</b> 42:1 <b>screed</b> 221:5 <b>scrutinizes</b> 11:18 <b>sea</b> 158:2,9 <b>seal</b> 313:12 <b>search</b> 21:20 27:19,22 28:3 28:7,11 37:3 37:17 38:2,7 38:18,19 39:1 39:3,4,9,13,15	43:18 48:4 115:6 124:4 130:1,2,6 140:7 146:16 146:21 147:6 148:3 171:17 172:10 190:4 193:4 197:20 201:2 206:7 <b>searched</b> 115:11 198:11 <b>searches</b> 36:22 37:18 50:9 79:6 115:3 123:16,16 130:12 175:18 177:14 179:18 180:11 184:5,8 184:13 185:9 185:11 194:13 <b>searching</b> 38:20 78:10 137:22 174:14 175:17 <b>second</b> 6:16 10:13 26:4 29:19 39:9 48:13 58:22 74:18 106:18 110:14 112:4,8 113:5,9 114:7 114:21 122:17 126:4 129:1,16 130:4 133:9 134:21 145:17 188:21 203:13 222:1 250:13 251:21 273:12 278:8 305:5 <b>secondary</b> 37:16 <b>Secondly</b> 31:14 232:16 256:21 310:10 <b>seconds</b> 124:8 280:21	<b>secrecy</b> 84:9 <b>secret</b> 77:7 135:9 292:11 293:6 <b>secretly</b> 240:19 <b>section</b> 1:7 2:10 5:10,15 7:17 8:12,14,17,21 10:3,5,11,20 11:8,18,22 12:5,9,21 13:8 13:10 25:4,8 37:9 48:20 56:8 65:6,14 66:9 92:18 100:1 111:4 112:15 117:13 118:11 119:11 121:1 123:13 123:21 124:10 124:11 125:16 125:19 126:12 126:18 128:4 128:12 129:4 130:18,21 131:6,11 132:22 133:3 135:4,6 141:17 151:4,7,8 157:7,8 158:22 170:7,7 202:10 202:12 203:14 207:22 219:3,4 239:6 240:4 258:8 273:8 292:20 <b>sections</b> 177:4 208:5,7 <b>sector</b> 6:22 <b>secure</b> 238:17 <b>security</b> 2:15,20 3:10,18 35:18 93:1 113:16 119:20 139:19	139:20 140:16 141:2 142:7 198:6,7 209:14 210:11,12 218:10 219:10 228:4 230:6 232:18,21 236:18,20 240:12,17 241:20 242:5 242:12 253:11 253:14,15 254:14 255:17 272:11,16 273:9 275:20 277:12 286:2 287:9 300:2,9 300:15 <b>see</b> 27:6 35:5 36:15 45:10 48:5 54:4 56:13,14 62:21 65:12 74:2 87:2 118:1 154:22 155:7,9 162:4,5 172:9 173:5 178:5 198:5 201:6 204:15 252:10 256:6 266:5 271:20 277:2 291:21 295:1 303:20 <b>seeing</b> 220:2,9 <b>seek</b> 28:16 140:7 241:3 <b>seeking</b> 20:10 <b>seen</b> 93:6 236:5 254:5 279:13 <b>segregated</b> 34:4 95:19 <b>segue</b> 145:12 <b>seize</b> 12:18 <b>seized</b> 198:10
<b>S</b>				
s 252:7 <b>sabotage</b> 285:5 <b>sacrifice</b> 228:12 <b>safe</b> 220:11 300:11 <b>safeguards</b> 160:1 237:14 275:22 284:11 <b>safer</b> 228:10 238:13 283:9 <b>safety</b> 228:11 <b>Sara</b> 252:6 <b>satisfied</b> 212:14 <b>satisfy</b> 173:2 <b>save</b> 175:13 <b>saw</b> 253:3 293:2 <b>saying</b> 25:9 32:10 37:2 53:4 56:18 64:10 70:6 76:7 145:14 148:22 164:8 167:22 171:22 176:7 191:3 197:10 199:11 217:4,7,10 262:19 265:16 265:17 286:6 287:22 294:17 <b>says</b> 53:21 89:8				

<b>seizure</b> 190:3 197:20	<b>send</b> 198:8 200:9	<b>set</b> 8:14 18:20 34:16 71:12 84:8 95:14 113:17 119:10 192:20 222:11 250:6 260:16 288:20 309:14	<b>showed</b> 277:11	<b>simply</b> 100:2 111:21 119:4 217:2 220:8 225:21 234:5
<b>selected</b> 155:2	<b>sender</b> 229:3	<b>sets</b> 72:17 220:18	<b>showing</b> 198:21	<b>single</b> 61:16 74:2 246:4 253:9
<b>selection</b> 26:13 147:19	<b>Senior</b> 3:18 209:14	<b>setting</b> 60:22 93:10 113:3 266:22 295:12	<b>showings</b> 149:6	<b>sitting</b> 277:21
<b>selective</b> 50:2	<b>sense</b> 18:19 20:18 38:4 46:2 197:3 224:20 253:2 254:16 270:8 281:22 289:13 291:15 299:12 310:1	<b>severe</b> 136:13	<b>shown</b> 275:8	<b>situated</b> 229:6
<b>selector</b> 10:9 24:21 28:2 50:13,18 51:2 51:4,13,14,22 51:22 52:4 53:7,8,10 54:6 54:11 55:8,11 55:17 56:1 59:2 61:15 71:8 78:10 80:15 100:21 173:7 294:19	<b>sensible</b> 131:11	<b>severely</b> 115:1	<b>shows</b> 73:12	<b>situation</b> 24:14 75:22 115:19 138:6 142:10 156:4 168:5 199:6,6 226:5 228:15 310:12
<b>selector-based</b> 25:9 26:9	<b>sent</b> 181:15	<b>sexual</b> 302:3	<b>side</b> 20:20 21:2 29:9 121:19 138:12 188:21 243:17 257:10	<b>Sieber</b> 3:20 209:15 215:10 230:10,11,12 254:21 255:5 255:14,18,21 260:8 261:14 262:18 266:3 301:16
<b>selectors</b> 9:4 10:7 23:20 25:11 26:1,12 26:13 36:21 37:3 47:21 56:10 57:12,17 63:8 71:5 123:17 135:15 161:15 163:3 189:6 295:2	<b>separate</b> 58:17 61:14 63:10 89:20 111:19 119:10 152:22 163:1 193:7	<b>shadows</b> 154:20	<b>SIGAD</b> 191:5,5	<b>signals</b> 81:2 195:12 217:15
<b>self-defense</b> 262:21	<b>separated</b> 257:16	<b>shaking</b> 101:19	<b>significance</b> 137:15 143:15 185:12	<b>signals</b> 81:2 195:12 217:15
<b>self-executing</b> 236:21 306:15	<b>separating</b> 221:10	<b>sham</b> 145:1	<b>significant</b> 21:21 69:13 134:7,10 138:18 170:16 170:17 208:18 219:1,16,17 272:2 273:3	<b>significantly</b> 178:22
<b>self-interest</b> 277:1	<b>separation</b> 256:22,22 257:3,11	<b>shape</b> 66:20	<b>shared</b> 112:8 136:5 291:3 310:19	<b>silence</b> 194:2,21
<b>self-restrain</b> 286:7	<b>sequitur</b> 300:15	<b>share</b> 5:2 112:21 136:14 176:22 218:19 221:17 273:7,13,14 293:18	<b>sharing</b> 112:4 239:1 242:1 276:8 283:11	<b>silent</b> 176:21 177:1 193:18 193:21 276:18
<b>semiannual</b> 62:12 72:15	<b>series</b> 64:1 200:18	<b>sharon</b> 5:4	<b>sharply</b> 112:4 239:1 242:1 276:8 283:11	<b>silos</b> 220:5,14
<b>senate</b> 251:6,18 251:20 264:19 290:21,22 291:4	<b>serious</b> 232:10 232:13 257:5,6 289:7	<b>shed</b> 135:3,12	<b>sharon</b> 5:4	<b>similar</b> 18:18 48:2 239:11 257:20
	<b>seriousness</b> 75:10	<b>sheer</b> 65:9	<b>sheds</b> 135:3,12	<b>similarities</b> 238:7
	<b>serve</b> 204:17,17	<b>sheet</b> 61:7,7,14 63:9 86:11	<b>sheer</b> 65:9	<b>Similarly</b> 223:5
	<b>served</b> 210:8 252:15	<b>shift</b> 50:8,20 63:9 86:11	<b>sheet</b> 61:7,7,14 63:9 86:11	<b>Simone</b> 5:6
	<b>servers</b> 231:10 303:16	<b>short</b> 113:4 172:3 173:1	<b>short</b> 113:4 172:3 173:1	
	<b>service</b> 7:15 25:15 26:8 69:18,18 168:3 238:12 239:2	<b>shorter</b> 93:21 94:19 95:21	<b>shorter</b> 93:21 94:19 95:21	
		<b>shorthand</b> 25:21 26:5 41:5	<b>shorthand</b> 25:21 26:5 41:5	
		<b>show</b> 164:19	<b>show</b> 164:19	

276:6	143:5 144:13	144:14 163:12	<b>spy</b> 265:16	149:22 155:5
<b>so-called</b> 123:15	144:15 148:20	<b>speaks</b> 273:19	<b>spying</b> 215:17	198:5
173:6 210:19	162:4,6 163:12	<b>special</b> 16:3	264:20 265:8	<b>state</b> 129:10
242:4	166:10,12	32:9 234:18	<b>square</b> 191:10	181:3 210:9
<b>social</b> 299:21	170:4 181:9	257:17	<b>stab</b> 50:22	212:7 215:4
<b>societal</b> 219:18	185:5,17,22	<b>specific</b> 8:5	244:10	224:16 231:6,9
<b>societies</b> 237:6	193:5 194:6,14	13:10 14:22	<b>staff</b> 5:4 312:3	232:20,22
<b>society</b> 157:13	199:3 202:22	25:22 47:12	<b>staffs</b> 99:13	233:2 234:7,14
175:2 299:20	203:9 205:15	61:4 66:14,15	<b>stage</b> 8:14 37:1	252:16 261:20
<b>soil</b> 142:8	207:21 243:12	71:5 81:8	87:20 118:18	264:9 313:5
<b>solely</b> 69:12	244:7,17	88:15 122:9	146:11	<b>state's</b> 225:22
174:13	264:10 281:14	137:1 141:15	<b>stages</b> 103:22	227:13 230:19
<b>Solicitor</b> 167:6	296:1 299:12	191:16 216:17	146:11 188:22	241:13 248:2
<b>solution</b> 181:4	299:13	231:1 235:21	<b>stake</b> 27:5	262:3
233:16 237:3,9	<b>sorts</b> 81:13	252:17 253:4	240:17	<b>stated</b> 146:3
<b>solutions</b> 172:3	171:9	278:9 294:16	<b>stakes</b> 124:21	187:11
218:19 220:18	<b>sounds</b> 299:11	294:19	<b>stance</b> 224:15	<b>statement</b> 8:9
221:5 222:3,11	<b>source</b> 65:4	<b>specifically</b>	<b>stand</b> 264:4	13:21 140:19
<b>solve</b> 247:13	198:15 250:18	24:16 80:4	<b>standard</b> 72:12	152:22 209:20
<b>somebody</b> 80:7	<b>sources</b> 13:14	100:17 107:12	72:20 79:9	213:8 222:22
114:8 161:6	206:14 230:16	117:13 229:13	86:8 105:17	223:12 264:14
167:22 171:5	268:10	239:5 266:9	137:7 180:13	271:22 304:10
177:3 302:4,12	<b>sovereign</b> 231:4	291:22	180:14 199:21	308:14 309:1
<b>someone's</b> 12:18	262:3 264:15	<b>specificity</b>	204:1 206:19	<b>statements</b> 70:5
226:6,8	264:22 304:18	194:22	206:19 207:17	71:2 93:7
<b>somewhat</b> 89:7	<b>sovereignty</b>	<b>specifics</b> 88:18	208:4 280:6	136:21 153:13
89:8 274:17	231:7,14,18	95:11	281:15 305:21	159:11 213:19
279:11 309:16	261:21 262:1	<b>spectrum</b>	306:6,10,11	216:22 222:14
<b>soon</b> 239:12	265:5 305:8	153:19	<b>standards</b> 18:11	250:7 251:11
<b>Sooner</b> 306:3	<b>space</b> 154:17	<b>speech</b> 277:10	21:14 25:17	<b>states</b> 8:4,19
<b>sorry</b> 40:11	298:17,18	<b>spend</b> 85:16,16	31:15 136:12	9:12,15 10:15
48:11 57:9	<b>Spain</b> 239:11	215:17	222:18,20	10:21 29:8
93:3 116:19	<b>spatial</b> 234:18	<b>spending</b> 84:21	223:3 278:17	39:21 40:4
141:12 155:3	<b>speak</b> 44:11	113:1	<b>standing</b> 185:21	67:9,11 71:18
191:14 192:9	72:22 78:18	<b>spent</b> 36:1 98:6	<b>standpoint</b>	71:20 72:3
202:19 250:15	88:3 106:16	<b>sphere</b> 184:19	228:20	73:11 86:20
269:15	126:4 138:12	<b>spirit</b> 132:21	<b>start</b> 13:22 51:2	89:5,10,11,13
<b>sort</b> 11:3 24:8	149:18 251:9	<b>split</b> 243:12	54:11 64:9,10	89:15,17,22
24:10,10 32:21	261:11 264:7	263:4	113:18 144:4,6	90:2,13,15
34:10 54:10	<b>speakers</b> 6:5,9	<b>spoke</b> 147:10	209:22 223:17	91:10 97:17,21
64:11 72:7	312:3	203:20 308:15	230:21 243:6	97:21 103:10
76:1 80:17	<b>speaking</b> 15:1	<b>sponsored</b>	<b>started</b> 98:19	104:18 114:19
84:22 133:20	39:5 63:15	247:19	289:1	115:13 128:3
138:7 139:9	107:17 115:12	<b>spot</b> 33:21 62:7	<b>starting</b> 118:1	129:9,13,20,22

130:14,22	13:1 22:10,18	<b>stay</b> 259:14	193:20	153:12 156:18
131:2 133:7	23:16 40:8,13	<b>steal</b> 197:15	<b>structure</b>	<b>subsequent</b>
137:10,12,13	43:5 52:16	<b>stems</b> 224:6	132:22 133:22	27:18 77:1
138:7 140:14	54:22 55:10,12	<b>stenographica...</b>	134:20 164:13	191:22 193:3
147:6 151:17	59:6 60:11	313:7	309:17 310:5	193:11 201:13
159:18,19	84:11 89:8	<b>step</b> 25:2 44:8	<b>structures</b>	213:7
162:2,18	91:11 96:1	58:22 273:3	309:16	<b>subsequently</b>
176:20 180:19	97:14 109:2	<b>steps</b> 103:18	<b>structuring</b>	27:16 28:6
182:3 210:7	121:2,8,13,19	222:17,19	309:12	44:2,3 196:14
211:15,18	121:21 122:1	223:1,5 256:9	<b>struggle</b> 304:1	198:1 199:20
212:5,5,15,16	122:17 123:2	272:5 273:4	<b>struggling</b>	<b>subset</b> 56:9
212:18 213:4	133:1 134:1,4	274:3 275:1	157:20 288:17	82:16
213:20 214:9	134:11,20	<b>stolen</b> 197:18	<b>studies</b> 64:22	<b>substantial</b>
215:8 216:5,6	148:12 151:8	<b>Stone</b> 76:2	<b>study</b> 110:18	99:13 241:19
216:8 217:7,15	155:1 159:10	<b>stop</b> 66:22	<b>stuff</b> 200:20	<b>substantive</b> 78:9
224:8 229:6	159:13,14,15	227:18 304:8	<b>sub-questions</b>	78:12,17 79:1
230:17 231:5	160:14,22	<b>storage</b> 238:12	44:7	236:1 243:2
231:14 232:2,6	161:2,10,19	238:14 239:4	<b>subject</b> 6:15	<b>substituting</b>
232:18 235:17	162:13 163:22	282:13	11:4 19:13,17	106:18
239:16,20	164:9,19 166:9	<b>stored</b> 228:19	19:19,22 25:17	<b>subterfuge</b> 9:16
241:8,10	166:20 167:5,8	<b>stories</b> 64:1,12	86:12 133:16	<b>succeed</b> 205:5
243:20 245:6,9	167:13 176:21	<b>storing</b> 235:12	212:10 213:3	<b>success</b> 64:1,11
245:12,14	177:1,2 187:18	<b>straightforward</b>	214:20 215:1,6	<b>successful</b> 263:7
246:3,11 248:5	187:22 188:1	239:19	224:10 243:14	<b>succinct</b> 309:4
248:10,12	194:19 195:5	<b>strategic</b> 301:7	244:18 247:11	<b>Sue</b> 5:4
250:2,8 251:13	195:15 200:22	310:7	292:4,5 296:5	<b>sufficient</b> 41:1
251:15 253:11	202:15 203:8	<b>stream</b> 190:3	296:6	42:2,4 160:1
254:7 261:19	203:15 247:4	192:14	<b>subjected</b> 18:10	173:11 174:3
264:16 267:9	270:3 293:10	<b>strength</b> 42:6	211:4	177:13 179:7
268:17 269:14	293:16	<b>strict</b> 129:3	<b>subjects</b> 36:17	198:13 272:21
270:8 274:4	<b>statute's</b> 123:3	225:13 269:16	<b>submission</b>	<b>suggest</b> 41:12
276:5 277:14	<b>statutes</b> 121:16	<b>stricter</b> 257:8	132:18 159:5	45:11 72:10
279:9 281:9	232:8 287:5	<b>strictly</b> 224:15	161:11 246:15	77:9 83:15
285:3,13,22	<b>statutory</b> 6:18	<b>strikes</b> 178:13	<b>submit</b> 312:7,8	148:14 195:1
287:11,18	25:17 54:6,13	178:14 187:12	<b>submitted</b> 7:11	215:20 216:14
288:1,2,4	58:17 69:4	<b>strong</b> 135:19	8:22 19:15	274:21
290:8 291:6,16	90:7 104:14	174:8 256:6,22	22:10,20 117:2	<b>suggested</b> 28:14
292:8 294:17	114:2 127:18	257:11	211:21 312:11	68:9 162:21
297:13 305:8	130:16 148:13	<b>strongest</b> 160:22	<b>submitting</b>	252:14 275:1
306:8 307:3,12	161:17 164:13	161:17	116:21 117:4	278:21
309:18,18	164:13 165:13	<b>strongly</b> 185:10	182:16 312:10	<b>suggesting</b> 34:3
<b>status</b> 41:13	170:22 176:15	206:18	<b>subpart</b> 109:9	137:5 148:18
262:3	183:13,16	<b>struck</b> 288:15	161:21	167:3 199:9
<b>statute</b> 12:6	187:16 310:5	<b>structural</b>	<b>subpoena</b>	215:6,22

<b>suggestion</b> 135:18,19 244:18 275:1	185:20 187:6 189:14,15 199:22 207:14	206:6,10 210:6 210:18 211:7 214:19 215:7	197:4 235:17 277:19	92:17,17 109:10 113:4
<b>suggests</b> 41:21 41:22 166:16 245:18	216:14 222:6 222:20 245:16 248:13 270:1	215:11 216:20 221:4 225:15 225:21 226:19	<b>survive</b> 125:2 <b>survived</b> 187:1 <b>suspect</b> 49:1 156:1 302:4	119:12 124:18 151:20 156:6 156:17 157:6 166:20 168:5
<b>sui</b> 207:22	301:22 311:17	227:11,18,19	<b>suspected</b> 151:16 198:14	171:4 174:11 187:10 190:14
<b>sum</b> 237:2	<b>surprised</b> 119:8 246:9	227:21 230:15 231:15 232:3	<b>suspicion</b> 48:19 199:2 302:9	193:3 196:3 197:15 209:2
<b>summary</b> 54:3	<b>surveil</b> 123:10 123:11 151:16	232:16 233:12 235:1 238:13	<b>suspicionless</b> 281:14	217:16,22 223:1 224:1
<b>sunset</b> 69:3 100:12	172:22	238:17 239:6 239:17,21	<b>swath</b> 192:6	225:13 227:19
<b>supervised</b> 83:9	<b>surveillance</b> 1:6 1:8 2:11 3:3	240:2,4,5,7,13 240:15 241:7	<b>switch</b> 189:8 303:16	232:17 244:10 289:17 291:3
<b>supervision</b> 7:16	6:14 7:18 11:13,17 29:11	242:3,6,8,12 244:19 245:2,5	<b>synthesizes</b> 239:9	296:12 306:17 311:19
<b>supplanted</b> 184:21	43:3 44:22 45:4 49:2	246:7,11,18 252:12,19	<b>system</b> 33:9 42:14 80:10	<b>taken</b> 22:1 145:14 190:10
<b>supply</b> 295:22	116:2 121:4,10 121:15 123:9	253:3,7,20 255:3,8 257:17	119:18 124:14 125:2 130:17	211:16 222:18 247:17 249:9
<b>support</b> 123:2 218:14 238:16	124:14 125:16 126:2,6,9	261:21 262:7,8 264:10,17	184:22,22 185:4,5 233:5	252:3 270:8 273:5 274:3,4
<b>supported</b> 233:17	127:15,19 128:1,7,9	265:7,19 268:22 269:3	233:10 256:3,5 309:12,19	273:5 274:3,4 <b>takes</b> 156:4
<b>suppose</b> 49:4 109:13	129:12,18,20 131:15 133:14	270:6,9,16 271:1 272:1,15	310:1	224:15 269:1
<b>supposed</b> 285:15	133:17 139:1 139:16 140:17	274:12 275:12 277:1,4 278:3	<b>systemically</b> 292:7	<b>talk</b> 8:12 20:14 24:2 25:1,3
<b>Supreme</b> 15:8 129:9 167:6 249:10	141:5,16 150:11,21	279:4 280:1,8 283:9,10,11	<b>systems</b> 44:18 45:2 72:21	28:19 29:1 39:18,21 89:1
<b>sure</b> 15:4 24:1 24:22 28:22	151:2 158:8,8 158:10,11,17	289:21 290:1 291:11,17	154:17 231:8 232:21 241:8	98:20 120:12 174:9 182:20
33:6 36:7,8 40:6,22 44:8	160:7,9 161:1 164:10,11,14	293:15 295:11 296:14 300:2,9	258:18 259:8	191:15,15 213:15 223:15
52:20 56:17 58:20 74:13	165:2,5,6,9,11 166:8,11,13,17	300:15,21 301:12 302:8		265:10
85:13 92:7 94:7,20 96:18	166:19,21 167:3 169:1,11	304:13 306:7 307:18 308:2	<b>T</b>	<b>talked</b> 23:17,20 27:13,14 61:2
100:13 105:11 111:14 113:19	170:13 171:11 181:22 182:21	308:17 310:7	<b>table</b> 44:13 105:20	105:21 137:3 168:18 204:11
127:5 149:1 153:21 154:5	183:14 188:8 188:14,18	<b>surveilled</b> 269:20	<b>tail-end</b> 44:12 <b>tailored</b> 30:17	260:20 261:18 278:7 310:3
168:10,21 169:14,17	195:17 196:22 196:22 197:2	<b>surveilling</b> 151:14 175:7	47:12 88:18 228:6	278:7 310:3 <b>talking</b> 30:12
178:5 181:8 182:1,4,19			<b>take</b> 15:4 41:10 42:6 50:22 53:9 77:6	31:17 36:11,16 38:2 52:19 58:7 68:2 72:1

72:2 76:1	43:19 48:8	176:18	52:5 54:6,6,7	230:19 231:11
81:21 86:2	52:12 60:7	<b>task</b> 53:2,4,7,8	54:10 55:10	232:17 233:3
90:11 98:6	124:5 149:9	<b>tasked</b> 95:4	70:13,14 82:7	234:18 235:16
99:21 103:20	167:18,18	<b>tasking</b> 50:17	95:4 96:15	235:19 246:7
112:14,19	169:22 229:14	53:2,3,19 54:9	97:3,5,8 99:17	246:22 247:3,5
137:9 146:12	253:4 279:5,21	61:7,21 100:20	106:21 159:7	247:10 248:2,4
168:1 189:16	<b>targeting</b> 9:9,10	188:16,17	230:5	248:5 270:3,5
205:22 216:16	10:20 13:12	189:4,5	<b>terms</b> 19:5,9	285:11 296:5
249:20 270:16	15:6 16:11,13	<b>taskings</b> 53:22	21:22 33:21	303:14,15
284:1 287:16	17:1,6 21:13	<b>technical</b> 34:2,6	38:3 50:15,19	<b>terrorism</b> 13:14
287:19 292:19	22:9 24:9	45:1 46:2 89:7	50:20 58:3	34:17 172:18
<b>talks</b> 161:19	37:10 40:9,16	119:3,3 227:15	66:18 69:17	285:6
270:3	42:15,22 49:20	<b>technically</b>	71:15 83:3	<b>terrorist</b> 51:10
<b>target</b> 8:2,6 9:4	51:5,22 52:8	137:9 144:14	102:1 106:1	53:12 57:13
9:10,14,16	54:21 55:3,4	<b>technological</b>	110:13 117:9	103:9 151:17
10:17 12:3	55:10,11,12,14	204:19 228:20	118:18 147:19	169:2,7 297:14
14:3 29:7	55:21 59:18	<b>technologies</b>	196:10 202:21	<b>terrorists</b> 51:6
40:13,14,19	81:18 89:2,14	219:7,11	208:20 228:12	60:19
50:17 51:1,14	89:21 90:4,6,8	<b>technology</b> 3:17	244:3,8 264:9	<b>test</b> 42:5,5 156:3
52:14,17,20	90:10,21,22	137:18 182:2	272:13 275:11	243:1,2
54:5,14 55:15	91:1,2,3,4,6,7	209:13 227:9	295:4	<b>testify</b> 218:8
55:19 58:14	92:11 97:20	270:9	<b>terrible</b> 167:16	<b>testimony</b>
61:10 71:2	101:2 103:14	<b>telecommunic...</b>	<b>territorial</b>	121:13 218:16
80:15 82:9,10	114:3,14,22	235:7,9 282:9	138:17 139:3	222:3 239:9
89:2,9,11,12	117:14 119:13	<b>telephone</b> 9:4	139:10 143:16	252:9 279:11
90:1,12,21	120:14 122:4	10:8 14:5	224:15 231:5,6	282:2 294:5
91:8,16,17	123:14 130:22	47:22 48:18	232:1,5 243:10	<b>tests</b> 178:12
92:1,6,8,13	133:17 147:11	190:11,15,19	243:15 264:15	<b>text</b> 161:7
97:1,18 116:6	161:2,7 162:1	190:19	264:22 265:5	164:13,17
116:9 131:8	162:6,14 163:7	<b>telephony</b> 66:11	278:16 295:12	167:12
133:5,20	177:6,7 200:21	<b>tell</b> 60:21 65:21	305:8	<b>textual</b> 160:22
137:12 141:12	203:11 204:5,6	80:3 93:9	<b>territoriality</b>	164:5 176:22
141:12,15,19	205:9,11	107:11 260:4	258:8 303:11	194:7
147:12,13,14	206:19 281:11	<b>telling</b> 168:2	303:19 304:14	<b>thank</b> 4:22 5:3
150:21 154:8	294:1,12,16	<b>tells</b> 293:10,17	304:18,20	8:10,10 13:20
154:22 155:2	310:7	<b>temporarily</b>	<b>territorially</b>	27:7 35:5,19
161:12,15	<b>targets</b> 8:18	47:21 229:13	271:11 297:11	43:15 113:1,6
163:22 164:20	12:4,12,18,20	<b>tendency</b> 266:10	<b>territories</b>	113:19 116:15
165:15 166:2	37:14 60:15	<b>tends</b> 154:19	220:12	117:1 120:17
166:21 167:4	114:6,6 120:3	<b>tens</b> 134:15	<b>territory</b> 129:8	125:5,6,7
201:11 206:22	122:8,20,22	163:5 219:14	212:9,16,19	132:8,10
207:7 281:16	123:7 134:6	<b>term</b> 38:18,19	213:3,13	136:18,20
<b>targeted</b> 10:7	135:14 151:15	39:6,7,12	214:11 215:5	145:11 152:13
24:16 25:8	163:2 167:9	50:13 51:3	224:9,17,19	167:14 172:6

182:6,7,15	136:11 161:10	98:18 99:5	187:4,15 188:4	208:14
208:22 209:4	182:14 200:18	102:17,18	189:19 190:6	<b>thinks</b> 288:1
210:3 218:3,4	202:17 244:11	103:20 106:9	192:13 193:18	<b>third</b> 11:4 66:17
218:5,5,8,9	245:15,20	107:2,3,18	194:5,7,14,17	72:17 114:9
223:9,10,11	253:22 257:13	108:20 110:5	195:1,18 196:7	116:12 117:6
230:10,12	258:1 259:16	110:15 111:3,4	196:16,20	140:8 203:22
237:22 238:1,2	265:14 266:8	112:11 118:16	197:16 198:18	209:3,8 288:10
242:17,20	279:7 287:8	119:12 120:9	200:5 202:9,14	296:3
248:19 252:20	289:9 296:20	125:10,15	203:6,13 205:7	<b>thirdly</b> 31:14
260:6,14 266:7	302:21 303:1	131:20 132:7	205:18,21	<b>thirty</b> 124:8
266:15 273:1	306:4 307:10	134:18,22	206:1,3 207:5	<b>thirty-five</b> 150:9
291:13 295:6	<b>think</b> 13:18	135:1,16 136:9	208:8,12 210:8	187:1
311:9,21,22	15:19 19:1,7	137:14,17	210:16 221:9	<b>thought</b> 58:1
312:20	19:14 20:1	138:9,13,20	222:10 223:7	72:2,4 110:2
<b>thanks</b> 20:2	23:14,21 24:1	139:5,10 143:1	244:20,22	146:7 170:20
35:20,20	25:4 28:9,14	143:3,17 144:3	245:7,9 246:3	183:15,17,21
120:19,20	31:4 32:7,8,8	144:17 145:19	247:13 248:16	188:20,21
125:7 160:18	33:8 34:1,2,5	148:19 151:11	248:21,21	252:22 275:17
160:18 209:6	35:22 36:12,13	152:21 156:3	249:10,19	310:16
247:15 288:21	36:15,17 39:5	157:13 158:1,4	253:14,21	<b>thoughts</b> 272:9
307:15 312:2	40:6 43:15	158:9,19 159:6	254:13 260:3	298:7 310:10
<b>theoretical</b> 48:7	46:15,22 47:19	161:8,15,17	260:17,22	311:3,5
<b>theoretically</b>	48:6,10,11,14	162:5,21,22	261:3,12 262:6	<b>thousand</b> 43:11
247:9	49:9,10,13,15	163:9,21 164:8	262:9 263:21	74:6
<b>theories</b> 38:13	56:4 57:3,21	164:8,10,12,19	264:12 266:3	<b>thousands</b>
<b>theory</b> 39:19	58:6 60:2 61:7	165:7,12 166:4	266:19 267:3	134:15 163:5,5
195:17 206:1	61:18,19 62:17	166:7 167:10	269:7 274:15	<b>threat</b> 32:16
<b>thing</b> 38:17 65:8	63:19 64:3	168:19 169:12	274:17 276:18	108:8 232:10
71:1 77:17	65:21 66:21	170:3,5,12,13	279:2,15 280:1	253:11 300:11
138:10 145:2	67:3,5,10,13	170:19,20,21	280:12 282:18	<b>threats</b> 13:15
167:16 168:4	67:15,19 68:1	172:13,19	283:6,19 285:9	60:19 103:6
179:16 182:5	68:2,5,8,10,18	173:10,11,18	285:19 286:15	236:9,10
201:16 206:2	69:2 72:22	173:21 174:2,7	287:3,7 288:13	282:10 283:1
208:12 226:9	73:20 74:1,5	174:8 176:4	288:22 289:5	<b>three</b> 6:11 11:5
253:19 305:12	75:4 76:6,13	177:1 178:2,3	291:15 292:11	63:21 121:22
<b>things</b> 25:11	76:21 77:5,8,9	179:15,19	294:4 296:10	139:22 202:17
26:1,11 34:7	77:11 80:6,21	180:11,16	298:2 299:18	220:18 243:7
34:11 36:16	82:5 83:8,15	181:4,8 182:1	300:6,8 301:13	<b>threshold</b> 104:2
38:9 45:10	83:17 84:2,5	182:2,12,12,13	305:5,11	116:10 198:3
52:7 57:14	85:9 87:10,13	183:5 184:1,3	307:20 309:13	<b>throwing</b> 173:3
59:11 63:10	87:18,19 88:5	184:10,11	310:22 311:10	<b>time</b> 12:14 20:1
71:5 85:18,22	91:6,16 93:2	185:6,10,11,13	311:15	20:4 27:6,8,22
95:18 104:7	93:11 94:9	185:19 186:4,7	<b>thinking</b> 162:14	28:3 29:19
105:8,12 135:8	96:14 97:5,12	186:11,17	203:13 208:2	30:2,5 35:6

36:6,10 40:3 50:4,5 51:18 56:13 62:22 65:12 67:5 72:9 75:1 82:2 82:20,21 85:16 85:17 87:15 92:17 93:22 100:14,15 113:2 125:12 175:13 195:13 212:2,12,21 215:17 237:8 247:13 266:18 271:20 278:13 283:17 286:19 295:6 300:8 306:12 311:20 312:1,19 <b>timekeeper</b> 269:16 <b>timely</b> 67:19 <b>times</b> 14:4 48:21 284:21 307:18 <b>tiny</b> 44:11 <b>tip</b> 118:7 <b>tipping</b> 157:6 <b>title</b> 12:16 29:4 29:10 111:3 116:4 121:16 141:10 155:21 171:17 179:2 194:3 197:18 206:7 <b>today</b> 5:15,20 6:11 98:10 99:21 113:2,20 121:18 124:9 124:21,22 125:8 196:17 200:17 209:1 218:8 220:6 236:15 239:9 239:18 243:17	260:17,20 261:16 264:4 266:7 273:19 292:12 312:5 <b>today's</b> 5:1 7:13 109:18 312:12 <b>told</b> 214:8 <b>tool</b> 65:22 66:4,7 66:13,22 67:1 <b>tools</b> 13:9 66:1,2 <b>top</b> 87:12 95:12 101:15 185:18 189:19 <b>topic</b> 37:13 50:8 63:10 232:4 312:8 <b>topics</b> 79:5 <b>torture</b> 225:20 270:14 <b>tortured</b> 270:18 <b>torturing</b> 270:20 <b>total</b> 144:22 234:17 <b>totality</b> 41:7 42:5 178:12 <b>totally</b> 9:13 104:5 196:5 <b>touch</b> 6:1 245:2 <b>trace</b> 156:8,8,10 157:10 <b>traces</b> 118:9 <b>track</b> 71:13,21 72:9 81:5 192:10 <b>trade</b> 300:13 <b>tradition</b> 125:21 128:21 130:14 130:17 185:16 <b>traditional</b> 14:16,17 153:8 153:12 155:6,8 156:10 158:2 206:7	<b>traditionally</b> 84:6 <b>trail</b> 118:6 <b>training</b> 34:6 41:18 62:4 86:6 <b>transatlantic</b> 300:12 <b>transcript</b> 7:9 312:12 313:8 <b>transfer</b> 229:1 <b>transfers</b> 241:3 <b>transformed</b> 219:22 <b>transiting</b> 138:7 <b>transmission</b> 235:10 <b>transmissions</b> 235:13 <b>transnational</b> 3:14 7:1 209:9 232:16,19 233:12 235:21 236:19 <b>transparency</b> 221:6,8,21 239:16 241:19 272:8,9,13 273:16,20 276:1 277:8 279:14,16 284:13 291:18 292:16 293:19 294:20,21 301:2 <b>transparent</b> 98:16 293:9 <b>trap</b> 156:7,8,10 157:9 <b>travel</b> 119:19 228:22 <b>treat</b> 280:7 <b>treated</b> 34:4 95:16 217:17	<b>treaties</b> 238:22 249:5 251:4,17 251:17 290:15 <b>treatment</b> 79:19 253:18 <b>treaty</b> 210:22 211:19 212:13 212:18 214:18 224:5,21,22 225:3,7,14 227:6 243:9 245:19 246:1 247:4 249:13 249:15 250:11 250:21 251:12 251:18 267:17 267:18,20 268:2,3,4,7,16 271:4 286:17 286:19 289:10 290:3,11 291:2 291:5 299:6 306:14 <b>tried</b> 205:1 223:22 <b>trigger</b> 15:12 <b>true</b> 135:22 181:12 187:11 213:14 289:16 313:8 <b>trust</b> 219:6,7 222:12 228:13 232:11 237:6 292:9 <b>try</b> 32:15,17 64:19,22 253:16 <b>trying</b> 52:9 60:9 61:9 69:16 88:14 90:1 108:15 144:18 146:8 164:1 165:13 172:1 186:11 191:17	199:6 247:12 267:1 286:8 <b>turn</b> 8:7 30:9 32:5 58:10 77:16 233:18 242:21 <b>turning</b> 230:22 <b>turns</b> 41:17 73:22,22 189:14 <b>twice</b> 69:5 <b>two</b> 5:9 6:19 25:7 30:13 39:1 41:22 42:1 47:14 53:1 54:16,17 65:16 73:6 82:8 94:22 101:11 110:5 125:13 126:10 127:4 129:5 132:17 133:2 146:2 162:6 168:6,17 171:19 175:18 176:2,11 178:13 180:17 182:14 187:14 188:22 201:5 218:12,16 225:3 230:16 230:18 232:3 243:1 248:20 249:16,16 263:9,15 271:5 277:16 278:4 282:17 289:15 <b>type</b> 10:19 25:19 25:21 26:4,15 32:22 33:17,20 57:7 58:19 59:5 66:7 105:18 132:3 157:10 178:12
---	---	--	---	--

183:17 260:18 288:7 <b>types</b> 25:3,7,14 25:16 27:2 29:3 30:13,18 33:11,19 34:10 66:8 73:6 139:11 <b>typical</b> 21:17 55:2 <b>typically</b> 39:13 51:4	92:2,9 94:12 96:8,10 97:19 101:3,8,18 102:12 103:11 103:13 106:3 106:19,20,21 107:1,19 108:16,19 109:17,19,22 111:5 112:17 114:8,14,18 125:15 126:8,9 127:6 128:9 129:19 130:1 130:17 131:8 133:5 138:2 139:21,21 142:7,8,8,8,17 143:20 149:3 152:5 172:11 172:21 175:17 176:5,18 177:3 177:7,9 178:6 180:2 183:12 183:22 184:2 193:4 194:12 194:17 201:1,2 211:2,18 212:20 213:18 214:14,20 219:7 223:15 224:2,5,14 225:12,13 226:6 227:3,7 227:8 228:4,19 229:5,11,18 230:1,5,15 232:11 233:6 234:7 236:18 237:1,4,13 238:14 240:1 241:2,21 242:8 242:10 244:12 244:19 245:3	248:13 250:20 251:10,16 256:3,11 260:21,22 265:19 267:12 267:15 268:2,6 268:7 272:4,15 278:3,14,16 279:17 280:7 282:9,16 283:1 283:15 284:14 295:11,21 297:12 300:6 304:1,5 310:18 <b>U.S.A</b> 219:8 236:22 <b>ubiquitous</b> 220:4 <b>Ukraine</b> 236:15 <b>Ulrich</b> 3:20 209:15 <b>ultimate</b> 49:4,8 <b>ultimately</b> 72:15 185:13 245:6 <b>unable</b> 98:8 <b>unanimous</b> 4:20 312:18 <b>unanswered</b> 135:10 <b>unavoidable</b> 96:17 <b>unclassified</b> 5:21 60:22 75:18 <b>unclear</b> 181:17 <b>unconsenting</b> 104:18 <b>unconstitutio...</b> 121:1,9 153:6 153:10,17 <b>unconstitutio...</b> 169:6 <b>unconstrained</b> 129:14	<b>uncontroversi...</b> 127:9 <b>uncovered</b> 201:12 <b>under-empha...</b> 125:14 <b>underlying</b> 49:14 <b>undermine</b> 134:10 222:18 223:2,3 <b>undermined</b> 150:8 <b>undermines</b> 163:9 230:5 <b>underscores</b> 247:19 <b>understand</b> 8:8 17:15 18:3 20:14 25:5 31:10 32:1 33:1 50:16 52:6 58:6 67:14 68:3 79:18 80:7 82:17 86:17 107:21 108:7 109:3 119:9 124:11 143:2 145:13 146:12 148:21 157:20 158:12 168:21 182:19 184:1 191:17 194:9 194:11 242:22 262:16 286:8 296:1 <b>understanding</b> 50:11 98:5 106:1 108:8 125:15 164:2 179:17 184:21 194:1 197:1 213:11 244:3	264:19 291:4 311:1 <b>understands</b> 56:18 <b>understood</b> 111:14,16 125:20 131:11 261:19 <b>undertake</b> 290:17,19 <b>undertakes</b> 69:6 <b>underwear</b> 34:18 <b>undisputed</b> 127:15 304:19 <b>undoubtedly</b> 235:16 <b>unequivocal</b> 222:13 <b>unexpected</b> 12:4 <b>unfair</b> 200:15 <b>unfortunate</b> 77:5 <b>unfriendly</b> 244:8 <b>unhappiness</b> 49:7 <b>unhappy</b> 49:2 215:11,18 <b>unilaterally</b> 278:1,1 <b>unintentional</b> 96:20 <b>Union</b> 3:7 <b>unique</b> 12:5 18:14 26:19 47:15 229:19 <b>United</b> 8:4,19 9:12,15 10:15 10:21 29:8 39:20 40:4 67:8,11 71:18 71:20 72:3 73:11 86:20
--	---	---	---	--

89:5,11,13,15	<b>universally</b>	39:6,7,9,13	<b>variety</b> 13:15	<b>views</b> 5:2 7:7
89:17,22 90:2	225:4 295:15	78:10 81:20	23:5,10 34:17	182:9 250:4
90:13,15 91:10	295:19 296:18	91:15 96:5,15	65:10 75:14	268:21
97:17,20,21	<b>universe</b> 197:3,9	97:18 98:12	84:4 94:16	<b>vigorous</b> 276:15
103:10 104:18	<b>University</b> 3:5,8	106:13 111:7	<b>various</b> 22:9	<b>VII</b> 194:3
114:19 115:12	113:11,14	142:11 147:18	46:20 67:7	<b>violate</b> 11:21
128:3 129:8,10	<b>unknown</b> 83:8	159:7 171:6	69:3 153:15	156:14,20
129:13,19,22	233:1	172:5 176:7	238:8	224:18 232:6
130:14,22	<b>unlawful</b> 199:10	181:17 199:14	<b>varying</b> 6:13	264:21 265:20
131:2 133:6	211:4 216:9,12	201:1,2 203:17	277:18	<b>violated</b> 227:14
137:10,12,13	216:15,20	206:16 253:18	<b>vast</b> 150:5	<b>violates</b> 121:2
138:7 140:14	296:16 298:4	265:6,17	279:18 286:1	210:19 211:8
147:6 151:17	298:14	<b>useful</b> 67:15	293:5	231:6,20
159:18,19	<b>unreasonable</b>	85:22 103:4	<b>vastness</b> 227:1	296:21
162:2,18	121:11	106:9 170:10	269:10	<b>violating</b> 158:3
176:19 180:19	<b>unregulated</b>	206:2 283:13	<b>veneer</b> 142:11	217:1 231:13
210:7 211:15	144:8	<b>uses</b> 55:10 66:17	<b>venue</b> 301:6,11	<b>violation</b> 158:1
211:18 212:5,5	<b>unsupervised</b>	99:16 119:11	<b>Verdugo-Urq...</b>	215:22 253:8
212:15,16,18	130:15 144:12	<b>usually</b> 106:8	129:11 147:5	261:22 262:3
213:20 214:8	<b>upheld</b> 126:7	128:3 162:14	<b>versus</b> 71:14	263:21 264:8
215:8 216:5,6	<b>upholding</b>	303:18	129:10	265:21 267:7
216:7 217:7	121:15	<b>utility</b> 64:13	<b>viability</b> 220:11	286:13,17
239:8,20	<b>upset</b> 246:10	65:10 69:13,14	<b>Vienna</b> 231:21	296:17 297:6
240:11 243:20	<b>upstream</b> 26:5,6	<b>utilized</b> 66:1	249:4	<b>violations</b>
245:6,9,12,14	26:15,19 30:15		<b>view</b> 10:13	153:20 232:10
246:2,11 248:5	30:19 36:21,22	<b>V</b>	50:16 67:6	232:13 233:1
248:10,12	37:6,10,21	<b>vague</b> 286:12	83:3 89:3 91:2	<b>virtual</b> 234:20
250:2,8 251:13	47:13,15 56:9	<b>valid</b> 12:3,12	97:17 98:21	234:22
251:15 253:11	56:10 57:19	13:5 59:6,8,15	120:22 121:8	<b>virtue</b> 135:21
254:6 267:9	63:6 93:6,8,16	92:6 253:12	123:1 125:10	<b>vis-a-vis</b> 80:5
268:17 269:13	93:20,21 94:3	303:4	145:22 154:17	93:8 293:14
270:8 274:4	94:6 95:16	<b>validity</b> 6:10	159:16 182:22	<b>visit</b> 120:1
276:5 277:14	101:12 187:7	<b>valuable</b> 13:9	184:2 185:17	<b>vocabulary</b>
279:9 281:9	248:14	66:6 67:8,11	190:5,18	158:13 188:20
285:3,13,22	<b>Ur</b> 76:2	102:17,18	191:18 192:18	189:15
287:11,17,22	<b>urged</b> 7:5	<b>value</b> 43:21 44:6	193:9,22 211:9	<b>voice</b> 191:9
288:2,4 290:8	<b>Uruguayans</b>	44:15 45:11,22	218:12 246:2	<b>voicemail</b>
291:6,16 292:8	246:18	46:8,18 47:2	246:20 250:2	190:19
294:17 297:13	<b>USA</b> 5:11	65:17 80:2,16	251:9 263:12	<b>volume</b> 93:7,8
306:8 307:3,12	<b>usable</b> 176:12	82:3 102:14	277:6 291:7	<b>volumes</b> 180:20
309:17,18	<b>USC</b> 111:2	103:2 110:8	296:11 310:13	199:1
<b>Unites</b> 89:10	<b>USD</b> 188:10	163:8,11 164:3	<b>viewed</b> 10:22	<b>voluntarily</b>
<b>universal</b>	196:6	191:12 230:4	24:10 273:3	240:22
210:19 217:6	<b>use</b> 13:4 34:21	<b>values</b> 310:19	<b>viewing</b> 88:12	<b>voluntary</b>

197:20 241:3	308:12 309:4	247:1 260:14	<b>way</b> 16:16 20:22	110:21 112:14
<b>vote</b> 213:5	<b>Wald's</b> 77:13,16	261:13 266:21	31:4,4,12 34:4	113:8 115:2
<b>voted</b> 100:11	111:14 117:8	272:5 284:4,4	34:9 35:7	118:1 124:10
<b>vs</b> 139:21 142:8	<b>walk</b> 145:16	291:12 311:8	44:18 57:20	124:22 126:14
<b>vulnerability</b>	153:18	<b>wants</b> 59:1	64:12,14 78:2	137:9 142:11
229:6	<b>wall</b> 141:9	201:7 295:8	85:1 99:2,7,19	177:6,7 189:15
<hr/>	<b>walled</b> 220:5,7	<b>War</b> 225:2	101:22 104:5	194:9 198:5
<b>W</b>	220:14	<b>warrant</b> 8:5	137:18 138:13	199:5 207:21
<b>wait</b> 175:14	<b>want</b> 4:22 10:2	15:20 16:1,6	143:2,2 144:13	209:2 215:18
<b>Wald</b> 2:5 4:15	10:11 13:7	16:17 21:20	153:2 154:21	216:16 218:17
43:14,15 44:11	20:6 23:12	28:11 115:16	157:12 158:16	218:20 219:5
44:19 45:5,20	24:13,15 50:8	121:9 128:3	169:12 175:2,3	219:19 220:2,9
46:6,10 47:18	50:20 53:4,5	129:18 130:1,5	175:4 180:9,10	228:15 254:9
48:10 49:4	59:16 60:5	136:15 137:6	184:4 197:1,5	287:3 295:6
50:2 78:7,8,20	64:10 68:5	139:20 140:12	198:19 199:3	<b>we've</b> 11:15
79:12,15 81:16	69:10 76:20	142:5,9 143:6	203:3 208:4,9	23:8 27:13,14
82:17,20 106:2	77:4 85:4	146:21 147:2	208:10 219:22	29:15,16,19,20
106:3 107:5,11	86:16 89:1	150:2,16 151:6	222:16 225:8	30:11 36:1
109:9 110:1,9	91:9 96:5	151:12,14,18	246:1 257:5	58:5 61:2 65:6
110:12,19	100:8,13	152:8,10,10	268:4,7 271:8	70:7 84:8,8
111:12 112:16	103:11,15	154:2,10 160:8	278:20 280:1	85:1 172:12
112:19 167:14	112:22 113:18	172:9,10,16	287:12 309:11	176:7 188:21
167:15 168:12	125:9,13 132:6	173:1,11,13,15	313:10	189:19,20
168:15,17	145:13 149:19	177:11 180:8	<b>ways</b> 19:3 65:5	193:17 223:12
169:16 171:1	149:21 154:5	184:15,16	65:16 68:9	252:3 254:15
171:19 173:13	172:7 174:6	185:14 205:15	95:19 135:3	260:20 278:7
173:17 175:13	175:16 179:14	206:4,7 281:5	188:6 228:6	278:17 279:13
200:14,15	182:10,11,18	281:8	271:6 287:11	291:14
201:15,22	207:11 208:22	<b>warrantless</b>	306:22	<b>weapons</b> 59:13
202:4,19 203:3	209:7 215:9	14:12 115:2	<b>we'll</b> 8:14 32:13	285:6
203:11 204:5,8	218:14 233:16	121:4 126:8	32:14 50:5	<b>website</b> 312:9
205:12 207:8	242:21 243:6	128:7	77:21 113:4,5	<b>websites</b> 175:10
248:19,20	243:16 260:11	<b>warrants</b> 10:17	132:12 174:13	<b>week</b> 276:11
249:22 250:13	269:17 283:3	141:7 151:22	174:20 260:7	307:11
250:16 251:21	301:3 311:4,21	157:4,5 173:14	260:12 266:1,2	<b>week's</b> 239:14
253:1,13	<b>wanted</b> 5:3	256:15	<b>we're</b> 13:12,12	241:6
265:12 277:15	13:22 27:11	<b>Warren</b> 299:16	13:18 31:17	<b>weeks</b> 86:14
277:16 279:1	35:10 63:1,9	<b>Washington</b>	36:16 43:11	<b>weigh</b> 179:14
280:5,20 281:4	85:5,8 86:3,11	1:17 4:8	51:15,15,18	<b>weighed</b> 16:4
281:21 282:1	87:2 92:21	124:13 174:10	52:19 58:7	<b>weird</b> 138:5
282:21 283:15	93:5 96:4,17	<b>wasn't</b> 158:16	73:9,14 76:14	<b>welcome</b> 4:2
283:19 289:1	98:3 111:13	<b>wasting</b> 85:17	84:11 96:18,20	7:10 200:12
289:15 300:5	148:21 149:16	<b>Watch</b> 3:19	99:21 103:13	237:12
307:15,16	172:9 192:20	209:15 251:5,8	103:13,20	<b>welcomed</b>

311:18	90:5,17,20	308:19	228:11,14	<b>years</b> 11:20
<b>well-founded</b>	91:5,13,18,22	<b>wonderful</b>	<b>wouldn't</b> 23:14	47:14 69:5
234:5	92:4 103:8	168:2	48:2 52:5 90:3	94:22 99:9
<b>well-known</b>	105:14 107:17	<b>wondering</b>	92:10 168:7	101:9,11,11,12
35:22 274:2	108:2	172:2 252:15	171:2,16	101:12 104:9
<b>well-recognized</b>	<b>willfully</b> 224:18	<b>word</b> 56:6 96:5	<b>writ</b> 295:17	150:9 187:1
119:17	<b>William</b> 140:19	160:2 224:12	<b>write</b> 290:15,15	211:15 214:14
<b>went</b> 47:20	140:20	249:3,16	<b>writing</b> 245:19	301:8
140:11	<b>willing</b> 58:3	<b>wording</b> 213:11	311:6	<b>yesterday</b>
<b>weren't</b> 166:4	<b>willy-nilly</b>	<b>words</b> 26:14	<b>written</b> 7:9,20	124:13 174:10
188:7 274:21	297:19	38:6 45:12	87:8 88:4	<b>yield</b> 162:19
<b>Westphalia</b>	<b>wind</b> 216:3	57:13 107:22	116:21 121:13	288:9,11
305:1	<b>Winn</b> 5:5	108:4 127:17	132:18 159:5	<b>YouTube</b> 191:8
<b>whatsoever</b>	<b>winnings</b> 275:15	135:15 147:20	161:11 182:17	
134:9	<b>wire</b> 165:3	160:21 171:1	200:20 239:8	<hr/> <b>Z</b> <hr/>
<b>white</b> 140:10	<b>wire-brushing</b>	188:5 204:16	246:2 252:9	<hr/> <b>0</b> <hr/>
217:10 238:7	99:17	213:10 255:10	312:8	<hr/> <b>1</b> <hr/>
238:19 239:5	<b>wiretap</b> 12:16	260:9 278:11	<b>wrong</b> 40:3	<b>1</b> 43:9 258:8
239:10,13,19	12:16 14:16,18	<b>work</b> 238:10	66:21 67:2	<b>1:45</b> 209:3
240:8 241:16	21:19 29:10	266:6 282:19	71:19 72:3,5	<b>10</b> 93:16 313:17
242:18 275:13	115:16 146:20	302:18	73:20,22	<b>10th</b> 4:10
277:8 282:19	153:9 155:8	<b>working</b> 46:11	100:21 110:3	<b>1127</b> 1:16 4:8
<b>who've</b> 168:17	<b>wish</b> 104:4	79:15 110:20	160:2	<b>11th</b> 93:12
276:15	132:6 208:13	220:20 222:12	<b>www.regulati...</b>	<b>12333</b> 81:7,12
<b>wholly</b> 40:17	245:16 290:6	266:12	312:9	109:6,8
94:13 95:5,20	<b>withdraw</b>	<b>works</b> 20:15	<hr/> <b>X</b> <hr/>	<b>17</b> 210:21 211:3
95:22 134:15	300:11	108:20	<hr/> <b>Y</b> <hr/>	211:8 216:8
163:7	<b>witness</b> 256:4	<b>world</b> 83:10	<b>Yahoo</b> 191:7	217:1 233:20
<b>wide</b> 13:15	313:12	182:8 218:8	<b>Yahoo.com</b>	246:12 260:10
192:6	<b>witnesses</b> 35:21	219:12 234:15	207:3,4,5	261:17 267:7
<b>wide-ranging</b>	160:19 284:20	234:21,22	<b>yeah</b> 75:9 84:7	289:22
126:8	309:10 310:12	246:4 250:3	104:4 107:15	<b>18</b> 188:10 196:6
<b>widely</b> 277:18	<b>WMDs</b> 59:12	252:2 254:8	109:1 146:13	<b>1806</b> 111:2
<b>Wiegmann</b> 2:19	<b>Wolf</b> 3:22	262:16 264:2,3	155:7 164:17	<b>1881</b> 161:21
15:4 17:5 18:7	209:18 238:1,2	275:21 283:12	248:15 249:22	<b>1890</b> 299:19
18:12 19:1,21	254:22 275:7	289:19 293:11	249:22 255:10	<b>19</b> 1:10
20:16 27:21	275:13 277:5	305:6 307:6	288:21 296:2	<b>1950</b> 211:19
28:22 35:16	278:20 282:2	310:17	<b>year</b> 5:8 17:19	212:21 213:6
43:6 50:22	282:18 283:5	<b>world's</b> 229:19	22:8,14,16	<b>1967</b> 140:9
53:3,8,17 55:1	299:15	<b>world-wide</b>	23:1,4,7,15,16	<b>1970s</b> 15:21
56:1 60:1 61:5	<b>Wolf's</b> 274:1	231:14	47:8 74:20	<b>1972</b> 139:22
61:16 73:5	<b>won</b> 233:10	<b>worse</b> 260:5	219:20 220:20	<b>1973</b> 195:10
75:4 76:13	<b>wonder</b> 45:16	<b>worth</b> 68:3 74:8		
77:17 89:18,20	<b>wondered</b> 249:2	88:6 126:7		

150:13 <b>1990</b> 129:10 <b>1992</b> 211:2 <b>1995</b> 211:20 213:9 <b>19th</b> 4:6	<b>3</b>	78:3 79:2 80:5 81:1 88:15 90:9 91:15 97:18 99:21 100:1,10 107:8 111:4 112:15 113:21 117:13 118:11 119:12 121:1 123:13 123:21 124:10 124:11 125:17 125:19 126:12 126:15,18 128:5,12 129:4 130:19,21 131:6,11 132:22 133:3 135:4,6 137:9 141:17 145:22 148:7 151:4,8 151:8 152:20 158:22 160:14 165:5,10,10 170:7 186:9 187:5 193:1,18 194:3,13 196:7 200:17 201:6 202:12 203:14 204:15,17,21 205:12 207:22 219:4 221:12 221:17 223:6 228:2,3 239:6 240:4,7 243:3 243:19 267:2 267:16 272:2 273:9,20 274:10 277:22 280:22 281:6 281:11 291:20 292:20,22 293:21 <b>703</b> 177:4 <b>704</b> 92:18 177:4	3 231:21 <b>3:40</b> 312:20,21 <b>30</b> 61:20 <b>31</b> 234:2 249:4 249:20 <b>32</b> 303:22 304:4	<b>8</b>	<b>8</b> 213:6
<b>2</b>	<b>4</b>	<b>9</b>	<b>9/11</b> 34:17 257:2 257:13 <b>9:00</b> 1:17 <b>9:05</b> 4:6		
<b>2</b> 92:18 212:6 213:6 231:3 304:21 305:7 <b>2001</b> 210:11 <b>2002</b> 116:2 141:10 <b>2003</b> 1:17 <b>2005</b> 210:9,11 <b>2008</b> 75:15 77:15 247:17 <b>2009</b> 210:10 <b>2010</b> 234:7 <b>2011</b> 93:13 94:9 134:13 135:19 <b>2012</b> 69:6 100:1 <b>2013</b> 234:8 238:6 239:5 313:13 <b>2014</b> 1:10 4:6,10 5:14 313:17 <b>215</b> 5:10,13 47:20,21 48:16 48:20 49:16,21 50:3 69:1,4 152:22 157:7 170:7 204:11 204:18 219:3 221:18 272:12 273:8 292:18 293:2 <b>23rd</b> 5:13 <b>25th</b> 219:20 <b>28</b> 237:13 <b>28th</b> 7:12 312:10	402 157:8 <b>49</b> 40:2				
	<b>5</b>				
	<b>50</b> 111:2 <b>51</b> 39:19 40:2,21 40:21				
	<b>6</b>				
	<b>60</b> 42:18 59:21 62:8 <b>68167</b> 236:6				
	<b>7</b>				
	<b>701</b> 252:18 <b>702</b> 1:7 2:10 3:2 4:4 5:11,16 7:17 8:12,14 8:17,21 10:3,5 10:11,20 11:4 11:8,22 12:5,9 12:22 13:8,10 19:12,19 21:3 21:12 22:6 23:18 25:4,8 25:16 30:22 36:14 37:9 38:6 40:5 43:18 48:3,12 48:15,22 49:16 56:8 65:6,15 66:10 67:7 69:6,19,19,20 70:9 71:2,4 75:17 77:18,20				