

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

Consideration of Recommendations for Change:
The Surveillance Programs Operated Pursuant to
Section 215 of the USA PATRIOT Act and
Section 702 of the Foreign Intelligence
Surveillance Act

November 4, 2013

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

Reported by: Lynne Livingston

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

BOARD MEMBERS

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

PANEL I

- Section 215 USA PATRIOT Act and
- Section 702 Foreign Intelligence Surveillance Act

- Brad Wiegmann, Deputy Assistant Attorney General,
National Security Division, Department of Justice
- Rajesh De, General Counsel, National Security
Agency
- Patrick Kelley, Acting General Counsel, Federal
Bureau of Investigation
- Robert Litt, General Counsel, Office of the
Director of National Intelligence

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

PANEL II

Foreign Intelligence Surveillance Court

James A. Baker, formerly DOJ Office of
Intelligence and Policy Review
Judge James Carr, Senior Federal Judge, U.S.
District Court, Northern District of Ohio and
former FISA Court Judge, 2002-2008
Marc Zwillinger, Founder, ZwillGen PLLC and former
Department of Justice Attorney, Computer Crime &
Intellectual Property Section

PANEL III

Academics and Outside Experts

Orin Kerr, Fred C. Stevenson Research Professor,
George Washington University Law School
Jane Harman, Director, President and CEO, The
Woodrow Wilson Center and former Member of
Congress
Stephanie K. Pell, Principal, SKP Strategies, LLC;
former House Judiciary Committee Counsel and

1 Federal Prosecutor

2 Eugene Spafford, Professor of Computer Science and

3 Executive Director, Center for Education and

4 Research in Information Assurance and Security,

5 Perdue University

6 Stephen Vladeck, Professor of Law and the

7 Associate Dean for Scholarship at American

8 University Washington College of Law

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 PROCEEDINGS

2 MR. MEDINE: Good morning, I'm David
3 Medine and I'm the Chairman of the Privacy and
4 Civil Liberties Oversight Board.

5 Welcome to the first public hearing of
6 the PCLOB. It is 9:20 a.m. on November 4th, 2013,
7 and we're in the ballroom of the Mayflower Hotel,
8 located at 1127 Connecticut Avenue NW, Washington,
9 D.C.

10 This hearing was announced in the
11 Federal Register on September 16 and October 25,
12 2013. As chairman, I will be the presiding
13 officer.

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

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

20 (Aye)

21 MR. MEDINE: Upon receiving unanimous
22 consent we will now proceed.

1 PCLOB is an independent bipartisan
2 agency within the Executive Branch, established by
3 the implementing regulations of the 9/11
4 Commission Act. It is comprised of four part-time
5 board members and a full-time chairman.

6 The board's primary missions are to
7 review and analyze actions the Executive Branch
8 takes to protect the nation from terrorism and
9 ensuring the need for such actions is balanced
10 with the need to protect privacy and civil
11 liberties and to ensure that liberty concerns are
12 appropriately considered in the development and
13 implementation of law, regulations and policies
14 related to efforts to protect the nation against
15 terrorism.

16 Essentially the PCLOB has two
17 functions, an advisory and oversight role with
18 respect to our country's counterterrorism efforts.

19 I want to thank the many panelists who
20 will be participating in today's hearing for
21 agreeing to share their views with the board.

22 I also want to thank Sharon Bradford

1 Franklin, the Board's Executive Director, Sue
2 Reingold, the Chief Administrative Officer and
3 Diane Janosek, the Chief Legal Officer for their
4 tireless efforts in making this event possible.

5 PCLOB has agreed to provide the
6 President and Congress with a public report on two
7 federal counterterrorism programs, the Section 215
8 program under the USA PATRIOT Act, and the 702
9 program under the FISA Amendments Act.

10 The 215 program is sometimes referred
11 to as the business records collection program.
12 One of the things the government collects under
13 this program is telephone metadata for
14 intelligence and counterterrorism purposes
15 pursuant to order by the Foreign Intelligence
16 Surveillance Court.

17 The 702 program involves collection of
18 foreign intelligence information from electronic
19 communications service providers under Foreign
20 Intelligence Surveillance Court supervision.

21 The purpose of today's hearing is to
22 consider possible recommendations the board might

1 make regarding these programs, as well as the
2 operations of the Foreign Intelligence
3 Surveillance Court.

4 Just to be clear, the questions the
5 Board Members pose today do not necessarily
6 represent either their views or the views of the
7 board.

8 The purpose of this hearing is to
9 explore a wide range of recommendations to assess
10 their benefits, costs and possible unintended
11 consequences. The Board believes it will be in
12 the best position to make its recommendations by
13 having public discussion of these options.

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

19 After the first panel we will be taking
20 a lunch break.

21 This afternoon, the second panel will
22 include a former Foreign Intelligence Surveillance

1 Act judge and two lawyers who have appeared before
2 the court, the FISC, one on the government side
3 and one representing a private sector client.

4 Finally, the third panel will include a
5 former member of Congress and four academics who
6 will respond to the discussion during the first
7 two panels.

8 Board members will each pose questions
9 during each panel with ten minute questioning
10 rounds for the first panel and five minute rounds
11 for the other two panels. Panelists are urged to
12 keep their responses brief to permit the greatest
13 exchange of views.

14 This program is being recorded and a
15 transcript will be posted on www.pclob.gov.
16 Written comments from members of the public are
17 welcome and may be submitted online at
18 regulations.gov or by mail until November 14.

19 Since we are still waiting for one
20 panelist we might just take a few minutes break,
21 or we can get started. It might be helpful to
22 maybe just take a few minutes break.

1 MR. DEMPSEY: Why don't we get started.

2 MR. MEDINE: You want to get started?

3 Okay, we'll jump in and then we'll pick up with
4 the rest of the panel.

5 I want to introduce our panelists,
6 Rajesh De, who's the General Counsel at the
7 National Security Agency, Patrick Kelly, who's the
8 Acting General Counsel at the Federal Bureau of
9 Investigation, and Brad Wiegmann, who's the Deputy
10 Assistant Attorney General at the National
11 Security Division of the Department of Justice.

12 There were allegations in the press
13 last week that the NSA had secretly broken into
14 main communication links that connect Yahoo and
15 Google data centers around the world under
16 something called Project Muscular, which allows
17 the NSA and the British Intelligence Agency
18 Government Communication Headquarters or GCHQ to
19 copy data flows across fiber optic cables that
20 carry information among the data centers of these
21 Silicon Valley companies.

22 Could the panel please explain what

1 that program is about and what impact it has upon
2 the programs that are the subject of today's
3 hearing, which is the 215 and 702 program?

4 MR. DE: Why don't I start on that.
5 I'm sorry, I can't address the veracity or lack
6 thereof of the details of the article, but I think
7 it's worthwhile making a few general points for
8 everybody.

9 Even by the terms of the article itself
10 there is no connection to the 702 or 215 programs
11 that we are here to discuss. I would suggest
12 though that any implication which seemed to be
13 made in some of the press coverage of this issue
14 that NSA uses Executive Order 12333 to undermine,
15 or circumvent or get around the Foreign
16 Intelligence Surveillance Act is simply
17 inaccurate.

18 As the panel will know, and as the
19 public should know, FISA is statute that has
20 particular jurisdictional coverage. You're either
21 covered by FISA or you're not covered by FISA.
22 And historically FISA was intended to cover that

1 type of collection that most would impact U.S.
2 person privacy and the key factors which many
3 learned scholars, folks like David Chris, have
4 written about, are things like the nationality of
5 targets, location of coverage, location of
6 targets, where the collection and how the
7 collection is undertaken.

8 I would note just as a general matter
9 though that any collection NSA does would involve
10 minimization procedures that are approved by the
11 Attorney General, or if coverage were under FISA,
12 by the FISC, that has rules in place to minimize
13 the collection, retention and use of any
14 incidentally collected U.S. person information.

15 The last point I'd make is, and I'd
16 implore you and the public that as you read
17 articles that may or may not be true, just to read
18 them with the rigor that you would expect us to
19 speak about activities.

20 And so in some of these articles, I
21 think I noticed you would have a line in paragraph
22 two of the article that says, NSA is well

1 positioned to collect vast amounts of U.S. person
2 information, and somewhere around paragraph 30 you
3 might have a line that says, it's unclear how much
4 U.S. person information NSA collects or retains.
5 And so I think it would be useful for everybody to
6 read coverage with a certain amount of rigor.

7 And I'd leave it at that.

8 MR. MEDINE: Then I want to turn to the
9 215 program that is the subject of today's
10 hearing. As you know there are a number of
11 legislative proposals that have been introduced
12 to, a range from abolish the program to modify the
13 program, and a lot of concerns have been raised
14 about the scope of collection, the information
15 held by the government.

16 What is your response to the proposal
17 that the 215 bulk program should simply be shut
18 down?

19 MR. DE: Well, why don't I speak to the
20 operational part of the program for a minute and
21 then I can maybe turn it over to Brad for
22 Justice's point of view and obviously to the FBI

1 for whom this program is extremely beneficial.

2 So from NSA's point of view, I think
3 we've made a few points publicly which is that
4 this is a valuable program, that along with many
5 other surveillance tools contributes to our
6 mission. It was intended to help cover a seam to
7 make the connections between foreign threat
8 streams, any domestic nexus that those might
9 threat streams might have.

10 I think I'd make the point though that
11 215 in particular, which is the telephone metadata
12 program, and maybe I should just start with some
13 basics since obviously the panel is well-versed in
14 this program, only involves telephone metadata.
15 It does not involve any content of telephone
16 calls, it does not involve any identifying
17 subscriber information, and NSA does not collect
18 any cell site location information.

19 This tool is used primarily as a
20 discovery tool in order to discover, unearth
21 potential leads to domestic ties to international
22 threat streams. And if such tips are evidenced we

1 hand them over to the FBI for further
2 investigation.

3 I think though that in the public
4 debate there's been a lot of discussion of, name a
5 plot, that without this tool inevitably would have
6 happened, and I think that's probably not the
7 right question to ask.

8 From the intelligence community's
9 perspective intelligence is a function that is
10 brought together by lots of different tools that
11 work in complement to one another.

12 And I would also suggest that any
13 particular plot, it's rare that you're going to
14 find a situation where some particular event was
15 only unearthed or only stopped as a result of one
16 particular intelligence tool. And I think that
17 probably misleads the debate in terms of the value
18 of the program, but I'd ask my FBI colleagues and
19 DOJ colleagues to weigh in.

20 MR. KELLEY: We find the 215 program to
21 be very helpful to us. We, since 9/11 have been
22 charged not with retroactively solving, which we

1 continue to do, but on the national security side
2 to prevent terrorist attacks. Now that's a
3 fundamentally different and much harder thing to
4 do. So we need information.

5 This is one tool. It's not the only
6 tool. It's not a tool that we can say is
7 absolutely must have. It is extremely critical
8 though and helpful to us. When we try to connect
9 the dots, the more dots that we have to connect,
10 the better off we are in accomplishing our mission
11 of preventing terrorist attacks. So the program
12 that we have here -- good morning.

13 MR. LITT: Sorry I'm late.
14 Transportation into Virginia is a little
15 difficult, although I will note that the panel
16 started early.

17 MR. KELLEY: As I said, the 215 program
18 as Raj indicated provides us with metadata. It
19 does not provide us with content of
20 communications, just data such as the number from
21 which a call was made to the number that is
22 dialed, the length of the call and the date of the

1 call.

2 So it's primarily of interest to us
3 because we may have telephone numbers from our own
4 other tools, investigative tools, but we may not
5 realize the significance of the number, without
6 the 215 abilities that NSA has to analyze that
7 data and then provide context to us in turn, we
8 may not realize the significance.

9 It provides a way for us to be agile.
10 It provides a way for us to respond more quickly.
11 Time in counterterrorism investigation is a very
12 important element. It has resulted in several
13 cases over the years, more than several, being
14 opened that we may not have otherwise opened.

15 It has also permitted us to focus
16 resources. We may have had a preliminary
17 investigation, for example, open and then when the
18 information came to us that this number we had was
19 contacting a known or suspected terrorist safe
20 house, for example, overseas, it then would
21 provide us the requisite articulation of facts to
22 escalate that preliminary investigation to a full

1 investigation.

2 That in turn allows us to focus our
3 resources better and focus our energies and our
4 investigative efforts.

5 I think that over the years we've had a
6 number of open declarations filed that give us an
7 indication of the value of the program. In 2009
8 Director Mueller filed an affidavit with the FISC
9 Court that indicated that at a particular time
10 there were 27, I think, full investigations open.

11 It's very difficult in any particular
12 investigation to say that this fact or that fact
13 is very important, but over time we can say that
14 these things are extremely helpful to us. So we
15 do think there's value in the program.

16 MR. MEDINE: I guess my question is if
17 the program was discontinued would it be a
18 practical option as some have suggested to just
19 gather information from the telephone company
20 providers rather than having NSA maintain data on
21 all Americans' phone calls?

22 MR. DE: Let me defer to Pat on the use

1 of NSLs perhaps, which would presumably be the
2 alternative.

3 MR. KELLEY: If we did not have this
4 program and used other lawful investigative ways
5 to obtain particular phone numbers from particular
6 subjects, we wouldn't be able to see the patterns
7 that the NSA program provides us.

8 We would be able to, for example,
9 through the use of a grand jury subpoena or a
10 national security letter on the national security
11 side, obtain information about a particular phone
12 number and we'd get the first tier of the phone
13 numbers that that number had connected with, but
14 we would not be able to go into a second tier or a
15 third tier, hops it's commonly called, which the
16 NSA program provides.

17 Additionally, we would be able to
18 perhaps go to service provider, to service
19 provider, to service provider and then
20 individually try to connect those dots, but
21 without the ability to look at all the data in a
22 composite way, it would be much harder, it would

1 be much slower, much more difficult for us to do
2 that.

3 So with those two indicators there,
4 we'd be less agile, we'd be less informed, and
5 we'd be less focused and we think that as a result
6 we'd be a lot less effective in preventing the
7 attacks that the American people want us to
8 prevent.

9 MR. MEDINE: I see that my time has
10 expired. Ms. Brand?

11 MS. BRAND: Thank you, Mr. Chairman.

12 Let me just follow-up on that since
13 your time ran out. I had some questions related
14 to the same subject.

15 Even if you were able to use a grand
16 jury subpoena or an NSL to go provider to provider
17 to ask for the information, would the information
18 be there without a record retention requirement?

19 MR. KELLEY: That's a very good
20 question. Without the 215 program it would be up
21 to the service provider to determine how long they
22 would keep the records. I think FCC regulations

1 require them to keep these things for 18 months.

2 The NSA program keeps them for five years.

3 So the likelihood without the 215
4 program would be that much of that information
5 would simply not be there, so there would be no
6 dots to connect.

7 MR. LITT: Can I add something on that?

8 MS. BRAND: Sure.

9 MR. LITT: It's my understanding that
10 FCC regulations, and I'm not an FCC lawyer by any
11 means, but that the FCC regulation relates to toll
12 billing records.

13 It's not at all clear to me that if all
14 providers moved to a system where there are no
15 longer -- first of all, that doesn't include local
16 calls. And second, if providers move to an
17 environment where none of them are billing for
18 toll calls at all whether those records would be
19 retained even pursuant to the FCC regulation.

20 MS. BRAND: Thank you. You just
21 answered my next question.

22 MR. LITT: Sorry, Rachel.

1 MS. BRAND: Perfect. No, that's good.

2 Relatedly, we've heard some talk about
3 sort of a competition downwards in terms of
4 retention requirements where it's not required by
5 FCC regulation that providers for sort of
6 commercial competitive reasons would decrease
7 their own record retention periods. Have you seen
8 any evidence of that actually happening or is that
9 more of a theoretical concern?

10 MR. DE: I can't speak to that
11 particular issue but I probably should add one
12 other point in addition to what Bob and Pat made.
13 In order to run a program like the 215 program the
14 data has to be provided or kept in a way that
15 allows it to be integrated.

16 And so I think in addition to the
17 availability of the records, they have to be
18 available in a way that would allow for the sort
19 of analysis that the 215 program allows.

20 MS. BRAND: Can you, any of you, speak
21 to whether there might be some privacy concerns
22 that would be created if, just posit for a moment

1 that there is a record retention requirement of,
2 say, two years for something more than toll
3 billing records, or perhaps even just toll billing
4 records, does that in your mind create additional
5 privacy concerns?

6 And relatedly, would there be any
7 reason why those retained records could not be
8 sought in civil litigation, divorce proceedings,
9 criminal proceedings, immigration proceedings or
10 any other kind of legal process?

11 I don't know who wants to take that,
12 maybe DOJ. Brad, do you want to?

13 MR. WIEGMANN: Sure. So, you know,
14 these are records that the companies keep for at
15 least some period of time now and they can be
16 obtained, as Pat mentioned, through an NSL or
17 through grand jury subpoena, etcetera. So these
18 are records that don't enjoy Fourth Amendment
19 protection under the Supreme Court's holdings.

20 But I think the longer you require the
21 companies to keep them, then that's data that is
22 being kept by a company for a longer period of

1 time.

2 So if you create a five-year period
3 then that's information that's available there and
4 can be subpoenaed. You know, private lawyers can
5 subpoena the data. I mean the data is not, it's
6 not private in that sense, but to the extent
7 people have concerns about the data being
8 compelled, it would be held for a longer period of
9 time by the private sector rather than by the
10 government. So that's at least conceivably a
11 privacy concern for them.

12 MR. KELLEY: In addition to that, once
13 the data's destroyed by the companies, of course
14 then it's not available, which is on the privacy
15 side a good thing because hackers can't get into
16 it, and as you indicated in your questioning it
17 couldn't be used for other purposes.

18 I've been told, for example, that if
19 the data exists, other levels of law enforcement
20 from local, state, federal would want it for
21 whatever law enforcement purposes they were
22 authorized to obtain it, and civil litigation

1 could also seek to obtain it for such things
2 relatively mundane as divorce actions. Who's
3 calling who and your spouse if it's a contested
4 action, for example.

5 So if the data is kept longer by the
6 companies then I think the privacy considerations
7 certainly warrants some scrutiny.

8 MS. BRAND: The hacking point that you
9 raised is to my mind both a national security
10 concern and a privacy concern, but I have to ask
11 in light of some of recent revelations, do you
12 think that, is the data in the government's
13 possession more protected from hacking than it
14 would be if it were in the possession of the
15 private sector? And what are you doing and what
16 can you do to make sure that it is?

17 MR. DE: I think that's a great
18 question and I think that any evaluation of where
19 else to keep such data should take that comparison
20 into account.

21 So we don't have any reason to believe,
22 based on current assessment, that Edward Snowden

1 had access to raw material in the business records
2 database. Now why is that the case?

3 I think I'd make the case that the
4 current program is one of the most highly
5 regulated programs in the federal government today
6 and I think that regardless of the benefit of
7 folks who have privacy concerns or interests in
8 the protection of such data.

9 So what do I mean when I say it's a
10 highly regulated program? For one, pursuant to
11 the court's orders, the data has to be kept
12 segregated from all other types of raw
13 intelligence.

14 Two, the purpose of the program is
15 purely for counterterrorism purposes so this data
16 can't be used for other purposes, as we've just
17 been discussing might be the case in other
18 circumstances.

19 Three, the program is re-authorized
20 every 90 days by the Foreign Intelligence
21 Surveillance Court. We at NSA, together with
22 Justice report to the FISC every 30 days on the

1 use of the data. The program is audited every 90
2 days by the Department of Justice.

3 Pursuant to the court's orders only 22
4 senior officials may approve queries into the data
5 and those queries have to be based on a reasonable
6 articulable suspicion that the number used is
7 associated with a specific foreign terrorist
8 organization.

9 Only seven officials by court order are
10 authorized to disseminate information to the FBI,
11 for example, if any U.S. person information is
12 involved.

13 There are significant technical
14 controls limiting access to the data. So for
15 example, a typo in this case can't go through in a
16 query because there are technical controls that
17 only allow RAS approved numbers to be used as
18 query terms.

19 And finally, pursuant to the court's
20 orders there are rules for the Inspector General
21 at NSA and of course we have oversight from the
22 Department of Defense which has its own inspector

1 general, as well as the ODNI which has its own
2 inspector general.

3 MS. BRAND: I just want to follow-up on
4 the RAS, the reasonable articulable suspicion
5 standard, and I have a series of questions which
6 I'll continue in the next round if I need to.

7 But can you explain what that means?
8 What is RAS? Give me an example of how much
9 information would be enough to meet it. Is this
10 the Terry stop standard? Is it something more?

11 MR. DE: So this is a legal standard
12 that does sort of have origins in Terry stop
13 jurisprudence. And I'll turn to Brad in a minute
14 to articulate that.

15 But what that would mean is it's
16 effectively the same standard that's used for stop
17 and frisk for a law enforcement officer to pat
18 down somebody on the street. Every single RAS
19 determination has to be documented before a query
20 is made.

21 MS. BRAND: But give me an example of
22 what would be enough. Give me an example of sort

1 like the basis for a RAS determination.

2 MR. DE: So it could be, for example,
3 through other intelligence a known connection of a
4 telephone number to an Al Qaeda operative, for
5 example.

6 The intent of the standard is to be
7 significant enough that a query can't be made on a
8 hunch or for no particular reason at all, but
9 sufficiently able to be met so that the tool can
10 in fact be used as a discovery tool to discover
11 unknown operative, which is the whole point of the
12 program.

13 MS. BRAND: And what is the paper
14 trail, what kind of records create the basis for a
15 RAS determination?

16 MR. DE: So every RAS determination is
17 documented and kept in a computer database. They
18 are only, every RAS determination is only valid
19 for a set period of time pursuant to the court
20 orders. It's 180 days if it's a U.S. number or
21 365 days if it's a non-U.S. number.

22 NSA as a matter of proactive

1 compliance, reexamines RAS determinations in half
2 that time. Every 90 days the Justice Department
3 comes to NSA and audits RAS determinations,
4 written RAS determinations, as does our Inspector
5 General, pursuant to the court's orders.

6 MS. BRAND: And after 180 days does the
7 RAS selector disappear? Can you get it
8 re-authorized? What happens with that?

9 MR. DE: It may not be used to conduct
10 queries unless a new RAS determination is made or
11 a continuing viability of the existing RAS
12 determination.

13 MS. BRAND: And what's that
14 re-authorization process? Is it simply reliance
15 on the evidence that was provided the first time
16 or does that evidence have to be reverified?

17 MR. DE: It certainly has to be
18 reverified as of the time of the determination.
19 So any time a RAS determination is made the
20 information used to support that determination has
21 to be to the best of our knowledge current at the
22 time of the determination.

1 MS. BRAND: So one suggestion that
2 we've heard to improve the process would be for
3 DOJ to have more involvement in the RAS process,
4 the process of approving a particular RAS
5 selector. I think the theory there is that DOJ
6 has more experience with determining whether
7 standards of proof have been met.

8 Does the administration have a position
9 on that suggestion? Brad, I'm looking at you
10 because you're from DOJ, but anyone can answer it.

11 MR. WIEGMANN: I really think I
12 understand that argument but I think the better
13 analogy is to the operator on the street who's
14 making that determination. I mean lawyers don't
15 make that determination if there's reasonable
16 articulable suspicion to stop someone and frisk
17 them on the street because they're suspected of
18 criminal activity.

19 I think for the same reason here we're
20 not going to be in as good a position as an
21 intelligence operative is to know whether there's
22 suspicion that a number is associated with a

1 particular foreign terrorist organization
2 overseas. So I think we've got it about right
3 where we have it now to leave that with the
4 operators.

5 So the example I always think of, you
6 ask what would be a RAS determination would be,
7 you know, a laptop is obtained when a foreign
8 government arrests a terrorist overseas and that's
9 a laptop that we believe is used to communicate,
10 that terrorist has used to communicate with other
11 terrorist operatives, and on that laptop there's a
12 bunch of phone numbers.

13 That's the type of situation where a
14 phone number obtained on that, and you look up and
15 you see there's a U.S. phone number, the
16 government wants to know who is he calling in the
17 United States.

18 And so that's the kind of classic
19 example I always think of, and that's something I
20 think that's really more operational and not so
21 much a DOJ lawyer sitting back in Washington
22 making that judgement.

1 MR. MEDINE: Thank you.

2 Ms. Cook?

3 MS. COLLINS COOK: Thank you. And I
4 wanted to thank you guys for coming today. I
5 think it's helpful to have the opportunity to ask
6 some more and more specific questions as we are
7 moving through our process of analyzing these
8 programs.

9 I did want to ask one follow up
10 question, Brad, on what you were just talking
11 about. It's certainly true that the police
12 officers are the ones on the street making the
13 determination in a specific case, but that's
14 typically after a long period of training, a lot
15 of thought given on how the training is developed
16 and implemented.

17 To what extent is DOJ involved in the
18 development of the RAS standard, the training of
19 that and the oversight to ensure that the operator
20 on the street is in fact appropriately using the
21 RAS standard?

22 MR. WIEGMANN: Well, we do, as Raj

1 said, we do review each and every RAS
2 determination after it's made at the Department of
3 Justice. We're not doing it in real time because
4 we think, as I said before, and on the front lines
5 that's the operators who are in the best position
6 to do that.

7 But also to say, the point I didn't
8 make was that this is designed as kind of an alarm
9 system. It's a kind of rapid reaction program so
10 that the government, when they have this number
11 they want to know right away whether that number's
12 calling any numbers in the United States to see
13 whether we can find out if there are any contacts
14 and whether there's terrorist plotting that's
15 occurred.

16 But given a little more time,
17 absolutely, lawyers are involved, heavily involved
18 in reviewing every single RAS determination to
19 look back at all the facts and say, was there
20 enough there.

21 So there is that kind of balance. You
22 have both the operators, but then the lawyers come

1 in after the fact to make sure that those were all
2 correct.

3 And if we were to find a compliance
4 problem with a RAS determination that would be
5 reported, and is reported, to the court, again, in
6 conjunction with those 90 day reviews that Raj
7 mentioned.

8 MR. DE: If I could add one point onto
9 this. I think the now-public court orders
10 authorizing the program expressly articulate that
11 which actually happens in practice, which is we
12 and Justice work together on all significant legal
13 interpretations of the 215 program and that
14 includes training materials and other things like
15 that.

16 MS. COLLINS COOK: So I wanted to go
17 back to something you had mentioned earlier, Raj.
18 You started off by saying that there's a lot of
19 talk about how many plots have been disrupted or
20 thwarted, and you said that's not the right
21 question.

22 So I have a two-part question for you,

1 what is the right question and how frequently is
2 the Department of Justice asking the question, how
3 often is NSA asking the question in a serious and
4 systematic way, is this an effective program? It
5 turns out it's going to be a three-part question,
6 and when you do so what metrics are you using?

7 MR. DE: So I think that is a very
8 valuable question to ask across the board for NSA
9 intelligence programs, and I'm sure Bob will speak
10 to intelligence programs regardless of the agency.
11 So let me give you a few data points for the 215
12 program.

13 As I mentioned, this program is
14 re-authorized every 90 days by the FISC --

15 MS. COLLINS COOK: Actually can I stop
16 you there. I'm asking about the effectiveness of
17 the program and not necessarily compliance or
18 whether it continues to meet legal requirements,
19 but as a counterterrorism tool, whether as rapid
20 response, as Brad, you've characterized it, or
21 prevented it, as Pat, you've characterized it, the
22 effectiveness of the program.

1 MR. DE: So every 90 days we submit a
2 declaration both from NSA and from the
3 intelligence community that articulates the need
4 for the program and how, as part of the relevant
5 standard.

6 And so in other words, the standard to
7 make the relevance showing needs to articulate why
8 such telephone records are helpful in the
9 counterterrorism mission, to put it in lay person
10 terms.

11 And so I would say at a minimum every
12 90 days there's some internal mechanism built-in
13 to at least revalidate the program.

14 I'd also add that as Congress has been
15 doing recently adding legislative sunsets to
16 provisions, regardless of whether one thinks
17 that's a good idea or a bad idea, that is a built-
18 in idea that Congress should reevaluate the
19 effectiveness of intelligence programs.

20 The 215 program was re-authorized twice
21 within the last five years and apart from current
22 efforts is up for expiry in 2015. And so those

1 are natural points to evaluate the effectiveness
2 of the program.

3 The third thing I'd mention is like all
4 federal agencies, NSA has significant resource
5 constraints and so apart from the mission value of
6 the program, we are constantly reevaluating all
7 sorts of programs, particularly expensive ones
8 like the 215 program, to see if they're worth the
9 expenditure.

10 And then the fourth data point I'd add
11 is there's been some public discussion of another
12 metadata program that was conducted on email
13 metadata that's no longer in existence. And that
14 program was ended in 2011 precisely for the reason
15 you raise which was, at least in part, an
16 evaluation was made that it wasn't meeting
17 operational effectiveness needs.

18 MR. KELLEY: And if I could add to
19 that, it's very difficult to say, just say we've
20 stopped this number of attacks, or opened this
21 number of cases, or produced this number of
22 intelligence reports. But as I indicated before,

1 we have provided publicly some numbers and some
2 illustrations, including a plot that was to bomb
3 the New York subway system. So that's one case
4 and one plot disrupted.

5 There was a similar attack in Madrid
6 several years ago, as you know, and hundreds of
7 people were killed and wounded in that single
8 attack.

9 So when you evaluate effectiveness,
10 it's not just numbers that you have to look at,
11 but you have to look at victims who are no longer
12 victims or never were victims. And I think to put
13 everything into context here is very important.
14 So I think that question deserves a lot of public
15 attention and looking at the full spectrum of the
16 value includes everything from people who are not
17 victims up to intelligence reports that are
18 produced.

19 MS. COLLINS COOK: You had mentioned
20 earlier in response to some of the questions that
21 Rachel had asked that you could end up with a
22 situation without the 215 program where you would

1 have data perhaps up to 18 months, the age of the
2 data would be 18 months, as opposed to five years
3 now.

4 To what extent do you in a systematic
5 and regularized way assess the helpfulness of the
6 data that is two years old, three years old, four
7 years old, five years old? Is there an empirical
8 basis for believing that these older records are
9 still in fact useful?

10 MR. KELLEY: I'm not aware of any study
11 where we've gone back to look at those specifics.
12 But again, in this counterterrorism environment we
13 have to look in terms of a very broad programmatic
14 review, not just attacks thwarted but how
15 terrorism organizations exist, what their finances
16 are, what their objectives are, how they operate.

17 So if we, for example, had a different
18 type of tool to obtain numbers, most of those
19 numbers that we would obtain would be going
20 forward. We wouldn't have the ability to look
21 back. So if the data is retained for a shorter
22 period of time then ours to analyze is also

1 reduced.

2 So again, I don't think that we can put
3 precise numbers or definitions on it, but I do
4 think that in the long run the more dots we have
5 to look at these analytical or through these
6 analytical tools, then the better we will be at
7 connecting them.

8 MS. COLLINS COOK: And I just wanted, I
9 think I have -- yes, good, I still have a little
10 bit more time. You had indicated there could be
11 limits on the use of either grand jury subpoenas
12 or NSLs because you would only get what you
13 referred to as the first hop. But couldn't you do
14 sequential NSLs or sequential grand jury subpoenas
15 to obtain exactly that second or third hop type of
16 information?

17 MR. KELLEY: I think we perhaps could.
18 I don't know if we could get the second and third
19 layer, as you said, without going repeatedly. We
20 would end up probably going to court very
21 frequently and very routinely.

22 As Raj indicated, the systems that we

1 have, we have to go back to court every 90 days as
2 it is and get the determination of the court that
3 what we're doing is warranted, and part of that
4 includes the relevancy and the value judgement
5 that allows the system to go forward.

6 MS. COLLINS COOK: Although just to be
7 clear, you would not have to go to court to use
8 national security letters.

9 MR. KELLEY: No, I'm sorry, that's
10 correct.

11 MS. COLLINS COOK: Which may be a
12 different reason not to use national security
13 letters, but just to be clear on that.

14 MR. WIEGMANN: So I think part of the
15 concern on that is that, one, it's a slower
16 process to issue NSLs and grand jury subpoenas,
17 and as Pat said, you have to do it repeatedly.

18 And then critically you'd have to do it
19 across providers. So if you have multiple
20 providers participating then you have to go to
21 provider A, and then if that number calls someone,
22 the number is for provider B then you have to

1 issue an NSL to provider B and C, and then you see
2 the networking. In other words, you're having to
3 do multiple.

4 And if those numbers are calling
5 numbers back again across the different data
6 streams from different providers it makes it
7 infinitely more complicated to start to try to do
8 NSLs or grand jury subpoenas to multiple different
9 providers for multiple hops. So I think that's
10 part of the reason why it's complicated.

11 In addition to the fact you said about
12 how long is the data to ensure as a legal matter
13 that it has to be retained. And again, I think
14 it's important to say that some of these providers
15 may retain the data voluntarily for a length of
16 time but without something like this order you
17 don't have a guarantee that they're going to keep
18 the data.

19 MR. MEDINE: Thank you.

20 Mr. Dempsey?

21 MR. DEMPSEY: Thanks, and good morning
22 again. Listening to the discussion about the RAS

1 and you know, thinking about Terry vs. Ohio, which
2 is the reasonable specific articulable facts
3 giving reason to believe, it seems to me there are
4 two issues there.

5 One of course is when you think about
6 it, that's the very standard the New York City
7 police has used in its stop and frisk program,
8 which is at the very least highly controversial
9 and a lot of people feel has ended up being
10 implemented in a discriminatory way. The police
11 in New York City would say, well, every single one
12 of those stops was based upon a RAS.

13 Secondly, in the police stop case it
14 seems to me that the good aspect of it and the bad
15 aspect of it is, is that the issue is resolved
16 immediately. Either the police find something and
17 they arrest you or they let you. Again, in New
18 York there was the humiliation of being stopped,
19 which is not nothing clearly, but it's resolved
20 immediately.

21 And it seems to me that you've picked
22 up the first half of Terry, specific and

1 articulable facts giving reason to believe, but
2 the second half of Terry was that some criminal
3 activity is afoot, that there's some suspicion of
4 criminal conduct which you resolve immediately
5 through the stop, which is the purpose of the
6 stop.

7 But here I'm wondering about the second
8 half, so specific and articulable facts giving
9 reason to believe, and then it seems to get vaguer
10 that the selector being used is associated with a
11 terrorist group and associated -- is there a way
12 to make that more concrete?

13 You cite the example of, well, we've
14 got a terrorist's computer and there were phone
15 numbers in it. Well, yeah, let's find out who
16 those phone numbers are calling and are any of
17 them in the United States.

18 But what else could associated with
19 mean? And then how can you give it more
20 concreteness so you avoid this problem?

21 Because it seems to me that you make
22 the determination and then the information is

1 tipped, so to speak, or given to the FBI to
2 pursue. And it's not the kind of thing that can
3 be so immediately resolved.

4 So I'm wondering even is the Terry
5 example the right reference point here, or is
6 there another way to define what you're looking
7 for? You know, reason to believe that a search of
8 the number will be likely to uncover somebody in
9 the United States who may be engaged in terrorist
10 activities for example, something more definitive
11 than this just associated with.

12 MR. LITT: So let me offer some
13 comments on that. The first is that I think
14 actually the comparisons to the police Terry stop
15 all run in favor of this program as a considerably
16 lesser intrusion. For one thing I think the
17 actual degree of intrusion based on the
18 determination is considerably less.

19 A Terry stop involves a policeman
20 stopping you and frisking you on the street, which
21 is by itself a considerably greater intrusion on a
22 person's privacy than simply running a telephone

1 number that's not associated with any individual
2 name against a bunch of other telephone numbers
3 that aren't associated with any individual name.

4 The second thing is that the
5 consequences that can flow from that are
6 considerably different. Obviously one of the
7 consequences that can flow from a police Terry
8 stop is an immediate arrest without any subsequent
9 review, without any intervening review or judicial
10 determination.

11 In this case the only consequence that
12 can flow is that a telephone number is tipped to
13 the FBI for further investigation, and that
14 further investigation requires independent legal
15 justification. And in particular if there's any
16 desire to intercept anybody's communications, any
17 American's communications, that requires a
18 judicial warrant based on probable cause.

19 The third difference I think is the
20 degree of oversight. As was mentioned before, to
21 my knowledge generally speaking there's no
22 systematic oversight by prosecutors and/or

1 inspectors general and/or others of day-to-day
2 determinations that lead to Terry stops by police.
3 That's one of the reasons why there's the
4 litigation in New York. As Raj has said at some
5 length, there is systematic oversight here.

6 So I think that all of those
7 determinations make this a considerably lesser
8 intrusion than the police Terry stop.

9 In terms of the possibility of an
10 alternate standard, obviously there are a number
11 of alternate standards that could be applied. But
12 the important thing to remember is that this
13 program is a discovery program.

14 The whole idea of this program is to
15 identify avenues that warrant investigation and to
16 rule out avenues that don't warrant investigation.
17 And the more you require, the more you add on to
18 the standard that's required before you can even
19 investigate, the less useful the tool becomes.

20 So for example, if you talk about
21 reason to believe that the number may lead to a
22 contact in the United States, well that's exactly

1 what we're trying to find out here. We've got a
2 number. If we've got a terrorist's phone number,
3 exactly what we're trying to find out is do we
4 have information to think that this may lead to
5 productive investigation in the United States.

6 MR. DEMPSEY: And just one quick thing
7 Raj, if I could. On the question of follow-up,
8 Pat or others, there's very close review of the
9 RAS determinations itself. What sort of review is
10 there of how does the FBI use the information that
11 is generated?

12 MR. KELLEY: Well, we use the
13 information, as Bob indicated, to further our
14 investigative efforts, so we can open a
15 preliminary investigation perhaps or we can open a
16 full investigation.

17 MR. DEMPSEY: But my question is, does
18 the, sort of review process go and look at what
19 was the outcome, how was it used, how did we
20 confront or not confront an individual? Sort of
21 tracing all the way down to the street or to the
22 FBI's follow-up investigation, what sort of

1 assessment or tracking is there of that?

2 MR. KELLEY: Well, I think what you're
3 referring to is our oversight and compliance
4 efforts. We have both internal and external up to
5 and through Congress, as well as the Department of
6 Justice, the Department of Justice Inspector
7 General, the Department of Justice Office of
8 Intelligence routinely do reviews and audits
9 internally.

10 From the street level, for example, the
11 investigative cases that we have are reviewed by
12 supervisors every 90 days to see what the status
13 is.

14 In addition to that, the FBI has an
15 Office of Integrity Compliance where we are
16 continuously looking at the risk that we will, in
17 executing our mission, not to follow the letter of
18 the law.

19 So through all of those internal and
20 external systems of oversight we are continuously
21 reviewing the way we conduct our business.

22 MR. DEMPSEY: Raj, you had a point?

1 MR. DE: I want to add one point. Just
2 to put a fine point on the comparison to the New
3 York controversy because I think at NSA we're
4 really worried about conflation of the public
5 record, so I just want to give folks a sense of
6 what using the Terry stop standard means here, the
7 comparison to a stop and frisk.

8 That would mean a police officer writes
9 down the reason for a stop and frisk, as we do for
10 telephone metadata, before they did that activity.

11 It would mean that only one of 22
12 supervisors would approve that stop and frisk
13 before it happened.

14 It would mean that, in our case, the
15 data is all anonymous, as opposed to a stop and
16 frisk where have a physical human being, Bob was
17 alluding to that point, in front of you.

18 The stop and frisk standard, we have
19 post-query audits every 90 days, so that would
20 mean a police department audits every 90 days what
21 happened.

22 And we also report to a court every 30

1 days and get it re-authorized every 90 days.

2 So while, yes, in some legal sense the
3 standard, the legal standard derives from the
4 Terry stop standard, I think just those factors
5 alone distinguish the use of that standard in this
6 context and clearly evidence that it's a far, far
7 more regulated and rigorous process than is
8 feasible in the physical search context.

9 MR. DEMPSEY: Thank you.

10 Judge Wald?

11 MS. WALD: Thank you. I'm going to
12 open with a kind of a general question. Since the
13 revelation of the 215 program, which was a secret
14 program before, there have been, as you well know,
15 a plethora of suggested reforms, quote, reforms,
16 or suggested changes, etcetera.

17 I'm interested in whether or not you
18 think any of these suggested reforms that you're
19 aware of deserve, not just serious consideration,
20 but perhaps adoption.

21 Let me just give you sort of an
22 example. It was a secret program, it's now no

1 longer the fact of the program and many of its
2 operational details that the government has
3 revealed, are no longer secret.

4 Now I assume from the fact that you're
5 here today and from many of your answers that you
6 think that the program deserves to be continued.
7 So there are two parts to my question.

8 You know, one is whether or not any of
9 the reforms suggested by various people that you
10 think are worthy of consideration, or two, do you
11 think the fact that you want the program to
12 continue could cast some doubt on the need for
13 secrecy of the fact of the program to begin with,
14 which of course is one of the big questions being
15 debated, whether or not when you have a bulk
16 collection program of any kind that affects a lot
17 of citizens, a lot of residents, the fact of that
18 program, if not all the details of its operation,
19 deserve to be debated publicly in Congress and
20 known to the public?

21 It's kind of a double-barreled
22 question. I'll let anybody that wants to.

1 MR. LITT: I'd like to take a crack at
2 that, but first I have a personal favor to ask and
3 that is if Jim Dempsey could turn his tent a
4 little because the floodlight is shining. Thank
5 you very much. I'm getting blinded by it.

6 So to answer your second question first
7 about secrecy, I don't think you can draw from the
8 fact that we want the program to continue the
9 conclusion that the program should never have been
10 secret.

11 There are many intelligence programs
12 that operate more effectively when they're not
13 known because disclosure of what we obtain and how
14 we obtain it can enable our adversaries to avoid
15 or take steps to avoid what we're doing.

16 That said, that doesn't mean that once
17 they've been disclosed they're entirely
18 ineffective. There's no question in my mind that
19 this program is at least potentially less useful
20 now than it would have been before disclosure.
21 Whether it's actually less useful or not is going
22 to take time to determine.

1 But going forward obviously we have
2 declassified and released the last two orders of
3 the FISA Court and we are obviously under the
4 President's direction in a more forward leaning
5 mode with respect to transparency.

6 But we still, as sort of custodians of
7 the intelligence apparatus that protects the
8 nation, we still have to be sensitive all the time
9 to the fact that disclosures do risk compromising
10 our capabilities.

11 With respect to your first question, I
12 think that we have repeatedly said that we're open
13 to consideration of a variety of possible reforms
14 to the program, so long as they don't eliminate
15 its utility.

16 We've talked about shorter retention
17 periods. We've talked about possible limitations
18 of the number of hops that we can make queries
19 out. We've talked about some sort of process for
20 after the fact review of RAS determinations by the
21 FISC. We've talked about providing greater
22 transparency as to the manner and the extent to

1 which the program is used.

2 All of these are subject, again, to the
3 qualification that we don't want to impose such
4 restrictions, that they would eliminate the
5 utility of the program. And we don't want to
6 impose on ourselves burdens that we can't meet.
7 Some of the transparency proposals are things that
8 we simply can't do with any reasonable
9 effectiveness, so.

10 MS. WALD: But to follow-up a little
11 bit on that, there have been some articles
12 recently in the paper, and I think they contain
13 some polls, I know there are lots of polls, but
14 suggesting that there's widespread public distrust
15 of NSA as a result of many of the revelations over
16 the last several weeks.

17 Do you think that there's some need for
18 some, whatever you want to call it, remedial
19 effects, making changes, some more types of public
20 disclosure?

21 For instance one, you've suggested that
22 there may be, but one area that's covered in some

1 of the bill in Congress is that need for a more, I
2 think the word used is secure foundation for the
3 215 program and specific, legislative. I know
4 it's been re-authorized, but in a specific
5 legislative acknowledgment of that program.

6 There's certainly been a fair amount of
7 confusion and some criticism of the fact that if
8 you read 215, the public records bill, on its
9 face, you don't get much notion that this might be
10 involved, etcetera. And so as you know, some of
11 the efforts are said to put it on a sound specific
12 legislative basis that everybody knows what you're
13 going to do or that there is such a program,
14 etcetera. What are your feelings about that?

15 MR. DE: Can I speak to the first
16 point, Judge, which I think --

17 MS. WALD: Yeah, sure.

18 MR. DE: Is a very valid point. So you
19 know, as the General Counsel for NSA my first duty
20 to is to make sure that our activities are lawful.

21 But I view my role and all of the
22 senior officials at NSA to ensure the extent

1 possible given the nature of our work, the public
2 legitimacy of what our agency does. There is no
3 doubt that is an important factor.

4 That being said, I think this
5 particular program had historically all the
6 indicia of institutional legitimacy that one could
7 expect given the current setup of the FISC and
8 institutional oversight that we have.

9 So in other words, and some of this is
10 obviously known to you all but just to make sure
11 members of the public are aware, not only was this
12 program approved by the Foreign Intelligence
13 Surveillance Court every 90 days, it was twice,
14 the particular provision was twice re-authorized
15 by Congress with full information from the
16 Executive Branch about the use of the provision.

17 Now as to whether that should be
18 codified separately or not as a confidence
19 building measure, for all intents and purposes I
20 think the public debate we're having now
21 effectuates the public legitimacy aspect of the
22 program, and we'll see how it plays out and how

1 the reform measures are taken.

2 But I don't think a separate
3 codification is necessary for the legal legitimacy
4 of the program but I think your point is well
5 taken that public confidence needs to be ensured.
6 I would only suggest that to the extent public
7 confidence is shaken, in part that is as a result
8 of historical secrecy and in part it's a result of
9 a large amount of misinformation and confused
10 public debate. And it's hard to separate the two.
11 Those are two, they're intermingled of course.
12 And so I think it's the former that is certainly
13 necessary for a democratic institution to
14 continue.

15 MS. WALD: So if there were another --
16 I'm sorry, go ahead.

17 MR. LITT: I just want to add one very
18 brief comment to Raj's in terms of the extent to
19 which Congress was kept informed. By statute
20 we're required to provide copies of significant
21 opinion and decisions of the FISC to the
22 Intelligence and Judiciary Committees of both

1 Houses of Congress and they got the materials
2 relating to this program, as we were required to
3 by law.

4 MS. WALD: So last question on my last
5 minute. If there were, if there were another bulk
6 data, metadata program type to come along, based
7 on your experience with this, all that's happened
8 with 215, do you think it would be desirable,
9 undesirable for it to become a matter of public
10 knowledge and open discussion in Congress? Not
11 the details of the program but that there was to
12 be a bulk program which would affect a large
13 amount of the citizenry?

14 MR. LITT: So I think that really very
15 much depends upon the nature of the program and
16 what it is.

17 I think if the nature of it can be
18 disclosed without compromising intelligence
19 sources and methods, then that's something that
20 would be considered.

21 But if the public discussion is going
22 to lead to a considerably disclosure of sources

1 and methods, I don't see how we can do that. This
2 is why the Intelligence Committees of Congress are
3 set up. This is why we're required to notify the
4 Intelligence and Judiciary Committees of things
5 that we do pursuant to FISA because they
6 essentially stand as the proxies for the people in
7 overseeing sensitive intelligence collection
8 programs.

9 MR. MEDINE: I guess we'll turn to the
10 subject of oversight of the program. As I
11 understand it there is judicial approval of the
12 program itself but there is not judicial approval
13 of the selection of particular phone numbers, the
14 RAS determination, reasonable articulable
15 suspicion, either before, nor is the court
16 afterwards apprized of what selectors have been
17 chosen so that they can evaluate whether the
18 program is operating consistent with the
19 authorization for the program itself.

20 Would it be practical, assuming that
21 there was an exception for exigent circumstances,
22 where there was an urgent need to pursue a

1 particular phone number with perhaps after the
2 fact reporting, would it be practical with that
3 exception for the court to approve the RAS
4 determination in advance or to review RAS
5 determinations after the fact, perhaps as part of
6 the 90 day review process and approval process, to
7 make sure the program is operating as the court
8 expected it to be operating.

9 MR. DE: So we are, we're certainly
10 open to an increased role for the FISC, I think.
11 And the same, in particular I know ODNI and other
12 agencies feel the same.

13 I'd make a couple of points. One, I
14 think among the criteria that are necessary to
15 maintain the usefulness of the program, we've
16 heard a variety of things this morning. We tend
17 to summarize them in sort of four kind of major
18 buckets.

19 One is maintaining privacy protections.
20 We hit on that earlier. One is maintaining the
21 comprehensiveness of the data. The third is
22 maintaining the depth of the data, the number of

1 years you keep it. And the fourth is operational
2 agility, getting to the question you've just
3 raised.

4 I think we have concern that it will be
5 difficult and not practical to preserve the
6 operational agility of the program, to have
7 ex-ante approval by a court for every RAS
8 determination.

9 But I think you've raised a very
10 valuable point that we currently have reporting
11 requirements to the FISC, and in fact we report to
12 the FISC every 30 days in fact, even though the
13 program is authorized every 90 days. And so that
14 30 day vehicle could well be a useful vehicle to
15 provide RAS determinations to the FISC, for it to
16 review the documented determinations that are made
17 today.

18 I'd just note that those
19 determinations, and Brad mentioned this earlier,
20 are currently reviewed by the Justice Department.
21 But to the extent it builds public confidence I
22 think it would be of no concern for NSA in

1 particular to have the FISC review those after the
2 fact.

3 MR. LITT: One concern that we have
4 actually talked about in our own internal
5 discussions with the idea you articulated of
6 ex-ante review with an emergency exception is that
7 given that the nature of this program is such that
8 we're frequently operating in exigent circumstance
9 we'd be a little uncomfortable with a scheme
10 that's set up where the statutory exception
11 essentially swallows the statutory rule.

12 MR. MEDINE: And what about after the
13 fact? The court has, I think indicated publicly
14 that it's difficult for the court to assess
15 compliance with its own orders. What if there's a
16 mechanism for every 30 days to report back on the
17 RAS determinations that were made so it wouldn't
18 interfere with operational concerns but it would
19 give the court the chance to, say, correct
20 direction if you're exceeding the court's
21 expectations or give validation if you are
22 squarely within what the court expected you to be

1 doing?

2 MR. LITT: I think that that's
3 something we're very open to, to considering.
4 Obviously all of these things, it depends upon
5 what exactly the proposal is, but I think that in
6 concept that's something that we would be
7 comfortable with.

8 MR. WIEGMANN: We also have to keep in
9 mind the burdens on the court as well and what
10 their resources are to do that. But for the
11 reasons that Raj and Bob explained, I agree that
12 post, ex-post review of RAS is an idea worth
13 considering.

14 MR. MEDINE: I want to shift to the 702
15 program briefly, which is the electronic
16 communication service provider program. As we
17 know, over the last couple of weeks there's been a
18 lot of concern by non-U.S. persons, foreign
19 citizens about being subject to surveillance.

20 What are your thoughts about whether,
21 that this program essentially is designed to focus
22 on the rights of U.S. persons being surveilled and

1 court approval for U.S. citizen? What do you
2 think about extending some degree of protection to
3 non-U.S. persons who are being, whose
4 communications are being reviewed pursuant to the
5 702 program?

6 MR. DE: So I think maybe I can start
7 and then you can speak. Just as a general matter,
8 one, there is in fact for all of our collection a
9 policy process in place, an interagency process to
10 determine that for which we conduct foreign
11 intelligence generally.

12 And so I would like to make sure folks
13 don't have the misimpression that intelligence
14 gathering is not directed in the first instance.

15 Secondly, all collection has to be
16 related to an authorized FI purpose. That
17 includes our 12333 collection.

18 And our 702 collection in particular
19 has to be conducted pursuant to certain
20 certifications that are submitted to the court for
21 particular foreign intelligence purposes.

22 The third point I'd make is that even

1 though we have a number of protections in place
2 for U.S. person, information beneficiaries of that
3 also are foreign nationals who may be subjects of
4 investigation. So in other words, our retention
5 limits and other protections that are currently in
6 place in fact serve as protections for any subject
7 of intelligence collection.

8 And then fourth, I know the DNI is
9 currently considering whether we want to document
10 any further protections for non-U.S. persons
11 beyond those that are articulated today.

12 MR. LITT: So if I can just follow on,
13 there is I think a good reason why not only the
14 United States but most nations provide a greater
15 degree of protection for their own citizens and
16 nationals and others with respect to intelligence
17 activities.

18 Historically the great fear of
19 intelligence agencies has been that like the
20 example everybody always gives of the Stasi, that
21 their powers will be directed inappropriately
22 towards repression of their own citizenry. And I

1 think that's why historically in this country we
2 have a greater degree of protection for U.S.
3 persons, but as Raj says that doesn't mean that
4 there are no protections for other persons.

5 In that regard I think it's worth
6 noting the letter that the NSA Inspector General
7 sent to, I believe it was Senator Grassley a month
8 or six weeks ago, which has now been released
9 publicly, which identified a dozen or so instances
10 in which they had determined that NSA personnel
11 had inappropriately used collection authorities.

12 And I believe that the majority of
13 these involved -- first of all, they were all
14 under Executive Order 12333. None of them were
15 under FISA. There's never been a finding of a
16 willful violation of FISA.

17 But even in this case the majority of
18 these were improper queries of information about
19 non-U.S. persons. And so it's not only the fact
20 that we have rules that protect non-U.S. persons
21 but those rules are actually enforced. These
22 people were disciplined or resigned from NSA as a

1 result of this.

2 And I would just reiterate what Raj
3 said, which is that we are open to considering
4 whether there's some value in formalizing and
5 making more public the rules that we do have for
6 protecting the personal information about non-U.S.
7 persons.

8 MR. MEDINE: And so turning to the
9 protections for U.S. persons, as I understand it
10 under the 702 program when you may target a
11 non-U.S. person overseas you may capture
12 communications where a U.S. person in the United
13 States is on the other end of the communication.

14 Would you be open to a warrant
15 requirement for searching that data when your
16 focus is on the U.S. person on the theory that
17 they would be entitled to Fourth Amendment rights
18 for the search of information about that U.S.
19 person?

20 MR. DE: Do you want me to take this?

21 MR. LITT: Thanks, Raj. Raj is always
22 easy, he raises his hands for all the easy ones.

1 MR. DE: I can speak for NSA but this
2 obviously has implications beyond just NSA as
3 well.

4 MR. LITT: I think that's really an
5 unusual and extraordinary step to take with
6 respect to information that has been lawfully
7 required.

8 I mean I started out as a prosecutor.
9 There were all sorts of circumstances in which
10 information is lawfully acquired that relates to
11 persons who are not the subject of investigations.
12 You can be overheard on a Title III wiretap, you
13 can overheard on a Title I FISA wiretap.
14 Somebody's computer can be seized and there may be
15 information about you on it.

16 The general rule and premise has been
17 that information that's lawfully acquired can be
18 used by the government in the proper exercise of
19 authorities.

20 Now we do have rules that limit our
21 ability to collect, retain and disseminate
22 information about U.S. persons. Those rules, as

1 you know, are fairly detailed. But generally
2 speaking, we can't do that except for foreign
3 intelligence purposes, or when there's evidence of
4 a crime, or so on and so forth.

5 But what we can't do under Section 702
6 is go out and affirmatively use the collection
7 authority for the purpose of getting information
8 about U.S. persons.

9 Once we have that information I don't
10 think it makes sense to say, you know, a year
11 later if something comes up we need to go back and
12 get a warrant to search that information.

13 MR. MEDINE: One last question on this
14 round, which is that under 702, as I understand
15 it, you can collect information about a target
16 rather than to or from the target, and some
17 concerns have been raised about the breadth of
18 that, the scope of that authority.

19 What impact would there be if that was
20 narrowed to limiting targeting of communications
21 to or from the person that's about this person of
22 interest?

1 MR. DE: Let me make a couple of
2 general points. One, I think a balanced
3 collection, just speaking at the most general
4 level, is helpful from a discovery standpoint.
5 And it's hard to articulate more in an open
6 setting exactly how that collection is useful.
7 But it has uses beyond that of to or from
8 collection.

9 I'd say a couple of points in terms of
10 the privacy protections around a balanced
11 collection. The data that comes in, in that way,
12 and it's hard to get more specific, is treated
13 differently than other data, and in fact has a
14 shorter retention period. So there are procedures
15 in place that are intended to account for the
16 greater privacy impact of a balanced collection.
17 And those procedures have been approved by the
18 FISC.

19 MR. MEDINE: Thank you.

20 Ms. Brand?

21 MS. BRAND: Thank you. I want to
22 follow-up on a couple of things that have been

1 raised before, I'm going back to 215 now.

2 Bob, you said there were certain, in
3 response to Pat's question about what proposals
4 the administration could accept, you said there
5 are certain transparency proposals that we just
6 couldn't do. What ones are those?

7 MR. LITT: Well, in the absence of
8 interagency clearance and OMB approval I'm
9 reluctant to state official administration
10 positions on any particular proposals.

11 MS. BRAND: What ones do you think we
12 can do?

13 MR. LITT: I do think that proposals,
14 for example, that require us to count things that
15 we aren't now counting and that might be difficult
16 to count present problems for us.

17 For example, I don't know if there is
18 such a proposal, but if there were a proposal, for
19 example, that says tell us the number of U.S.
20 person telephone numbers that have been acquired
21 every 90 days pursuant to this, that might be a
22 very difficult thing for us to accomplish because

1 we don't go out and count that.

2 So things that impose substantial
3 burdens on us like that might be the sort of thing
4 that would present problems for us. And again,
5 I'm not speaking with respect to any specific
6 proposal but that's the kind of consideration that
7 we would take into account.

8 MS. BRAND: Okay. I'm going to come
9 back and --

10 MR. KELLEY: I have a point on that.
11 Again, not talking or addressing any specific
12 proposal, but if we were required to for a
13 particular service provider, carrier,
14 telecommunication provider to disclose the number
15 of orders that were served on them, that would
16 give our adversaries a very good indicator,
17 perhaps depending on the relative numbers, whether
18 to use that service provider or not use that
19 service provider.

20 The adversaries are listening just as
21 we all are to this discussion so that kind of
22 specificity is very, very difficult for us to

1 accept.

2 MR. DE: If I may add to that. One
3 thing which presumably the panel is aware of, the
4 DNI has announced a proactive transparency measure
5 which is an annual report of the number of orders
6 issued under various provisions of FISA and the
7 numbers of targets affected.

8 And so I think what you're seeing is
9 the Executive Branch trying to the extent possible
10 to take the proactive steps towards transparency
11 that can be taken consistent with operational
12 effectiveness. And so that report would delineate
13 the number of orders and targets affected for FISA
14 orders that are based, premised on probable cause,
15 FISA orders under Section 215, orders under
16 Section 702 of FISA and so forth.

17 MS. BRAND: Okay. And I want to come
18 back to FISA or transparency, especially in the
19 FISC context if I have time, but I did want to
20 follow-up on the discussion about a return
21 requirement on RAS selectors to the FISC.

22 That sounds like a good idea in the

1 abstract but I'm a little unclear about what
2 exactly it would add in practical reality.

3 What exactly would the court do with
4 it? I mean I presume the way it would work, I
5 guess, is on a regular basis, 30 days for example,
6 you would provide a list of RAS selectors to the
7 court, along with some documentation. I'd be
8 interested to hear what that documentation would
9 be. What would the court do with that
10 information?

11 MR. DE: I'll defer to Brad on the
12 second part of that, but in terms of the
13 documentation itself, today we keep the
14 documentation of the factual basis that
15 established the predicate for the query in the
16 first place.

17 And so at least from NSA's perspective
18 we keep that sort of documentation and it wouldn't
19 be a great burden to provide it to another
20 oversight mechanism.

21 But as to how the FISC would handle
22 that, I'll defer to Brad who, the Justice

1 Department represents us all obviously before the
2 FISC.

3 MR. WIEGMANN: One option would be all
4 those RAS determinations and if it found
5 compliance problems on its own, then it could call
6 in the government and say I'm not comfortable with
7 how the program is being implemented. And so --

8 MS. BRAND: Can I just, I think there's
9 something wrong with Brad's microphone. I'm not
10 sure what we can do about that.

11 MR. WIEGMANN: I got a new one. Is
12 this better?

13 MS. BRAND: Yes, thank you.

14 MR. WIEGMANN: So in other words, it
15 could function much like current. Right now if
16 the Justice Department identifies problems with
17 RAS determinations we report those to the court
18 and information could be purged. The court could
19 respond if we have a compliance incident and order
20 relief. They could suspend the operation of the
21 order, suspend the program. They could take
22 whatever remedial steps that they thought were

1 appropriate in order to enforce the requirements
2 of the order.

3 So this could be the same mechanism,
4 except that it would, the Justice Department
5 wouldn't necessarily be the intermediary in
6 between --

7 MS. BRAND: I guess I'm wondering --

8 MR. WIEGMANN: Rather than us reporting
9 the compliance then the court could on its own
10 independently review the RAS determinations.

11 MS. BRAND: Well, that's what I'm
12 getting at. I'm not asking exactly about what the
13 court would do if it found a compliance problem,
14 but how the court would figure out if there is a
15 compliance problem, if you would expect them to be
16 literally looking at every RAS selector and
17 assessing whether the evidence justified the
18 determination or what?

19 MR. LITT: So I think it's important to
20 remember that in the last year there were 288 RAS
21 selectors, so we're not talking about thousands
22 and thousands.

1 But somebody, I think it was the
2 chairman, may have mentioned the idea of having
3 some sort of outside assessment of are we in fact
4 applying the RAS standard appropriately.

5 And it seems to me that a judge could
6 look at, in the same way that judges review the
7 validity of Terry stops by police, was this
8 information sufficient to form a reasonable and
9 articulable suspicion to support a stop and frisk,
10 a judge could look at the documentation that NSA
11 has and say, are you setting the line in the right
12 place? Are your people, do your people in fact
13 understand what the RAS standard is and are they
14 applying it appropriately?

15 And if a judge felt that they were
16 either being, setting too high a standard or too
17 low a standard the judge could provide that
18 feedback, along with whatever remedial measures
19 Congress deemed were appropriate.

20 MS. BRAND: And is that, just stop me
21 and tell me if we need to talk about this in a
22 different setting. But in the analogous return

1 requirement in Section 105 of FISA for multi-point
2 wiretaps, is that what the court does with
3 information returned to it under that provision?

4 MR. WIEGMANN: I'd have to get back to
5 you on that.

6 MS. BRAND: Okay. If you would get
7 back to me on that, that would be great. That's
8 something I've been wondering about.

9 I wanted to ask you about a provision
10 in the Leahy bill which would change the standard
11 under 215. As I understand it, that first it
12 would add the words material, so relevant and
13 material to a FISA investigation. And then it
14 would limit 215 to being used to seek information
15 that pertains to a foreign power or agent of a
16 foreign power, activities of a suspected agent of
17 a foreign power who's under investigation, or
18 someone in contact with or known to a suspected
19 agent of a foreign power.

20 So you may not have an official
21 administration position on this provision yet but
22 I'd like to ask you about it anyway, and answer it

1 to the extent that you can. First of all, what do
2 the words and material add? What would the court
3 do with that?

4 MR. LITT: I had the same question as I
5 read this bill over the weekend. I'm not sure
6 what the intent is. I think you'd have to ask the
7 chairman.

8 I think the obvious intent is to try
9 to, I think it's no secret that the sponsors of
10 this bill want to eliminate the bulk collection
11 program and I think that the intent of the
12 language that they're proposing is to prevent bulk
13 collection. How it accomplishes that, I'm not
14 entirely sure.

15 MS. BRAND: Do you have a sense of what
16 evidence you present to the court to establish
17 materiality that's additional to or different from
18 what establishes relevance, any of you?

19 MR. WIEGMANN: I don't. I mean I'm not
20 sure how it would be different.

21 MS. BRAND: And then can you address
22 the other limitation, sort of three categories of

1 information that would be allowed and how that
2 would practically impact investigations since this
3 would be no longer like the current 215, which is
4 sort of a general subpoena authority under FISA?

5 MR. LITT: So I think that the purpose
6 of this pertain to language is -- I believe that
7 the intent is to try to ensure that queries, that
8 business records can only be obtained with respect
9 to identifying individuals. I think that's what
10 their intention is here. And for the reasons
11 we've previously discussed, that would essentially
12 shut down the program.

13 MS. BRAND: How would it affect though
14 individual, sort of run of the mill, 215 orders,
15 or would it? I mean is your opinion that it
16 affects only bulk collection or would it affect
17 your everyday 215 application?

18 MR. KELLEY: Well, I think that from
19 our perspective the proposal is flawed in the
20 sense that it has the assumption or presumption
21 that we know the person that we're after, and
22 that's the essence of the terrorism prevention is

1 we don't know who we're after. So if we are
2 limited to seeking numbers from a known, then
3 we're not going to be very effective.

4 Again, it bears repeating that we're
5 connecting the dots here, so the fewer dots that
6 we have the fewer connections we will make. So
7 again, I don't think that model works.

8 I think given the type of data that
9 we're talking about that is susceptible to
10 analytical connectivity, unlike other types of
11 business records, then we need large volumes of
12 that data in order to make those connections.

13 So whether we are changing the standard
14 from relevant to relevant and material, or saying
15 that there must be a connection to someone who's
16 known, you are reducing the amount of data
17 available and therefore making it much more
18 difficult to make the connections that we need to
19 make.

20 MR. WIEGMANN: Just to add to that, I
21 think it is important to recognize that those
22 changes would apply not only to the bulk

1 collection but to regular 215 orders.

2 I mean people are forgetting, because
3 this is the authority used in the bulk context,
4 that the predominant use of the authority is to
5 obtain individual records in a more targeted way
6 and this would essentially change the standard to
7 closer to the pre-PATRIOT Act standard.

8 So rather than a broader relevance
9 standard, which gives you more of the flexibility
10 that Pat was talking about, in your ordinary case
11 where, let's say you want to get hotel records, or
12 car rental records, or whatever that might be
13 relevant to your investigation, you'd have to meet
14 that higher showing in order to get those regular
15 records that are more targeted in an
16 investigation.

17 So it would have a kind of collateral
18 impact on ordinary 215 orders that have nothing to
19 do with the activities that are the current
20 subject of controversy.

21 MS. COLLINS COOK: Thank you. Raj,
22 going back to what you were talking about that the

1 administration is going to be disclosing in terms
2 of the types of requests by, I think you said
3 target, which I understand in the electronic
4 surveillance context where the statute explicitly
5 talks about targets of surveillance. What does
6 that mean for Section 215?

7 MR. DE: So right now the DNI is
8 leading a process to figure out how we can best
9 articulate that language in a way that's
10 meaningful to the public, because obviously in the
11 context of 215, we would have one order but it
12 involves quite a significant amount of records.
13 We would want to make sure we provide some
14 information that's useful, and in fact transparent
15 in some way.

16 And the same sort of analysis is
17 happening now with respect to Section 702 as well.
18 What's the best means to provide insight into
19 orders and targets affected but at the same time
20 preserve the sort of national security needs we
21 need too. So that process is underway and the DNI
22 is leading that.

1 MS. COLLINS COOK: I also wanted to
2 follow-up, there's been a lot of discussion about
3 the ability of private sector, I will call them
4 partners and their ability to disclose on a
5 company by company basis their cooperation with
6 the government.

7 Do you think that there are proposals
8 out there that would allow company by company
9 disclosures that would be advisable or feasible?

10 MR. LITT: So first of all, this is a
11 matter that's currently in litigation. As you
12 know, there are papers that have been filed
13 articulating positions of the companies and of the
14 government on this.

15 MS. COLLINS COOK: Sure. Putting aside
16 whether or not it's permissible under the current
17 regime, whether there could be a statutory regime
18 that would be advisable or feasible.

19 MR. LITT: So again, I think the point
20 is that we, the proposals that we've articulated
21 would allow on the one hand a government -- for
22 the public to know on the one hand on a

1 government-wide basis how often various
2 authorities are used.

3 And number two, on a company by company
4 basis how often they are turning over information
5 about their subscribers to the government.

6 Where we start to have a problem is, as
7 Pat said, when you allow the companies to
8 breakdown on an authority by authority basis what
9 they're providing, because that starts to give a
10 lot more granularity about what our capabilities
11 are against particular platforms, given the kinds
12 of authorities that we are exercising.

13 If all of a sudden a company that has
14 not had a large number of Title I FISAs all of a
15 sudden has a spike in Title I FISAs, that's
16 something that's going to be noticed by our
17 adversaries and may lead them to shift away from
18 that provider.

19 I think the flip side of that is from
20 the viewpoint of public transparency what's
21 important to the subscribers is to know how often
22 is the government going to get my information.

1 And in particular I think frankly from our
2 perspective how rarely it happens compared to the
3 overall number of subscribers, that the number of
4 subscribers of these services, the percentage
5 whose information is provided to the government is
6 a minuscule fraction, even when you take into
7 account all of the government authorities
8 together.

9 So the overriding concern we have is
10 not having this information broken down at a level
11 of detail that would enable people to avoid
12 surveillance.

13 MS. COLLINS COOK: So following up on a
14 couple of questions that came up in the first
15 round. There are now a fair number of proposals
16 and discussions about alternative means for
17 accomplishing the Section 215 program or something
18 approaching that program.

19 My question to you is, how often do you
20 assess alternate means during the course of a
21 program?

22 So absent the public disclosures,

1 absent the need to opine on legislative proposals,
2 how often are you internally considering ways to
3 do programs through means which might raise fewer
4 privacy concerns?

5 MR. DE: So let me speak first to that.
6 I think there's a very valid and reasonable
7 question of the intelligence community generally
8 and to NSA in particular as to how often programs
9 are reevaluated and on what sort of rigorous
10 schedule does that happen.

11 As I mentioned earlier there's some
12 natural points at which that happens, whether it
13 is in the context of renewals of authorities,
14 whether it's in the context of congressional
15 re-authorizations, whether it's in the context of
16 budget decisions that need to be made.

17 And frankly, in a place like NSA, it
18 happens every day in the context of normal work
19 assessments. As to whether there should be a more
20 focused process for periodic reevaluations of
21 assessment of reporting requirements, I think
22 that's something we should be thinking about.

1 MS. COLLINS COOK: So following up on
2 something that Pat had asked earlier and one of
3 the themes and one of the themes that she was
4 hitting, do you think that this discussion today
5 and the amount of information that is currently
6 publicly available about the Section 215 program
7 is predictive of our ability to have a similar
8 conversation about other programs, whether they
9 are current or future?

10 And that's probably to Brad or to Bob.

11 MR. LITT: I guess I'm not sure I
12 understand the question.

13 MS. COLLINS COOK: I think we've heard
14 a few times that the fact that we're having this
15 hearing or the fact that the government's legal
16 rationale has now been made public, that certain
17 FISC orders and accompanying materials have been
18 made public demonstrates that we could have this
19 type of discussion about any range of programs,
20 whether current or future. Do you think that that
21 position is logical or correct?

22 MR. LITT: So I can start by recounting

1 the story that may or may not be apocryphal about
2 Zhou Enlai, who reportedly was asked what he
3 thought about the French Revolution and his answer
4 was, it's too soon to tell.

5 And I think that's very true here.
6 It's too soon to tell really what the effect of
7 these disclosures is going to be. In the
8 intelligence community we are always looking at
9 risks. What's the risk that if this comes out
10 into the public there is going to be damage?

11 And it's unquestionably and irrefutably
12 true that if information about how we collect
13 intelligence becomes public, it provides an
14 opportunity for our adversaries to avoid that.
15 Will they take advantage of that? We'll only know
16 over an extended period of time whether that's the
17 case or not. I mean we may never know for
18 certain. We may only see certain kinds of
19 information dry up without having somebody post a
20 sign that says, we are no longer doing this
21 because we know the United States can collect
22 this.

1 MR. KELLEY: I'll just follow up. In
2 the FBI, if you've been to FBI headquarters, as I
3 know you have, if you looked in the courtyard
4 there's a saying on the wall there that says the
5 most effective weapon against crime, including
6 terrorism is cooperation, cooperation of the
7 public.

8 We rely on the public. We want the
9 public. We need the public. It's our FBI but
10 it's their FBI as well. It's important for us
11 therefore to be sure that we understand where the
12 lines are and we want to go right up to the line
13 but we don't want to cross the line.

14 So the debate is helpful but at the
15 same time, as Bob has indicated, we have a process
16 in place for that debate. All three branches of
17 government have looked at the 215 program and have
18 said it was okay.

19 It took an unauthorized disclosure to
20 bring about this discussion, and we don't fear the
21 discussion. We think that the American public is
22 somebody we'd like to have a discussion about.

1 But it's the adversaries that we're concerned
2 about, because for every disclosure that the
3 public has, the American public has, our
4 adversaries have it as well.

5 So if we can stick within the
6 established channels to have that discussion to
7 protect the things that need to be secret, then I
8 think institutionally and individually we're
9 better off.

10 MR. DE: If I can add I think to your
11 question though as to the logical syllogism that
12 we're having this debate and discussion today does
13 that mean that the program never should have been
14 classified, clearly that's not true for the
15 reasons Bob articulated. We don't know the harms
16 yet and there may be harm happening today.

17 But given the disclosure happened and
18 the harms that will be effectuated are being
19 effectuated, I think what you're seeing is an
20 effort by the Executive Branch to try to be as
21 transparent as possible under the circumstances.

22 And to that point I think it's

1 certainly possible to think that greater public
2 discourse about intelligence matters is a good
3 thing without thinking that it took an illegal act
4 to expose lawful programs in and of itself was a
5 good thing.

6 MS. COLLINS COOK: One final question,
7 Raj, for you in this round. You had referred to
8 minimization procedures and they're traditionally
9 collection, retention and dissemination use.

10 Can you give an example of a collection
11 minimization requirement? I think that's
12 something that, you know, you look to the typical
13 Title III context and traditionally folks stopped
14 listening when you heard someone who wasn't the
15 target, you took the headphones off, and how that
16 translates into the national security context.

17 MR. DE: Let me try to address it in a
18 little bit more of a general sense and perhaps in
19 a classified setting we can get into the more
20 technical details.

21 I think here we're talking about where
22 collection is directed, how collection is

1 directed, the technical means by which it's
2 effectuated. There are a range of mechanisms in
3 order to minimize to the extent possible, minimize
4 the incidental collection of U.S. person
5 information on the front end as much as feasible
6 given the national security imperative of doing
7 the collection in the first place.

8 And then there are, we take, as you
9 alluded to, we take those steps that are the steps
10 possible at every stage in the process, not just
11 collection, but during use of information,
12 analysis, dissemination and retention of
13 information.

14 MR. LITT: If I can just add another
15 sort of conceptual type of minimization procedure
16 at the collection end in this regard is that in a
17 number of areas there are heightened requirements
18 of approval and legal review before collection can
19 be undertaken against U.S. persons.

20 MR. MEDINE: Mr. Dempsey?

21 MR. DEMPSEY: Thanks. I had a question
22 about the relationship between the government and

1 the communication service providers, particularly
2 in the sort of world of globalized information
3 services and American companies providing services
4 to people around the world.

5 Do you agree that it's important that
6 there be an arms length relationship between the
7 government and the service providers and that
8 there be a perception, that there be a reality of
9 an arms length relationship and that there be a
10 perception of an arms length relationship?

11 MR. DE: Yes.

12 MR. DEMPSEY: I've seen reference to
13 the NSA referring to corporations as its partners,
14 service providers as its partners, presumably
15 partners in surveillance.

16 Doesn't that undermine the perception
17 of an arms length relationship, referring to
18 corporations as the government's partners? Can
19 you see how that would be miss or interpreted
20 suggesting a close relationship?

21 MR. DE: I think this question probably
22 evinces the problem with selective and misleading

1 disclosures generally because certainly I review a
2 lot as the general counsel at NSA. I don't want
3 to review every PowerPoint. I don't review every
4 single employee's articulation of things.

5 I think the term partnership is
6 probably one that's used across government in a
7 variety of contexts. And so I take your point
8 that one wouldn't want to leave the public with
9 the misimpression that there isn't an arms length
10 relationship between any private entity and any
11 government entity.

12 On the other hand, I think I would
13 caution folks reading too much into particular use
14 of words in any given PowerPoint or whatever was
15 at the basis of your question.

16 MR. DEMPSEY: Under the 215 program
17 there's this thing referred to in the opinions as
18 the corporate store. So searches are run with the
19 RAS selectors, and as I understand it, the tree of
20 data that results from that goes into the
21 so-called corporate store where it's not subject
22 to the limitations that you've discussed today.

1 In terms of searching it, can it be now searched
2 without limitations.

3 Is there any quantification or could
4 there be a quantification of how much data is in
5 that corporate store?

6 MR. DE: I might have to take that for
7 the record and get back to you. I'm just probably
8 not prepared to speak to it today.

9 MR. DEMPSEY: And going to this
10 question of sort of 215, one question is, what's
11 next, or what could be next?

12 What if the government were to decide
13 that it wanted to go back and start using 215 for
14 Internet metadata.

15 All of the rationale -- well, I guess
16 the question, would the rational for telephony
17 metadata apply to Internet metadata? And then
18 would all of the controls carry over to that, or
19 how would such a program be developed and
20 structured?

21 MR. LITT: So let me offer a couple of
22 thoughts. First is to bear in mind that Section

1 215 requires that you obtain business records.
2 There have to be records in existence that you are
3 obtaining.

4 As we discussed earlier, the telephone
5 companies keep and maintain the metadata for their
6 own business purposes and that allows us to use
7 215 to get that. It's not clear to me that the
8 same legal authority could be used with respect to
9 Internet service providers.

10 More generally I think that the FISA
11 Court's approval of the use of 215 for --

12 MR. DEMPSEY: But just on that I mean,
13 it's my understanding that Internet service
14 providers do maintain data, sometimes for a short
15 period of time, sometimes for a longer period of
16 time, but under the rationale of 215 even holding
17 it for a minute or an hour is enough to --

18 MR. LITT: I don't know enough about
19 the technicalities of that. But I'm just saying
20 there's a general limitation on 215. It has to be
21 some sort of documents or tangible things.

22 More generally the FISA Court's

1 approval of the business record collection was
2 based, number one, in part on a specific showing
3 that was made that the collection of the metadata
4 in bulk was relevant to an investigation and that
5 it had to be collected in bulk in order to be
6 relevant. And we'd have to make that same showing
7 to the FISA Court for another category of data.

8 Number two, I think that while it may
9 or may not be strictly a part of the statutory
10 standard, I think that the FISA Court's approval
11 of this collection was based very much on the
12 limitations and restrictions that were imposed on
13 our ability to use the data.

14 It's not at all clear to me, we've
15 never made the request, but it's not at all clear
16 to me that the FISA Court would ever have approved
17 a request that said we want to collect all the
18 telephony metadata and use it for whatever purpose
19 we want to without any controls or restrictions.

20 So I would anticipate that if there
21 ever, if there were another bulk collection
22 program that we wanted to institute, the FISA

1 Court would look at the controls that were
2 proposed and the manner in which relevance of the
3 bulk collection was established and template them
4 up against each other and ensure that in fact both
5 the statutory standard and the Fourth Amendment
6 were met.

7 MR. DEMPSEY: You know right now you've
8 got 215 relevance and that covers everything from
9 one guy's hotel reservation at one hotel to
10 potentially every hotel reservation at every hotel
11 of everybody ongoing indefinitely, and all of that
12 hinges on relevance.

13 Is it possible to bifurcate 215, have
14 your more particularized requests under the
15 standard that's explicit in the statute and then
16 take this set of concepts and limitations that has
17 built up around the telephony metadata program and
18 come up specifically with a statute tailored for
19 something which I see as quite different, which is
20 the sort of bulk collection, the ongoing
21 collection?

22 MR. LITT: I think in the abstract,

1 yes, but statutes aren't written in the abstract.
2 And the question is what it would do, what that
3 statute would provide, whether it would work to
4 allow us to do what we think we need to be able to
5 do.

6 MR. DEMPSEY: Well, for example, in the
7 215 program, the telephony metadata program you
8 have something more than mere relevance. You have
9 a concept of necessity, which is not in the
10 statute explicitly but I think which is a premise
11 of the program, which is it's necessary to collect
12 all the data in order to be able to get the value.
13 Isn't that a standard that could be codified?

14 MR. LITT: Well, I mean I guess Brad
15 can perhaps speak to this better than I can. My
16 understanding of the basis on which the FISA Court
17 determined that the bulk collection was relevant
18 was in fact in part the necessity, that it wasn't
19 a separate concept that was --

20 MR. DEMPSEY: Necessity is not
21 something that comes from the law of relevance
22 because if you look at the law of relevance,

1 necessity is not, I think.

2 MR. WIEGMANN: Actually I mean if you
3 look at -- I think my mic still may not be working
4 so I've got some issues here.

5 If you have other contexts where let's
6 say computerized data is obtained, let's say under
7 a grand jury subpoena or in civil discovery, and
8 the question is always, like, okay, I want to get
9 a certain amount of data and how broadly can I
10 scoop in order to get the core data that I want?

11 And with the courts in looking at that
12 say, well, how broadly is necessary for you to be
13 able to get that core amount of data? Is it
14 necessary to seize the whole computer because
15 there are files on it that you know you can get?
16 And the courts have generally said, yeah, you can
17 get the whole computer maybe in order to get
18 certain information on it.

19 Or there's other cases about financial
20 records and some of the things the government had
21 cited in its white paper that we've published,
22 talk about this context in terms of analogies and

1 from other sayings.

2 So I think there are analogies that
3 show that basically you're kind of using a least
4 restrictive means test, or the means that if it's
5 necessary to get a larger amount of data in order
6 to get the core amount of data that's relevant to
7 your investigation, that that's okay.

8 But all that having been said, if you
9 wanted to codify that and set up -- I mean your
10 question is could you set up, could you segregate
11 the ordinary 215 applications from bulk and set up
12 special rules for bulk because it raises different
13 concerns? Sure, you could do that. I mean we
14 would just have to look at that and make sure that
15 it met the needs of the program and so forth, but
16 absolutely you could do that.

17 MR. DEMPSEY: That's it for this round.
18 Thanks.

19 MR. MEDINE: Judge Wald?

20 MS. WALD: I just want to nail down one
21 thing factually to make sure I understand it. And
22 that's with the 215 collected metadata which

1 includes all the telephone metadata for all calls
2 made in the United States those, that body of data
3 is subject, as I understand it or am I
4 understanding it correctly, to the regular
5 dissemination exceptions in Executive Order 12333
6 for any evidence of crime, or certain kinds of
7 personnel decisions, or to, quote, understand
8 foreign intelligence, is that right or not?

9 MR. LITT: You're talking about the
10 actual bulk collection itself?

11 MS. WALD: Yes, yes.

12 MR. LITT: Yes, it's subject to those
13 rules but more importantly it's subject to far
14 more stringent rules imposed by the FISC.

15 MS. WALD: Okay, but the actual program
16 as it's put forth by the government would -- the
17 reason I'm asking the question obviously is that
18 because there's been certainly perceived unrest or
19 unhappiness among some segments of the public with
20 knowing that all of their telephone metadata
21 though it may be, is out there, the notion of,
22 well, if it's out there but you're not subject to

1 any queries because the number that's actually
2 queried is very small, as you've reported, still
3 the question arises, well, would the data of
4 people who never get queried never get brought
5 into the query system still be subject to these
6 kinds of disclosures?

7 So you say, you point out that the FISC
8 Court may have interpreted it to require more
9 stringent data but still am I correct that some of
10 this evidence, metadata evidence can be
11 disseminated even under those restrictions for --

12 MR. LITT: Only the results of queries.
13 So the data --

14 MS. WALD: So if it's my phone --

15 MR. LITT: Can I just, just to make
16 this clear.

17 MS. WALD: Yeah, I want to get that
18 clear.

19 MR. LITT: The bulk data that is
20 collected can only be disseminated pursuant to the
21 procedures approved by the FISC, which supercede
22 the more general rules --

1 MS. WALD: 12333.

2 MR. LITT: 12333 in this regard. To
3 the extent that 12333 -- I mean 12333 governs
4 everything we do, but with respect to this
5 particular collection the FISC limitations are
6 much more stringent and we can only disseminate
7 query results and even -- and the 12333 then comes
8 on top of that, which is to say that the query
9 results can't even be disseminated unless they
10 meet the test of 12333.

11 MS. WALD: All right. Well, I just
12 wanted to get that.

13 MR. WIEGMANN: And so for any U.S.
14 person information, it's only for counterterrorism
15 purposes is the standard.

16 MS. WALD: I understood that part.
17 Okay, thank you.

18 Following up a little bit on the
19 necessity question that Jim asked, I think it was
20 pointed out in the white paper that came out on
21 the 215 program that it was necessary, it was said
22 this widespread collection was necessary. And the

1 necessity fell within the usual formula of being
2 necessary to a, quote, authorized investigation
3 included the relevance of necessity to the
4 technological tools, or getting the haystack, as
5 it were, rather than exclusively to the more
6 traditional interpretation of what related to an
7 authorized investigation means in criminal law, or
8 has meant in criminal law, as despite we could
9 fight about the grand jury cases, how far they go
10 on that. But usually the traditional
11 interpretation was it's related to an
12 investigation if it's going to lead to the actual
13 evidence relating to the subject matter of the
14 investigation.

15 To get down to the question would be,
16 if 215's relevance is keyed in part to the
17 technological capacity of your search instruments
18 then can that be further expanded if new tools,
19 new technological tools would allow you greater
20 search capacity in this or in other bulk programs,
21 could the, quote, haystack be made as big as the
22 technological tools that you have to use it are?

1 As opposed to the more traditional
2 grand jury which may have some exceptions, but
3 they weren't huge, which related to, is this going
4 to actually lead to evidentiary-wise to some
5 evidence that's relevant to the subject matter of
6 the investigation.

7 Sorry for the wordiness of the
8 question, but I think you know what I'm asking.

9 MR. WIEGMANN: So if your question is
10 do the changes that technology could allow for
11 different --

12 MS. WALD: Yeah. Yeah, you've said it
13 better.

14 MR. WIEGMANN: Standards, right. I
15 think it is. That was one of the factors that the
16 court looked at is what the technological means
17 that NSA had available to it to search this data
18 and how effective could those tools be in that
19 particular context.

20 So yes, I think as NSA develops new
21 tools or as other parts of the intelligence
22 community do that, that would be a factor that's

1 considered.

2 But it's not a dispositive factor. The
3 fact that you have the tools means that
4 automatically ipso facto you have the ability to
5 get whatever data that those tools permit you to
6 get if it leads to the information, because you
7 have to look at all the other factors that the
8 court considered. How important is the
9 information? How necessary is it to get the
10 information in a larger quantity? What's the
11 nature of the information?

12 And obviously that's a critical factor
13 here that the information is not protected by the
14 Fourth Amendment. It's just phone numbers, it's
15 not content and so that's obviously a key
16 consideration that would not make this program
17 available for other contexts, particularly with
18 respect to content information.

19 So I don't know if that answers your
20 question but I do think --

21 MS. WALD: Yeah, yeah.

22 MR. WIEGMANN: I do think technological

1 changes do make a difference.

2 MS. WALD: It does. I'm trying to get
3 at what to some has seemed an open-ended notion of
4 having a technology driving the extent of the
5 collection authority, as opposed to the old
6 fashioned method of is this going to lead to some
7 evidence.

8 Okay. That leads into my -- I think
9 I've got time for one more question, yeah. And
10 that is, as I read it the government's legal
11 justification as laid out in its papers and in
12 some of the material that's been disclosed for the
13 current 215 program has to and does rely heavily
14 on the Smith, Maryland notion that the telephone
15 metadata in that case did not constitute a Fourth
16 Amendment or legally cognizable privacy interest.

17 Now certainly Smith v. Maryland we all
18 recognize is still on the books, but there have
19 been some intimations of possible future changes
20 in the U.S. v. Jones case, both in the D.C.
21 Circuit and in some of the concurrences in the
22 Supreme Court, as well as since Smith v. Maryland

1 we've had a lot of research pointing out the
2 potential informative value of a lot of metadata
3 on a person. If you can find out really not
4 content but a lot of the metadata on the kinds of
5 communications the person has had, the places
6 they've gone, etcetera, etcetera, you're going to
7 know as much in many cases, maybe more in some,
8 than you'd get from the actual content of those
9 communications, suggesting to some that that
10 dichotomy is not such a definite one.

11 I guess my basic question is if in the
12 future Smith v. Maryland should be changed to take
13 account of some of these trends or as suggested
14 metadata, some situations may well have privacy
15 value, cognizant legal privacy value?

16 Would programs like 215 lose their, in
17 your view, lose their legal foundation, their
18 legal legitimacy?

19 MR. WIEGMANN: So I think that remains
20 to be seen. I understand you're referring to the
21 Jones case in the Supreme Court that talked about
22 Smith v. Maryland. Obviously it's fundamental, as

1 we've explained in our briefs, to the analysis of
2 the court here that the information is not
3 protected by the Fourth Amendment under Smith
4 because it's been shared with the phone company.

5 Again, the basic idea of Smith is
6 information that is a billing record that belongs
7 to the phone company that you have voluntarily
8 exposed to the phone company in making a phone
9 call is not protected by the Fourth Amendment.

10 To the extent that that changes in the
11 future because of changes in technology, changes
12 in how the courts perceive privacy in the context
13 of large amounts of metadata, I think it remains
14 to be seen.

15 I mean the holding in Smith and Jones,
16 again to be clear, was not based on that change,
17 it was based on the idea that there was a trespass
18 in putting a GPS device on your individual car.
19 So it was about a GPS device put on the bumper or
20 on the underside of a vehicle and tracking that
21 vehicle in that manner. And it was based on the
22 physical intrusion, which we wouldn't have in this

1 context certainly. So we don't think Jones is
2 controlling or causing to question our current
3 authorities.

4 But obviously if there are future
5 developments in the law those would have to be
6 reevaluated by the FISA Court and other courts as
7 they evaluate such a program, so.

8 MR. LITT: And if I can make one point
9 here, which I think is very important. There
10 certainly are a lot of academic studies that say
11 you could take metadata and extract a lot of
12 information from it. We aren't allowed to do
13 that. We don't do that.

14 We have a very specific, limited
15 purpose for which we use this metadata and that's
16 all we're allowed to use it for.

17 And I think, as I said earlier, I think
18 there would have been a very different situation
19 presented if we had asked the FISA Court to say we
20 want to get this metadata and we want to do
21 anything we want with it.

22 MR. DE: I just want to echo that point

1 that Bob made because it's really important for
2 folks who are engaged in this public discussion to
3 not conflate the very legitimate point you've
4 made, Judge, which is that perhaps a great deal
5 could be discerned from metadata in a variety of
6 contexts.

7 But in terms of this particular
8 program, it's only for counterterrorism purposes
9 per order of a court. There's no subscriber
10 information involved. And so I've heard people
11 spinning out threads that one could determine what
12 doctors one visits, who are one's best friends,
13 and a variety of things that in the abstract and
14 without any legal or policy controls in place
15 might be possible, but that's not the world we're
16 in with this particular program.

17 MR. KELLEY: And Judge, if I may, just
18 one final comment in that regard. The white paper
19 also pointed out that the relative balancing of
20 the minimal invasion of privacy compared to the
21 significant, the greatest interest of the
22 government in this particular fight against

1 terrorism.

2 We're not talking about local crime,
3 we're not talking about even organized crime.
4 We're talking about terrorism where I don't have
5 to say it, there are lots of compelling national
6 interests at stake.

7 So the government's interest in this
8 particular question is at its very greatest
9 compared to the minimal invasion of privacy, even
10 if it were protected under the Fourth Amendment.
11 I think that the key question is, is that outcome
12 reasonable under the Constitution, a reasonable
13 search, seizure? And I think the answer would be
14 yes.

15 MR. MEDINE: I think we have time for a
16 quick five minute round and still come in on time.

17 A lot of these programs were developed
18 outside the public view and we certainly have seen
19 that there's been a very strong public reaction to
20 the programs.

21 What steps could be taken to consider
22 privacy and civil liberties concerns as these

1 programs are developed and also public acceptance
2 concerns, because obviously we answer to the
3 American public, as we go forward in developing
4 these types of surveillance programs?

5 MR. LITT: I'm going to punt on that
6 question in the sense that, as you know, this is
7 one of the things that the President has asked the
8 intelligence community and you to look at.

9 MR. MEDINE: We're seeking your
10 guidance.

11 MR. LITT: And I think that rather than
12 offer views right now on how that could be done, I
13 think I'd just say that this is a process that's
14 ongoing and we're very sensitive to see whether
15 there are ways that that can be done.

16 MR. MEDINE: No other comments?

17 Going back to a question that was
18 raised in an earlier round about the age of data
19 in the 215 program. Do you track, and I'm not
20 asking you to reveal which cases you believe there
21 have been success stories in the use of the data,
22 but in those such cases, do you track the age of

1 the data that was used to determine whether it was
2 five year old data was necessary, whether three
3 year old data might have sufficed?

4 I know last week there was some
5 administration testimony that you might be willing
6 to accept a three year retention period instead of
7 a five year retention period. Was that based on a
8 study of the effectiveness of the data?

9 MR. DE: We have tried in view of
10 current discussions to do the best possible
11 assessment as to where the greatest value has been
12 gleaned in the past.

13 And so it's some of that evaluation
14 that has come into play in the public statements
15 that three years probably would be where the knee
16 of the curve is in terms of the greatest value.

17 Historically it's been difficult to
18 piece together. As you can imagine it's quite
19 complex to figure out where any particular piece
20 of data, phone record in a particular query, five
21 years ago came from and how available it was in
22 subsequent steps in the intelligence process. But

1 folks have tried their best under the current
2 circumstance to make that evaluation, and that's
3 where that three years comes from.

4 MR. MEDINE: I know there's been a
5 great interest in more transparency with regarding
6 how these programs operate, and currently
7 providers to the government of 215 data are
8 restricted in their ability to disclose
9 government requests.

10 Would you support reducing that
11 nondisclosure period to 30 days after a request?

12 MR. DE: We'd probably have to take
13 that into consideration as the government as a
14 whole.

15 MR. LITT: I guess my view is that
16 arbitrary limits really don't take account of
17 operational realities. And obviously most
18 limitations that I've seen allow for renewal.

19 I would think that requiring us to go
20 back every 30 days in what could be a lengthy
21 investigative period might put a burden on us.
22 But again, we'd have to look at specific

1 proposals.

2 MR. WIEGMANN: And I think it's
3 unlikely that the need for secrecy in these
4 contexts in intelligence investigations is likely
5 to fade after a 30 day period.

6 MR. MEDINE: And a final question is, I
7 just wanted to follow up on an answer I think
8 Mr. Litt gave earlier in response to Mr. Dempsey's
9 question about the corporate store, the
10 information that's collected under 215 as a result
11 of a query.

12 What are the standards that govern when
13 that collected data can be queried? That is, is
14 there a RAS determination, is there a 12333
15 criteria? What restricts access to the data? And
16 also is there an audit trail for requests,
17 inquiries into that database?

18 MR. LITT: Actually I don't think I
19 gave any such answer so I'm going to kick this to
20 Raj, who might know the answer.

21 MR. DE: That data would be subject to
22 our background minimization procedures that are

1 there. There's something called use 18. This a
2 Department of Defense, Attorney General approved
3 set of guidelines.

4 But to your auditing question,
5 everything that NSA does in terms of queries of
6 internal data is auditable and so we think that's
7 an important protection that we have in place.
8 And the law applies here as well.

9 MR. MEDINE: All right, thank you.

10 Ms. Brand.

11 MS. BRAND: Thank you. Concern was
12 recently raised to me about the absence of a
13 privacy officer at NSA.

14 Could you tell me two things. First of
15 all, how soon do you think you will have one?
16 What is your process for appointing one? And what
17 would that person's role be in programs like the
18 ones we're discussing?

19 MR. DE: So today we in fact have a
20 privacy officer and a civil liberties officer
21 separately. But a decision was made to put those
22 positions together in a role that would be a

1 direct report to the director.

2 This was announced over the summer and
3 we've been proceeding with the hiring process. If
4 I recall correctly I think the request for resumes
5 and for interest closes in the first week of
6 November. It's been publicly advertised. And
7 from that point forward we will proceed
8 expeditiously with the hiring process.

9 The one thing I would I would note
10 though is not only are those functions ones that
11 we think are critically important, today we also
12 work very closely with the DNI's Chief Civil
13 Liberties and Privacy Officer.

14 I think the attention, focused
15 attention that such a person could bring at the
16 NSA as programs are developed would be an
17 effective tool going forward.

18 MS. BRAND: I think you would be well
19 served to make that process as expeditious as
20 possible.

21 I wanted to ask a general question in
22 probably the two minutes I have left. With

1 respect to changes to the way the FISC operates,
2 both in terms of transparency and adversarial,
3 just to lump those together in the interests of
4 time, what changes could the administration
5 support?

6 MR. LITT: Again, not speaking for the
7 administration as a formal position, but I think
8 we have articulated that we are open to some kind
9 of a process for allowing the FISC to seek amicus
10 participation in cases that present important
11 legal or privacy concerns.

12 We have both practical and legal
13 concerns that need to be worked through in the
14 context of how one accomplishes that, but I think
15 that we are open to that.

16 In terms of transparency again, there
17 are already requirements for providing opinions to
18 Congress. We're already working on declassifying
19 opinions. It's not something where you can just
20 snap your fingers and say this opinion is going to
21 be released.

22 As you know, any judicial opinion is an

1 application of law to a set of facts. And it's
2 frequently, as Judge Walton, who's the Chief Judge
3 of the court has said, it's frequently very
4 difficult to separate out the classified facts
5 from the unclassified portions that can be
6 released.

7 I think we take very seriously the idea
8 that it's appropriate to get as much of these into
9 the public domain as possible, it's just, speaking
10 as one who's been personally involved in it, it is
11 a very, very time consuming and difficult process
12 and risks creating a document that is either
13 incomprehensible because of all the redactions or
14 affirmatively misleading because important parts
15 of it are left out.

16 MS. BRAND: When you say you can
17 support some kind of a mix, do you mean literally
18 an amicus process or do you mean some version of
19 the special advocate that has been suggested?

20 MR. LITT: As I said I think there are
21 both practical and legal concerns with a special
22 advocate. I think there's an Article III issue

1 with respect to the standing that a special
2 advocate would have in the court.

3 I think that there's also a sort of
4 precedential issue that we're very concerned
5 about.

6 MS. BRAND: Precedential you said?

7 MR. LITT: Yes. There are all sorts of
8 warrant requirements that are traditionally done
9 ex parte and an argument was made, I think this
10 was made by Chairman Rogers at the hearing last
11 week, are you going to set up a process that
12 provides more protection for foreign terrorists
13 than for Americans who are the subject of criminal
14 search warrants.

15 I think this is the sort of thing we
16 need to think through. I think that a proposal to
17 have the court have the ability to draw on lawyers
18 who can in an individual case present opposing
19 arguments I think accomplishes the need that
20 people feel that there be alternative arguments
21 presenting in a manner that is much less legally
22 problematic.

1 MR. MEDINE: Thank you.

2 Ms. Cook.

3 MS. COLLINS COOK: I'd like to follow
4 up on this conversation. We'll be having an
5 entire panel devoted to this. The next panel will
6 be discussing the operations of the FISC.

7 But I think many of the proposals that
8 we've seen are predicated on the notion that
9 because the process is not currently adversarial
10 it lacks rigor. Folks have pointed to what I
11 would call a win loss record of the government in
12 front of the FISC.

13 And I think it would be helpful to the
14 following panel if Brad or Raj, whoever is
15 situated to talk about this, can talk about how
16 the FISC operates and the process of seeking
17 authorization for a program like this, whether
18 it's helpful at all to simply look at a win loss
19 record.

20 MR. WIEGMANN: Yeah, so the FISC has
21 come under a microscope obviously as a result of
22 this, the recent disclosures. But we want to say

1 on behalf of the Department of Justice, the
2 National Security Division represents the
3 government in front of the FISC.

4 These are regular, life-tenured Article
5 III judges. They apply the same standards and
6 approach to doing their work as they do in their
7 regular cases, whether criminal or civil cases,
8 that they're handling during their regular work
9 the rest of the year. They're sitting on a
10 rotating basis so that means, I don't know, how
11 many, 13 judges or whatever on the FISC? Eleven
12 judges Raj tells me. They are coming in and
13 rotating through and doing a FISA docket in an
14 individual week.

15 I could tell you they apply
16 extraordinary rigor and care to every single
17 matter that they look at in this process.

18 The Executive Branch has already
19 applied a lot of rigor and care in making these
20 applications in the first instance. I mean
21 whereas an ordinary warrant can be approved at a
22 much lower level, or a Title III wiretap, these

1 warrant applications can only be approved by the
2 Attorney General or the Assistant Attorney General
3 for National Security. They go through a lot of
4 review on the front end.

5 And then as Judge Walton, the Chief
6 Judge of the FISC, has explained on the back-end
7 the fact that the court may have granted an
8 application doesn't mean that it hasn't been
9 modified.

10 And I think that he's publicly revealed
11 in a letter that upwards around 25 percent of the
12 cases that are submitted to him involve some
13 significant modification beyond just a typo or
14 something like that. But that's a much higher
15 number than you would have in the context of
16 regular Title III applications where I think the
17 overwhelming majority are approved without change.

18 So I think actually if you look at just
19 the, quote, unquote, win loss record it shows that
20 the FISC is applying a very rigorous standard of
21 review. But you would expect in this context, you
22 wouldn't expect the government to be filing a lot

1 of frivolous applications to conduct foreign
2 intelligence. You don't want, I think, a Justice
3 Department that's bringing and getting, you know,
4 50 percent win rate or something, or 50 percent
5 rate, because that would reflect a problem in
6 terms of us applying for things that really were
7 not justified in the first instance.

8 So the FISC really is not a rubber
9 stamp. If you look at the opinions that have been
10 released is the other thing I would say, we have
11 declassified some opinions now. You can see the
12 extent of review on some very complex and
13 significant constitutional issues that they've
14 looked at in conjunction with the bulk programs.

15 And they really are looking to
16 scrutinize to make sure that all of the
17 collection, to understand the highly technical
18 issues that are sometimes presented in these cases
19 and to ensure that the Constitution and the
20 requirements of the statute are being followed.

21 So I don't know if that answers your
22 question or if Raj and Bob want to.

1 MR. LITT: I just want to emphasize
2 what Brad said about the review that the
3 Department of Justice gives these before they ever
4 get to the FISA Court.

5 MS. COLLINS COOK: I understand. That
6 gives small comfort I would say to folks who are
7 concerned about the lack of an adversarial process
8 and I think y'all have made very clear the
9 professionalism with which you approach internally
10 and the high levels of accountability. You're
11 talking Senate confirmed individuals who are
12 signing off on each and every one of those. I
13 understand that.

14 MR. LITT: No, but it's relevant to
15 assess, to put the so-called win rate in context,
16 which is to say things don't ever get made,
17 applications don't ever get made to the FISA Court
18 unless the Department of Justice is very, very
19 confident that they are legally well-supported.
20 And they give them a wire brushing before they
21 ever get out of the Department of Justice.

22 MS. COLLINS COOK: A final question. I

1 think the some of the proposals also speak to
2 congressional oversight, and there again I think
3 there's some perception that the semiannual report
4 goes up to Congress and it's never looked at, and
5 perhaps if a sunset is coming up then oversight is
6 conducted.

7 Can you talk a little bit about your
8 experience with day-to-day congressional oversight
9 to the extent that that occurs?

10 MR. DE: Sure. So I would definitely
11 like to put to rest any notion that it's not
12 rigorous or frequent or exceptionally open, at
13 least I can speak to NSA's perspective. We work
14 with the Senate intel and House intel committees.
15 It's hard for me to describe, but on a very
16 frequent and detailed basis, sending people down
17 to provide briefings, informal notifications and
18 so forth.

19 As you know, pursuant to statute, the
20 Executive Branch must provide all significant FISC
21 opinions to both the intel and judiciary
22 committees. NSA in particular is not only

1 responsive to the intel committees but we're also
2 part of the Defense Department so we're responsive
3 to the armed services committees. As I mentioned
4 the judiciary committees are also relevant to us.
5 And finally, given our role in cyber activities
6 the homeland security committees of both the House
7 and Senate perform oversight of us as well.

8 MR. MEDINE: Thank you.

9 MR. DEMPSEY: A couple of questions on
10 702, and then also related 12333.

11 On 702 collection of the content
12 program, some of the communications that are
13 acquired are communications persons reasonably
14 believed to be overseas are to and from people in
15 the United States. And it's my understanding that
16 those are lawfully collected. It's not
17 inadvertent, it's intentional and lawful.

18 But then once that data is in it can be
19 searched looking for communications of a U.S.
20 person. So you have very low, sort of front-end
21 protections, then am I right to say, or let me put
22 it this way, what protections occur then on the

1 search side?

2 And I understand Bob's point that if
3 it's lawfully collected the rule is you can search
4 it and use it for a legitimate purpose. But even
5 with the 215 data you've imposed this RAS standard
6 and it's lawfully collected. Zero constitutional
7 protection but you've nevertheless surrounded it
8 with a lot of limitations.

9 What are the limitations surrounding
10 the incidentally but advertently collected U.S.
11 person communications?

12 MR. DE: So maybe I can start just with
13 the initial premise that you raised. So you're
14 correct that we must target non-U.S. persons
15 reasonably located to be abroad.

16 But one important protection is that we
17 can't willfully target a non-U.S. person in order
18 to reverse target a U.S. person, which I know the
19 panel is familiar with, but just so other folks
20 are familiar with that.

21 Our minimization procedures, including
22 how we handle data, whether that's collection,

1 analysis, dissemination, querying are all approved
2 by the Foreign Intelligence Surveillance Court.

3 There are protections on the
4 dissemination of information, whether as a result
5 of a query or analysis. So in other words, U.S.
6 person information can only be disseminated if
7 it's either necessary to understand the foreign
8 intelligence value of the information, evidence of
9 a crime and so forth.

10 So I think those are the types of
11 protections that are in place with this lawfully
12 collected data.

13 MR. DEMPSEY: But am I right, there's
14 no, on the query itself, other than it be for a
15 foreign intelligence purpose, is there any other
16 limitation? We don't even have a RAS for that
17 data.

18 MR. DE: There's certainly no other
19 program for which the RAS standard is applicable.
20 That's limited to the 215 program, that's correct.

21 But as to whether there is, and I think
22 this was getting to the probable cause standard,

1 should there be a higher standard for querying
2 lawfully collected data. I think that would be a
3 novel approach in this context, not to suggest
4 reasonable people can't disagree, discuss that.
5 But I'm not aware of another context in which
6 there is lawfully collected, minimized information
7 in this capacity in which you would need a
8 particular standard.

9 MR. DEMPSEY: Minimized here just means
10 you're keeping it.

11 MR. DE: I'm sorry?

12 MR. DEMPSEY: Minimized here means
13 you're keeping it, doesn't it?

14 MR. DE: It means -- there are
15 minimization requirements, both in terms of how
16 it's collected, how it's processed internally. I
17 mean we can go into more detail in a classified
18 setting. How it's analyzed and how it's
19 disseminated. So the statute requires
20 minimization to apply in every stage of the
21 analytic process.

22 MR. DEMPSEY: Okay. Am I right, the

1 same situation basically applies to information
2 collected outside of FISA? So FISA collection
3 inside the United States, 12333 collection outside
4 the United States, but those communications
5 collected outside the United States might include
6 collections to or from U.S. citizens, U.S.
7 persons, and again, those can then be searched
8 without even a RAS type determination, is that
9 right?

10 MR. DE: I think, yeah, I don't know if
11 we've declassified sort of minimization procedures
12 outside of the FISA context, but there are
13 different rules that apply.

14 MR. DEMPSEY: One question on that
15 because we're trying to keep to the five minutes.

16 MR. DE: If I could just --

17 MR. DEMPSEY: We have asked about, in
18 fact months ago, several months ago we asked about
19 guidelines for other types of collection, and
20 where do we stand on getting feedback on that?

21 Because you said 18, for example, is
22 the minimization provisions for collection outside

1 the United States, and that's pretty old. Where
2 do we stand on looking at how that data is
3 treated?

4 MR. LITT: I think we're setting up a
5 briefing for you on that. I believe we're setting
6 up a briefing for you on that. We did lose a few
7 weeks.

8 MR. DEMPSEY: No, I understand. I was
9 wondering if you could go beyond saying we're
10 setting up a briefing.

11 MR. LITT: Well, I mean we're in the
12 process of reviewing and updating guidelines for
13 all agencies under 12333. It's an arduous
14 process. You know, it's something that we've been
15 working on for some time and we're continuing to
16 work on it.

17 MR. MEDINE: Thank you.

18 Judge Wald, for the last round.

19 MS. WALD: Okay. This is another 702
20 question. Because of the pretty generalized
21 nature of the certification requirement that the
22 Attorney General and the DNI make under 702 yearly

1 I think it is, maybe it's biannually, and the
2 statutory authorization for very much I'll use
3 short-term category type of targeting that's shown
4 to the FISA Court, and the pretty standard, as I
5 understand it, minimization procedures that are
6 required in 702, there has been some suggestion
7 that the meat of 702, if there is to be any
8 control on it, lies in the so-called tasking
9 orders, which are then approved internally by the
10 government but never shown to the FISC Court, you
11 know.

12 And according to some of the
13 information or some of the opinions of outsiders,
14 including some of the providers, these don't get
15 any kind of outside look on whether or not they
16 really do strike the right balance between the
17 certification, the category targeting, etcetera,
18 certainly for privacy purposes.

19 So it has been suggested that there be
20 some review outside of the government on the
21 tasking orders, at least in maybe not an
22 individualized 702, but in any kind of large

1 categories. Maybe it would be after the fact,
2 maybe it would be along the RAS.

3 Do you have some reaction as to whether
4 or not any mechanism of that kind is, from your
5 point of view, tolerable, or what are the
6 downsides?

7 MR. DE: Maybe I can just start with
8 the basics of how 702, targeting the mechanics,
9 work today.

10 MS. WALD: That would help because not
11 only do some of us have questions about it, but
12 the more you read the newspaper articles it seems
13 to me they don't understand it either.

14 MR. DE: So we have at NSA internal
15 requirements that the targeting rationale to
16 establish that the target is a non-U.S. person
17 reasonably located abroad be written, documented.
18 That has to at least have multiple levels of
19 approval inside of NSA before it's effectuated.
20 And then every 60 days the Department of Justice
21 and the Director of National Intelligence review
22 each and every documentation of every single

1 targeting decision that takes place.

2 Now I know that's not getting to the
3 question you asked but at a minimum folks should
4 understand that there is a multi-agency review of
5 every single targeting decision made.

6 MS. WALD: I don't -- I am
7 interrupting, but am I correct though that the
8 targeting can be, at least this was debated when
9 it was re-authorized, the targeting can be a very
10 broad, I mean it isn't always a particular
11 individual, it can be a broad target.

12 MR. DE: I think what we've said is
13 what goes to the Foreign Intelligence Surveillance
14 Court are certifications that aren't individual
15 selector-based targeting decisions, but what I was
16 speaking of in fact are quite specific.

17 And probably to get more specific, we
18 need to do it in a different setting, but the
19 targeting decisions that are made by individual
20 analysts, reviewed by the Director of National
21 Intelligence and reviewed by the Justice
22 Department are in fact quite specific.

1 MS. WALD: So therein lies any control
2 over keeping the targeting to that which is useful
3 but not overly-broad?

4 MR. LITT: Yeah, so if I can just
5 emphasize here what we're talking about is
6 targeting of non-U.S. persons --

7 MS. WALD: I understand.

8 MR. LITT: Outside of the United
9 States. And it's a rather extraordinary step like
10 we have --

11 MS. WALD: But it brings in
12 incidentally, it can bring in U.S. persons.

13 MR. LITT: Of course it can and so can
14 lots of other things that the intelligence
15 community does.

16 And I think it's a rather extraordinary
17 step that we have in this country judicial
18 involvement in the targeting of non-U.S. persons
19 outside of the United States. And I think it's
20 very important to bear in mind the potential
21 operational consequences of increasing that
22 judicial involvement.

1 When FIA was passed I think there was a
2 conscious decision made as to what the proper
3 balance is between judicial involvement and
4 operational necessity. And I think that if you
5 start to say, well, the FISA Court needs to
6 approve every targeting decision, you're going to
7 bring the intelligence community to a halt.

8 MR. MEDINE: Any final questions?

9 Well, I want to thank all the panelists
10 this morning for a long but very, very helpful
11 session, so we appreciate you appearing before the
12 board.

13 We're going to take a lunch break now
14 and resume at 1:15 on a panel that will address
15 the Foreign Intelligence Surveillance Court.
16 Thank you.

17 (Meeting adjourned for lunch)

18

19

20

21

22

1 MR. MEDINE: Good afternoon. We are
2 now going to start the first afternoon session and
3 the topic again is the Foreign Intelligence
4 Surveillance Court.

5 We're pleased to have as witnesses
6 James Baker, who's formerly with the Department of
7 Justice, Office of Intelligence and Policy Review,
8 Judge James Carr is the Senior Federal Judge with
9 the United States District Court of the Northern
10 District of Ohio, and formerly a FISC judge from
11 2002 to 2008, and Marc Zwillinger, who is a
12 founder of ZwillGen, PLLC, and a former DOJ
13 attorney at the Computer Crime and Intellectual
14 Property Section.

15 I understand that each of you have
16 brief prepared remarks, so please go ahead and
17 then afterwards we will have, as we did in the
18 last panel, rounds of questioning, five minutes
19 this time for each of the board members.

20 But please go ahead, Mr. Baker.

21 MR. BAKER: Thank you very much, David.
22 I'd like to thank the board for inviting me back.

1 It's truly an honor to be here and it's an honor
2 to be able to discuss these kinds of issues in
3 this type of setting. So I appreciate the
4 opportunity.

5 I just have a couple of quick comments
6 really. The focus of our discussion today is on
7 Section 702 of the FISA Amendments Act and Section
8 215 of the USA PATRIOT Act.

9 And I would just say that while these
10 are very important statutorily authorized,
11 judicially reviewed, warrantless surveillance
12 programs involving the collection of
13 communications and communications-related data
14 with respect to many Americans, they're really
15 only part of the story, and I think that was
16 discussed this morning in the panel that I was
17 able to attend.

18 In particular, as the panel was aware,
19 the government conducts surveillance activities
20 using a number of different authorities,
21 especially including outside the United States
22 under Executive Order 12333.

1 And I would submit to the board that as
2 you're evaluating these issues you think broadly
3 about them because they do, the privacy issues
4 that you're confronting do pop-up in a number of
5 different contexts.

6 And as another example, even with
7 respect to telephone records, telephone calling
8 records, there are several ways, eight to ten by
9 my count, sometimes depending on how you count
10 them, eight to ten different ways that the
11 government can go about obtaining the same types
12 of records that you're talking about when you're
13 talking about 215.

14 So 215 is critically important with
15 respect to collecting these types of records, but
16 it's only part of the story. So I would just urge
17 you to think broadly.

18 And as I mentioned the last time I was
19 here, I would also urge you to think broadly
20 because the topic that has not been discussed very
21 much is cyber and the need to think about the
22 critical privacy issues and the data collection

1 issues as they pertain not only to
2 counterterrorism and foreign intelligence, but
3 also to cyber. And I'm happy to talk about that
4 at length if you're interested.

5 The other quick point I would make at
6 the outset is having to do with the Foreign
7 Intelligence Surveillance Court that I worked
8 closely with for many years when I was at the
9 Department of Justice, and I can elaborate at
10 length if you want me to.

11 But you know, in many ways I would say,
12 notwithstanding much of what has been written in
13 the press, the FISA Court is a national treasure.
14 It has done its job in an exemplary fashion during
15 wartime. And I think that has not been said
16 enough, and so I just want to say that at this
17 point.

18 However, the FISA Court is not some
19 type of super inspector general over the whole
20 apparatus that we have to collect intelligence
21 that's, you know, multi-billion dollar enterprises
22 conducted by thousands of people. That is not

1 what the court does.

2 And I think with respect to 702 and
3 215, I would submit that I think we've reached the
4 outer limits of what you can reasonably expect a
5 court to do in this setting. And I'm happy to
6 discuss that at length.

7 At the end of the day, to my mind, it
8 is the responsibility of the President, the
9 Executive Branch and Congress to conduct
10 management oversight and control over these types
11 of activities. I'm happy to talk about
12 transparency and the issue of whether we're going
13 to have an advocate or something like that in the
14 questions.

15 So thank you very much.

16 MR. MEDINE: Thank you, Mr. Baker, for
17 coming back with us again. Judge Carr.

18 MR. CARR: Yes, like Jim Baker, with
19 whom I did work for five or six years, I can't
20 recall whether you had left before I did or not,
21 Jim, but in any event, I'm pleased to be here and
22 be part of the conversation.

1 This comes about, as you may be aware,
2 that as a result of an op-ed that I happened to
3 publish on the 23rd of January, I think it was,
4 making what I consider to be a very modest
5 proposal, which I will repeat this afternoon, to
6 improve the, both I think the processing of
7 certain applications before the court, and I would
8 hope as well perhaps to enhance public confidence
9 in some of the decisions that the court reaches.

10 And that proposal is quite simply that
11 Congress give the FISA Court judges either the
12 discretion or perhaps direct them to obtain the
13 services of outside independent counsel when the
14 court is presented with something that's new and
15 novel.

16 And this would happen on very rare
17 occasions. I mean one of the things I want to
18 emphasize is how infrequently this kind of
19 representation would be necessary.

20 The vast majority of FISA applications
21 are simply fact-based. There's a very low
22 probable cause standard, affiliated or working on

1 behalf of a foreign government or a foreign-based
2 terrorist organization. That's the probable cause
3 showing.

4 Once it's made, we have to issue the
5 order. We do not have discretion to second guess
6 the government's purposes or reasons. To that
7 extent it's very much like a search warrant or
8 Title III order.

9 But on infrequent occasion I felt as a
10 sitting judge when Jim Baker, and he was the one
11 who would do it, would come to me and say, Judge,
12 you better pay special attention to paragraphs 62
13 to 73 because this is a new technique. There's
14 something new or unusual about this that takes it
15 outside of the ordinary really quite
16 straightforward and typical and routine FISA
17 application.

18 The government would do that. It would
19 do it for good reason because it knew that we had
20 to trust its integrity in order for us to function
21 effectively and have confidence in what they were
22 saying to us.

1 That requirement became codified in the
2 first draft in 2008 of the Foreign Intelligence
3 Surveillance Court rules. And the government is
4 required by those rules in that situation to call
5 to the courts attention in that sort of situation
6 to call that circumstance to the court's
7 attention, and I'm sure it does so.

8 That seems to me to be a good trigger
9 point for a judge either to exercise his or her
10 discretion or perhaps for Congress to mandate when
11 that notice, Rule 11 notice, is given, that then
12 the court calls upon one of what I would envision
13 to be a very small cadre of pre-cleared attorneys,
14 probably in the Washington area, probably with
15 some sort of experience in this area, I would
16 certainly hope so, so that they wouldn't have to
17 spend a lot of time learning how the wheel turns,
18 as it were.

19 But that individual could come in, in
20 that circumstance when called upon to do so, to
21 represent, and I was once asked who's the client,
22 I think it's to represent the interests of the

1 Constitution, the Fourth Amendment, and the rights
2 of all of us to communications privacy.

3 But it would be a very infrequent
4 occasion when this would be necessary. And again,
5 I want to underscore that.

6 And I think that the benefits to the
7 court and to the process would be quite
8 substantial. First of all, we judges are
9 accustomed, it's how we work, through the
10 adversary process. And what do you say, what do
11 you say? That's how we usually make decisions in
12 most of what we do.

13 Secondly, when the government wins,
14 close quote, when the judge says, yes, you can do
15 this or that, it has no interest in appealing. It
16 does not need to get that order reviewed. It's
17 not going to go to the FISA Court of review and
18 say, by the way, we won, but nonetheless look at
19 it.

20 However, in that circumstance limited
21 to when there's a new or novel technique or some
22 other aspect where the court has called upon an

1 individual, outside counsel, then that individual
2 would be able to appeal and secure appellate
3 review, which does not presently exist.

4 And an appellate review I think, and
5 certainly in my day-to-day functions as an
6 ordinary Article III judge, is very important. I
7 get reversed. And there are times when I do get
8 reversed, I say, my gosh, I was wrong, thank
9 goodness they're there.

10 And then finally, and this has occurred
11 to me since I first wrote that op-ed piece, it
12 seems to me that this outside counsel, I haven't
13 really got a name for it yet, could also perform
14 an important role when there's an issue, a
15 troublesome issue of noncompliance.

16 Once again the government is required
17 to report instances of noncompliance. It did so
18 when I was there. In every one of the those
19 instances it was fairly trivial. It wasn't
20 troublesome. However, Judge Bates, former
21 presiding Judge Bates's lengthy opinion that was
22 released earlier this summer suggests that there

1 may be instances where reports of noncompliance
2 are of a sort that, once again, as a judge of the
3 Foreign Intelligence Surveillance Court it might
4 be useful to have the discretion to reach out to
5 somebody to assist the court in understanding the
6 issues and ensuring that what went wrong has been
7 fixed and does not have any serious cause to it,
8 or if it does, see that that gets fixed.

9 And at some point I hope to be able to
10 talk about the role of the legal advisors because
11 their work for the court is absolutely crucial. I
12 don't think it's well understood by anybody
13 outside the court, and the role that they play is
14 extremely important. And I hope perhaps to have a
15 few minutes to talk about them and their role and
16 where it fits in everything, so.

17 And one final thing, Jim sort of
18 alluded to this, but it's my view that we should
19 all keep in mind when talking about foreign
20 intelligence collection, the function of those
21 agencies charged with that responsibility, and
22 then the activity of the judiciary, and it's a

1 very limited activity under the Foreign
2 Intelligence Surveillance Act.

3 If you look at Article II, and of
4 course that's the article in the Constitution that
5 establishes the office of the President and gives
6 the President his responsibilities and authority,
7 you don't find the word judge in there at all.

8 Now this is a very unique circumstance
9 where the third branch actually plays a role in
10 overseeing the activities of the Executive in an
11 area in which the Executive constitutionally has
12 exclusive responsibility, for the conduct of our
13 foreign affairs and protecting us against foreign
14 dangers and threats.

15 So I look forward to your questions,
16 and once again it's a real pleasure and an honor
17 to be here. Thank you.

18 MR. MEDINE: Thank you, Judge Carr.

19 Mr. Zwillinger.

20 MR. ZWILLINGER: Thank you for inviting
21 me as well, especially thank you for seating me on
22 the same side of the table as Judge Carr. This

1 might be the first time I've been on the same side
2 of anything with a FISA Court judge, even if it's
3 a former one.

4 As the board knows over the past
5 thirteen years I've helped dozens of clients
6 respond to government demands for customer data,
7 both in criminal cases and under FISA.

8 My clients have ranged from small app
9 providers to large tech companies like Yahoo and
10 Apple. And although my representation of Yahoo
11 before the FISA Court is largely why I'm here
12 today, my comments are entirely my own and are not
13 on behalf of any client.

14 That said, my client work has given me
15 a unique view into the position of providers,
16 Internet service providers who receive demands
17 under FISA and has helped me see two aspects of
18 the process which I believe are inconsistent with
19 the core principles of our legal system.

20 First the overbroad cloak of secrecy
21 that applies to everything FISA-related and the
22 lack of a true adversarial process. Together

1 these issues pose difficulties for providers and
2 by extension their users and the public.

3 To begin with when providers are served
4 with classified FISA orders or directives they
5 receive an entirely unfamiliar process containing
6 very few specifics, which they can review only for
7 a brief period of time before they have to hand it
8 back to the government.

9 Yet based on that mere glimpse, they're
10 being asked to disclose, compelled to disclose the
11 most private user communications they carry.

12 And due to the secrecy providers have
13 few places to turn for advice. While some have
14 experienced counsel that can help determine if a
15 request is routine, of the type that Judge Carr
16 referenced, or novel, providers with limited
17 resources struggle to even understand much less
18 react accordingly to the process they get.

19 Yet providers are the only parties with
20 the statutory authority and the opportunity to
21 challenge these orders before they're executed.

22 Indeed Section 702 is designed right

1 now to make them the last bulwark against
2 potential government overreaching because the
3 court is not given the authority to do a full
4 lawfulness review of a Section 702 directive
5 unless a provider first initiates a challenge.

6 But a decision by a provider to
7 challenge must be made alone under acute time
8 pressure with sensitivity to what's at stake, with
9 little context and while under a gag order.

10 And when providers do bring a challenge
11 trying to meaningfully litigate in an adversarial
12 way in the FISA Court it is an uphill battle.
13 Even now the rules for filings have barely been
14 tested. The logistics of handling classified
15 litigation are very difficult, and filing
16 documents with the court frankly has always been a
17 little bit like trying to get a letter to Santa
18 Claus. It requires a lot of blind faith. The
19 rulings come down the same way.

20 And even when appearing before the
21 court, the government regularly submits ex parte
22 papers that a provider is not permitted to read,

1 even if it's represented by a lawyer with the
2 right clearance.

3 Indeed, this happened again recently.
4 My second case in the FISA Court is a declaratory
5 judgement action brought by five providers seeking
6 the right to disclose the number of intelligence
7 process that they have received, just the numbers
8 for each form of process.

9 And to oppose this relief the
10 government has made a secret filing to justify why
11 that disclosure will cause harm, harm that would
12 outweigh their First Amendment interests, but it's
13 refused to let even cleared counsel see that
14 filing.

15 As you can imagine it's hard to respond
16 effectively to something you cannot read, which
17 means that even in the adversarial proceedings the
18 court is still hearing only one side of the issue.

19 In light of these issues I think
20 relying on providers who have to toil in secrecy
21 and fight in the court with one hand tied behind
22 their back as the last check on our government is

1 not ideal, which is why the creation of a special
2 advocate, one who would have the same access to
3 classified materials as the government could make
4 a real difference.

5 As Judge Carr pointed out and Judge
6 Robertson before him pointed out in the last
7 hearing, judges are used to making decisions after
8 hearing both sides of an argument. That's the way
9 our system is structured and that's what makes the
10 decisions informed and legitimate.

11 An advocate can help ensure that the
12 other side of the argument, not just in the
13 extremely novel cases, but in bulk collection
14 cases and other cases as well, the other side is
15 represented. The advocate can weigh in on the
16 novel issues that come up before the court and
17 serve as a potential resource for providers who
18 want to challenge compulsory process.

19 We need look no further than some of
20 the odd logic in some of the recently declassified
21 decisions to see what happens when the court and
22 the government work through the issues without any

1 balancing input.

2 And even if the decisions wouldn't have
3 come out any differently, even if the court had
4 heard from an advocate, adding an opposing voice
5 would give the process more legitimacy and restore
6 some faith in the court's decision-making.

7 I look forward to our further
8 discussion of the special advocate and other
9 issues related to the court.

10 MR. MEDINE: Thank you, Mr. Zwillinger.
11 We'll start the questioning with Judge
12 Wald.

13 MS. WALD: Thank you. I surmised from
14 the morning panel that the government, as well as
15 many outsiders, have commented, are reasonably
16 comfortable with the idea of the FISC Court being
17 able to call for an amicus to help them on
18 particular novel issues of interpretation.

19 I also think that Judge Carr and many
20 other people who have commented on the outside are
21 suggesting something that's a little bit stronger,
22 a little bit more energetic than that, namely that

1 you would have a body of outside counsel.

2 So I'd like to pin down a couple of
3 things, initially with Judge Carr but certainly
4 with other peoples' reactions too, and that would
5 be if you had such a body of advocates with secure
6 clearances on the outside, do you think that it
7 should be entirely in the discretion of the FISA
8 judge to decide when he or she wants that kind of
9 help?

10 And more specifically, I think, because
11 Judge Carr raised the problem of appeal, and I
12 think that most of us whose experience is familiar
13 with regular Article III, nothing meant by
14 regular, but Article III courts is that the appeal
15 is a very, very necessary part of the process.

16 Now there have been constitutional
17 questions raised by other people about whether or
18 not apart from the provider if you try to give an
19 amicus or appointed, somebody appointed from a
20 panel of secured lawyers the right to appeal you
21 might run into constitutional objections.

22 So I think those two basic questions

1 about whether or not you would leave the
2 initiation of the appointment of such a person
3 entirely in the hands of the FISC judge, and
4 whether or not once that person was in and had
5 participated in the lower court proceedings,
6 should that person, that advocate, whatever you
7 want to call them, can that advocate
8 constitutionally be given some right of appeal?

9 MR. CARR: Well, let me say to try to
10 analogize, I do not think that an office, an
11 outside office that reviews every single
12 application is necessary.

13 MS. WALD: No.

14 MR. CARR: My thought is, how I
15 envision this, have a relatively small number of
16 attorneys, something like a CJA panel in ordinary
17 criminal cases, Criminal Justice Act panel, who
18 will in time gain experience because of their
19 small number, who are completely wall-to-wall
20 security cleared.

21 Mr. Zwillinger raises something that I
22 hadn't really thought about but by all means I

1 think that individual should have as complete
2 access to everything that the court is hearing as
3 the Justice Department prosecutor has, that there
4 should be no withholding, no secret filing or
5 whatever.

6 And I actually hadn't thought about the
7 constitutionality of being able to appeal, but one
8 of the most important aspects of what I'm
9 proposing, because that would give the opportunity
10 for further review by a three judge panel, Foreign
11 Intelligence Surveillance Court review, would give
12 those three judges a chance to look at it again
13 and ultimately perhaps secure a Supreme Court
14 review.

15 But I cannot answer your question about
16 that. I'm not sure I should as a judge in any
17 event, but nonetheless, I don't know.

18 And finally, thinking about this
19 further I think that both under some circumstances
20 it should be necessary for the judge, don't let
21 the judge have discretion.

22 In other words, when what I call a Rule

1 11 notice is given, and I don't know whether it
2 would cover -- I think it would cover something
3 like the PRISM program and so forth, that was
4 certainly my intent, but also give the judge the
5 option, sort of two hand.

6 And so it's not just when a Rule 11
7 notice comes in, that could be a trigger, but then
8 the judge can retain discretion to reach out. But
9 it would be a small group of lawyers pre-cleared,
10 gain experience, and again, I think used
11 relatively infrequently.

12 Or perhaps, this just occurred to me,
13 when a provider has an interest and the provider
14 wants to appeal, perhaps the provider could also
15 request that the court appoint an outside
16 attorney.

17 MR. ZWILLINGER: If I could jump in on
18 that for a moment though. I would undoubtedly be
19 one of those attorneys. I've been before the FISC
20 twice. I'm the only private attorney to be before
21 the court of review. I don't think it's enough.

22 That is, you talk about the

1 constitutional questions of letting somebody have
2 the standing to appeal, the court believes that it
3 doesn't have the power to force the Executive to
4 make classification decisions differently.

5 So the Executive is not going to
6 provide this private counsel with full access to
7 the classified material that would be necessary,
8 and certainly not on a historical basis. That is,
9 maybe for the particular case, but an advocate
10 would know that two years ago the Solicitor
11 General stood up and made a representation to the
12 court that, for example, as happened in re
13 Directives case, that there is no database of
14 incidentally collected U.S. persons'
15 communications.

16 And only an advocate who had been in
17 several cases would know that the representations
18 the government is making in one case may be
19 inconsistent than the representations that are
20 made in another.

21 So as much as in my business interests,
22 I would love for there to be a small group that we

1 would have exclusive right to practice before the
2 court, I don't think it would satisfy the
3 interests of really protecting the Constitution
4 because, by definition that group is going to be
5 limited.

6 I would love for the special advocate
7 to be able to bring the help of outside and the
8 type of panel you described to bear on a
9 particular case, but I think there has to be
10 someone with an institutional interest that would
11 look across multiple cases and be able to
12 challenge the government's programs, not just in
13 the one case that they may be admitted to
14 practice.

15 MR. MEDINE: Thank you.

16 Mr. Dempsey.

17 MR. DEMPSEY: First, Jim Baker, do you
18 have any thoughts or comments on what we've been
19 talking about here?

20 MR. BAKER: Sure. I'll just try to be
21 brief.

22 I mean on the one hand, so you're

1 trying to balance I would think, speed and agility
2 and the ability of the government to move quickly
3 without adding more process. And the process was
4 discussed a little bit today, but there's a lot of
5 process already. So we're going to add more, in
6 theory, under any of these proposals.

7 Another issue is intruding on the
8 President's Article II authority to an even more
9 significant degree.

10 Everybody agreed I think, when FISA was
11 enacted that this was what everyone was doing.
12 This is what this act is all about. It was
13 justified for a variety of reasons back then. You
14 know, there may be reasons to have it now, but we
15 have to be mindful that that is what's happening.

16 And I am worried about delegating to
17 others, whoever it may be, the authority to
18 disclose information, the classified information
19 to yet another party.

20 I also worry about having an outside
21 panel. And the concept of an advocate versus an
22 amicus on a case-by-case basis we can talk about

1 later. But the main thing I'm worried about
2 frankly is just leaks of information.

3 So one of the things, it is hard to
4 prosecute a leaks case. So the criminal is there,
5 but it's hard to actually use. Something that
6 everybody who's in the system has to deal with if
7 they decide they want to leak something is the
8 fact that they may lose their job. They have skin
9 in the game that's real, that's important to them.
10 It's important to their families. And they have
11 to think long and hard about whether this issue is
12 something I'm going to try to leak something about
13 because you can lose your security clearance if
14 you leak and they still can't prove it, if you
15 have a situation where you can't prove a case.

16 So I'm worried about this at a variety
17 of different levels, and I can respond more
18 specifically to your question.

19 MR. CARR: If I could speak to that
20 because something just occurred to me. It seems
21 to me that, first of all, perhaps you could create
22 these people as some sort of, this small group as

1 somehow federally employed and appointed like the
2 federal public defender.

3 More importantly, it just occurred to
4 me as Jim was saying, I mean there's never been a
5 FISA leak by anybody affiliated with the FISA
6 Court, as far as I'm aware.

7 And then I'm not talking about a large
8 number of people. But as importantly, a lawyer
9 might be difficult to prosecute, but it wouldn't
10 be very hard to take his license and his
11 livelihood were he to leak. And so I think that's
12 something to keep in mind.

13 And Jim actually raised at lunch the
14 idea of a federal appointment. The more I think
15 about the risk of losing a license, plus the
16 public shame and disgrace, and the potential risk
17 of being prosecuted, I think at some point you
18 have to have confidence in the people who pass
19 these kinds of security clearances, that they will
20 do the job that their oath binds them to do and
21 maintain classification.

22 I'd like to ask one little, just raise

1 the question, and it is in response to Judge Wald.
2 I don't know, can Congress mandate, I mean
3 Mr. Zwillinger's concerns about the withholding of
4 classified information for this outside counsel,
5 whatever you call, I mean can Congress include
6 that and say that that person shall have the same
7 access to all documents and information classified
8 or not that the government provides? I don't
9 know. That is another constitutional issue.

10 MR. BAKER: Judge, if I can just add,
11 you know, I'm not a CIPA expert but, you know, by
12 and large in the Classified Information Procedures
13 Act setting in a criminal case the government
14 cannot be forced to disclose information to a
15 defendant, but the government can be forced to
16 make a hard decision about whether to prosecute
17 the person or the sanction they may suffer for not
18 disclosing the information to the defendant may be
19 dismissal of the case.

20 I don't know how it would work in this
21 context but at the end of the day I don't think --
22 I think it is a significant constitutional issue

1 about whether you can force the government to
2 disclose classified information to somebody that
3 the Executive, the President does not want to.

4 MR. DEMPSEY: Although would the
5 analogy in this situation be basically, the court
6 would in essence say, just as in CIPA, if you want
7 to prosecute this person you need to make this
8 information available in this way. If you want to
9 get your order you need to make this. I'm not
10 going to rule on this until I'm sure that I've had
11 both sides of the story.

12 MR. BAKER: Yeah, you'd have to figure
13 that out.

14 MR. DEMPSEY: The judge is sort of
15 nodding his head.

16 MR. CARR: As a matter of fact, it
17 would make sense, condition, you want this order,
18 well, we're going to play with a level playing
19 field and all the cards up on the table. And that
20 may be a way around it.

21 MR. DEMPSEY: One quick question, there
22 are two, I think, related ideas in play here.

1 Some people talk about the special advocate, some
2 people talk about amicus. Is it possible that you
3 could have a hybrid of this, that sometimes you
4 would have the classified lawyers, this sort of
5 cadre, handful of people pre-cleared, etcetera?

6 In at least one case the FISCR, the
7 FISA Court of Review has invited non-cleared
8 amicus to comment on a question of law. Is there
9 any possibility that that could happen in the
10 first impression or whatever, when the application
11 is first presented that the court could say, all
12 the details are secret but there is a question?

13 Is the law, the one where the amicus
14 participated in an unclassified context had to do
15 with the wall. So you could have a hybrid of both
16 of these. Do you feel that, or yes or no?

17 MR. CARR: I was trying to think
18 whether the, for instance, the PRISM program
19 itself, because it raises clearly Fourth Amendment
20 issues, I think it was you or somebody this
21 morning pointed out the reasonableness clause of
22 the Fourth Amendment. And I think that may well

1 be in play.

2 I think Smith is not a particularly
3 reliable basis. That was a pin register and so
4 forth. My problem is I'm not, as somebody else
5 mentioned, I'm not sure you can so easily untangle
6 the secret from the, quote, pure question of law.

7 Mr. Zwillinger may have a much better
8 grasp of that than I do.

9 MR. ZWILLINGER: I have the same view.
10 Just an actual example in the 2008 case the
11 question was whether the lawfulness and the
12 constitutionality of the directive, the court
13 relied heavily on the minimization and targeting
14 procedures to say that the procedures in place
15 were sufficient to provide constitutional
16 protection.

17 The provider never got to see the
18 minimization and targeting procedures, and had it
19 not been for the leaks it's not clear we'd ever
20 have seen them. So to argue even if you're in the
21 case or as amicus without seeing some of the
22 factual basis makes it very difficult to present a

1 constitutional argument about whether the
2 safeguards are sufficient.

3 MR. DEMPSEY: Okay, thank you. Thanks.

4 MR. CARR: Because many of the
5 circumstances that I have in mind raise new and
6 novel methods of collection. I'm going to point
7 at this point because it's public now, the whole
8 PRISM idea itself.

9 And so there's an intersection between
10 the technology keeps running ahead of the law,
11 both in Title III and everywhere else, and that's
12 part of the problem too. I'm not sure that it can
13 be quite so finely sliced.

14 MS. COLLINS COOK: Building on
15 something that you've just talked about right
16 there with the technological advances, what is
17 your understanding of the FISC's current ability
18 to use technical experts, technical consultants?

19 Is that something that the FISC, I
20 think we've heard competing views as to whether or
21 not the FISC can already do that, does it do it,
22 should it do it more?

1 And I'm here thinking about new
2 technologies, or to try and avoid what we've heard
3 to be a problem of miscommunications from
4 technologists through to lawyers through to
5 judges. So I ask the question whether there's
6 already that capacity.

7 MR. BAKER: Well, keep in mind I'm not
8 in the government anymore, so. But I would say, I
9 mean you've put your finger on a very important
10 issue, this translation, the game of telephone
11 where things get translated from technologists to
12 lawyers to judges. That's a real problem and a
13 significant problem.

14 My experience was that if the court had
15 a question we could bring in any expert from the
16 government to talk about any technological issue
17 that was required.

18 I guess just thinking about it, it
19 seems to me that if the court wanted to bring in
20 an expert from the outside, perhaps from one of
21 the companies that Marc's talking about, I don't
22 see any reason why that could not be made to

1 happen, if they wanted to actually speak to
2 someone who's, you know, connecting wires together
3 through machines and things like that.

4 I don't see that as being something
5 that would not be possible to do. You'd have to
6 bring in someone who has a clearance. You'd have
7 to figure out what kinds of questions you're going
8 to expose this person to, what kind of
9 information. There could be some security issues
10 around that I could see, but I don't see that as
11 being something that shouldn't be possible.

12 MS. COLLINS COOK: Does anyone else
13 want to opine on that?

14 MR. CARR: If I could say, well first,
15 and again I don't know back in 2002 part of my
16 experience as a rookie FISA Court judge was to
17 visit agencies and be shown and told about what
18 now of course probably is outdated, is the flip-
19 phone or the old car clunky phone,
20 technologically.

21 And I can recall one instance where we
22 had the opportunity and we took it to become

1 informed about a particular kind of activity.
2 Obviously I can't go into any detail, but I'm
3 quite comfortable with the idea. Certainly you
4 can reach within the government, and I don't see
5 why we couldn't reach outside the government to
6 get that kind of -- so we simply understand what
7 they're talking about.

8 MS. COLLINS COOK: When y'all were
9 discussing CIPA as a possible analogy I just
10 wanted to follow up on that briefly because CIPA
11 true, the government at the end of the day has the
12 ability not to bring criminal charges.

13 There may however be other alternatives
14 for the government to pursue such as immigration
15 consequences, PNG, you can envision a variety of
16 things that the government could do, and you're
17 talking about a situation where you've identified
18 who you believe to be the wrongdoer.

19 Does the analogy hold if you're talking
20 about the FISA Court where you have a hybrid
21 preventative mission of many of these authorities,
22 as well as an investigative?

1 If my question makes sense. It just
2 strikes me that it may not be the truest analogy
3 to the FISC situation.

4 MR. BAKER: I mean I haven't thought
5 through it completely, I just brought up the CIPA
6 example here.

7 But I am worried about, yes, that first
8 of all the President being forced to disclose
9 classified information and then what happens if he
10 decides not to. I think that's a big issue. I
11 don't pretend to have the answer here today, but I
12 think that raises real, real concerns.

13 For the President to give up the
14 ability to obtain some type of otherwise lawfully
15 authorized, statutorily approved type of
16 collection that's consistent with the Fourth
17 Amendment. Obviously you have to persuade the
18 judges about that. I don't know. I don't know
19 about that. It's a real hard issue.

20 MR. CARR: And again, I haven't thought
21 about it until about seven or eight minutes ago,
22 but it does seem to me as a judge, I mean we

1 would, as part of the ordinary process, we would
2 say, look, I've got questions. I would call one
3 of the OAPR attorneys and say, look, I've got a
4 problem with this. And it would be a fact kind of
5 a problem, it wouldn't be a technological kind of
6 problem.

7 But it does seem to me, I have the
8 ultimate authority. They have to give me, I
9 think, what I'm asking them to give me if they
10 want to get my approval.

11 It's my understanding also that if I
12 turn them down they can't simply show up next week
13 to the next person, they've got to come back to
14 the same judge who's turned them down.

15 MR. BAKER: Or appeal.

16 MR. CARR: Or appeal, absolutely. And
17 so again I think it's something that would
18 certainly bear looking into by people who've
19 thought about it and will think about it more than
20 I have this afternoon.

21 But the idea, look, if you had this,
22 I'm going to call it independent counsel, okay,

1 rather than special advocate because that has a
2 different connotation, or amicus I think has a
3 different connotation, but a small cadre.

4 And if I say I want that person to have
5 all the information you have, Mr. Baker, then he
6 has a choice. He can say, judge, okay, we're
7 going to appeal and find out if you can do that,
8 which may be the way to go. I mean that's the way
9 we do things as Judge Wald knows. If you don't
10 like what I do, go find three appellate judges,
11 they'll tell me.

12 MR. ZWILLINGER: One thing Judge Carr's
13 comments raised for me though is that the role of
14 the FISA Court as approver as opposed to resolving
15 an adversarial dispute, Judge Carr said that in
16 his time on the FISC there was not as much of an
17 adversarial role for the court and there weren't
18 these bulk collection decisions. So seeking
19 approval from the court, he had the right to
20 contact anybody he wanted in the government and
21 ask for information.

22 As someone who's been in an adversarial

1 role before the FISC I find the ex parte contacts
2 between the government and the FISC very difficult
3 to deal with and overcome. The fact that the same
4 judge who may have been involved in deciding that
5 the bulk collection is lawful, then be assigned to
6 the case to decide whether there's going to be an
7 adversarial challenge.

8 I mean it's not a different pool of
9 judges. It's not a magistrate issuing a search
10 warrant and a United States District Court judge
11 ultimately deciding if there should be
12 suppression.

13 So we're going in front of the same
14 pool of judges who have both an approval role and
15 an adjudicatory role and their ability to call in
16 ex parte contacts and get information from the
17 government may be different in an adversarial
18 proceeding than in an approval of an surveillance
19 proceeding.

20 MR. CARR: Well, but on the other hand
21 when the PRISM application first came in the
22 subsequent application, in all likelihood did not

1 go before the same judge, and that judge had the
2 independent authority to decide whether or not it
3 could be approved. So it's a different sort of
4 process.

5 It doesn't return to the same judge
6 because we're on rotation, these 90 expirations or
7 whenever. Once in a while I would get something
8 I'd had a year or two before, but it was very rare
9 that I got the sequential. And I don't think it
10 would be necessary in that situation where you go
11 in for renewal of something to go find the same
12 judge. In fact, I think it would not be.

13 MR. ZWILLINGER: My point is more that
14 the judges are playing two different roles.
15 They're working with the government, the Executive
16 Branch to approve a surveillance or say come back,
17 you haven't answered this, or I need some
18 expertise on that, and they're working through the
19 process of approval, but they're also the same
20 judge, the same court that listens to an
21 adversarial dispute whenever either a provider
22 wants to bring a challenge or if we create some

1 sort of additional advocate or amicus to being a
2 challenge. We have to talk about the court's dual
3 role and how to sort that out, I think.

4 MR. CARR: Well, I used that term
5 deliberately because I don't see the difference
6 between what I did as a judge on the FISC and what
7 I did as a magistrate issuing search warrants or
8 as a district judge later issuing Title IIIs.

9 I mean maybe the word approve, but the
10 process and review is the same. In that situation
11 I'm often the judge who winds up hearing the
12 suppression motion, and the law is quite clear I
13 can do that. So I don't see that there's that
14 much distinction, in fact, I don't think there's
15 any between the judge's job as a FISC judge and
16 the judge's job as an Article III judge or an
17 Article I judge magistrate in issuing more
18 conventional warrants and orders.

19 MR. MEDINE: Thank you.

20 Ms. Brand.

21 MS. BRAND: Thanks. I'd like to switch
22 gears a little bit from the adversarial process to

1 transparency. It's been the subject of some of
2 the other recommendations. And these questions
3 are more directed to Jim and to Judge Carr.

4 How feasible is it for FISC judges to
5 write opinions in the first instance with an eye
6 towards declassification or redaction later?

7 Just assuming for a moment we're
8 talking about prospectively as opposed to
9 retrospectively, is this an easy matter,
10 complicated? Can it be done?

11 MR. CARR: Well, first let me say it
12 was my experience, I mean I don't know about the
13 other judges with whom I served or judges today,
14 writing an opinion as we ordinarily understand,
15 that was a very unusual event. Because once
16 again, it's like with an ordinary search warrant,
17 you don't write an opinion. You look at it, if
18 there's probable cause you say, you issue it, a
19 Title III order, you issue it, and a FISA order,
20 you issue it.

21 MS. BRAND: In the unusual
22 circumstances though where there is an opinion.

1 MR. CARR: Again, when a judge, part of
2 my, implicit I suppose, when a judge felt the need
3 to actually write an opinion, and that's often
4 triggered by the notice from the government that
5 there's something going on that's unusual, and by
6 the work of the legal advisors. They too will
7 alert us to issues that call for further
8 consideration and reflection. I don't remember
9 the number of, quote, opinions, maybe a few pages,
10 maybe several pages I wrote, but it was a handful.
11 And I think that's probably -- so part of it is in
12 thinking about transparency, it's not like an
13 ordinary court with ordinary cases where day in
14 and day out you're writing opinions.

15 MS. BRAND: Right, but I'm trying to
16 figure out where there is an opinion, how easy is
17 it to -- because what you don't want to have is a
18 redacted opinion that's nonsensical because of the
19 redactions, right. So how easy is it to write
20 something that could be understood later in some
21 way in unclassified form?

22 MR. BAKER: So for example, in the

1 court of review, the first court of review
2 decision from '02, I think it was that clearly,
3 was written, in my opinion, it was clearly written
4 by the judges to publish it, because they boiled
5 down the classified stuff into a couple of
6 different sections, so that the legal analysis and
7 the historical background and so on and so forth,
8 they were able to put forward in a way that made
9 sense. It wasn't like a piece of Swiss cheese.
10 You could understand the logic and everything that
11 was going on and the classified stuff because it
12 was concise. And so --

13 MS. BRAND: You're talking about the
14 wall case?

15 MR. BAKER: Yes, exactly, yeah.

16 MS. BRAND: How translatable, because
17 that case clearly amicus participation was
18 feasible, right, and there was an opinion that was
19 public. So there was something about that case
20 that lent itself to public participation and
21 publication thereafter.

22 How translatable is that more broadly?

1 I mean how --

2 MR. BAKER: Well, if the court knows,
3 so if you were to have some act of Congress that
4 said, to the extent practicable, opinions of the
5 FISA Court shall be published or shall be
6 presented in a public, in a form that can be
7 readily published or something like that, if they
8 were sort of forced to do it basically, I think
9 they could do it in many instance.

10 There will be some instances where it
11 will be much more challenging. In some of the
12 very technical ones where the facts of the case
13 are interwoven with the legal analysis, that's
14 going to be harder.

15 In the FISC review decision it really
16 was a mega legal issue. There were a couple of
17 cases, if I recall correctly, that were at play,
18 but it really wasn't a factual or really heavily
19 technical kind of issue. It was much more of a
20 pure legal issue. So but my guess would be if the
21 court had that idea that it had to do that.

22 Another option might be, you know, the

1 court shall release an unclassified summary of the
2 key rulings of a case or something like that.

3 Sort of like headnotes or something where the key
4 --

5 MS. BRAND: Well, let me ask you about
6 that because we heard from another judge that he
7 would rather not see summaries because a summary
8 isn't always a full picture of what the opinion
9 would say, and so from that perspective redaction
10 is preferable to a summary.

11 Judge Carr, do you have a view about
12 that, if there were going to be an unclassified
13 summary versus just a redacted version of the
14 opinion, which one is better?

15 MR. CARR: Understanding that no two
16 judges might agree on whatever view I might have
17 thinking about this for the first time, again, it
18 all depends. What is the issue? Does it really
19 involve something that is classified or is it
20 simply, I mean can you recast it in a way?

21 I think it's impossible to predict in
22 advance how difficult or easy it might be.

1 However, were there a default or at least the
2 likelihood at some point of publication of part or
3 all of a decision, I think certainly a judge could
4 go into writing whatever he or she wrote with that
5 in mind and perhaps deliberately compartmentalize,
6 write the opinion with an eye to that.

7 But to try to tell you would it be easy
8 or difficult, it would certainly depend upon the
9 particular issue and the setting in which it came
10 up. It might be easy and it might be almost
11 impossible.

12 And I kind of like Jim's idea of a
13 summary. Without further detail, this is the
14 issue of law and we have approved, I have approved
15 this. Or if the court now sits en banc, and I
16 don't know if it ever has, but it has that
17 authority, which I think is very worthwhile.

18 But I can't really answer your question
19 directly, and I'm sorry.

20 MR. BAKER: If I can just add, you're
21 trying to find, it seems to me you're trying to
22 find balance here between disclosing,

1 unnecessarily disclosing classified information
2 that would harm us and providing adequate
3 transparency so people can understand what's going
4 on and have confidence in the system.

5 The summary is like a balancing type
6 thing. I mean on the one hand you're not going
7 to, you don't want to have no transparency and on
8 the other hand you don't want to have T.V. cameras
9 in the courtroom either, right. So it's an
10 option.

11 And what might make sense is, you know,
12 sort of a couple of different options for the
13 court to pursue or have available to give
14 transparency that they could figure out which is
15 the best fit in a particular case.

16 MR. MEDINE: I have a question for each
17 of the panelists which is, what is the role of
18 this outside person, whether they're an advocate,
19 or an amicus, or a staff attorney or whatever,
20 when they appear before the court?

21 And it's sort of really two questions.
22 One is, is there a charge to oppose everything the

1 government proposes?

2 And then secondly, how do they evaluate
3 assuming that they engage with the government, how
4 do they evaluate which arguments to make?

5 There are statutory arguments, there
6 are constitutional arguments, there are factual
7 arguments. How do they make those decisions and
8 who guides them in making the strategic decisions
9 they make in involving themselves in a case?

10 So maybe we'll start with Marc and go
11 on down.

12 MR. ZWILLINGER: I don't think they
13 should oppose everything the government seeks. I
14 think the goal of this isn't to make it harder for
15 the government to protect the country. The goal
16 of it is to make it simple for the government to
17 protect the country while respecting the
18 Constitution and to have somebody pointing out on
19 the other side what the constitutional balance is
20 versus the pure needs for, you know, security or
21 surveillance.

22 And I also think they'd lose

1 credibility before the court if they're just
2 opposing everything, as opposed to getting across
3 the message when this is important.

4 As to how to decide what cases to get
5 involved in or what arguments to bring, you know,
6 I do think the first person who occupies the
7 office should probably play a large role in
8 figuring that out. But it would occur to me that
9 novelty is one thing that's certainly there, bulk
10 collection, something that even if it's --

11 MR. MEDINE: So I want not as much
12 focus on when they should get involved as what
13 positions they should take once they're involved?

14 Again, do they argue the Constitution,
15 do they argue statutory noncompliance? I mean
16 lawyers strategize, but they partly strategize
17 based on who their client is. How does this
18 particular person make those decisions?

19 MR. ZWILLINGER: Right. So to try to
20 get at that in a short answer I would think you've
21 got it right as to who their client is if they
22 view their client as the, you know, either

1 American public or in some cases, you know, the
2 human race who has this sort of interest in sort
3 of human dignity and privacy in their
4 communications, their client is to offer the
5 perspective of those individuals who can't be
6 there to speak for themselves as to whether their
7 surveillance is appropriately narrowed or
8 necessary. And that may be both constitutional
9 and statutory.

10 I find it hard to say today how they
11 would choose between them. But I would think they
12 would be empowered to make both those arguments,
13 statutory noncompliance and constitutional
14 problem.

15 MR. CARR: Yeah, certainly I think that
16 they would have the authority and ability to make
17 whatever argument they thought was appropriate,
18 just like a lawyer does in any other instance,
19 whether it's in a trial court or in an appellate
20 court.

21 I think that the lawyer would be able
22 to make whatever argument he or she thought would

1 be plausible, credible and perhaps successful, in
2 a unique situation calling points to the court's
3 attention that the government isn't and that
4 lawyer thinks would be worthwhile.

5 But you raise an interesting -- a
6 thought occurs to me, and that is, and I think the
7 system I'm trying to propose could enable this,
8 lawyers often when confronted with new or
9 difficult issues talk to other lawyers and get
10 their input. What do you think? I mean I think
11 it's a natural source that a lawyer in that
12 situation would go.

13 So I think this is getting a bit more
14 elaborate I realize the further we talk, but on
15 the other hand, within the confines of what I'm
16 suggesting I think you could also enable this
17 small group, just like a small federal public
18 defender's office, they talk amongst themselves.
19 They're privileged. Nobody can make them disclose
20 it. You bounce ideas off.

21 And I think that would be very
22 important in an area where -- I mean part of the

1 problem is when these issues come up in front of
2 the FISC, nobody has been there before. You don't
3 have precedents. And you have to think things
4 through in a seminar kind of way.

5 So I think that's one way lawyers would
6 -- I'm sure Marc does that with his clients and
7 others in his office. What do you think? And
8 that's how it would honed.

9 I don't think we can prescribe a
10 template for you as to how that would occur. But
11 again, that lawyer would have as much opportunity
12 to raise whatever arguments the lawyer thought
13 were appropriate as the government in terms of
14 access to classified information, and now as I
15 think about it, at least within that small group,
16 talking amongst themselves and sort of jointly
17 coming up with how they go about representing.

18 And finally the question asked, no, I
19 don't think that that lawyer would be called upon
20 to dream up arguments just to dream up arguments
21 in opposition. He could well say, you know, we
22 have no opposition to voice to the government's

1 request. End of discussion.

2 MR. BAKER: As I mentioned, and I'll
3 just be brief, there are lots of issues associated
4 with the creation of this type of function,
5 office, whatever you're going to call it. But if
6 anything, I mean, it would seem to me that the one
7 thing you would want to do is make it clear to the
8 American people that this office is independent
9 and can decide whatever legal position it wants to
10 take in any particular matter. If it wants to
11 oppose the government, it can do so. If it wants
12 to say, okay, no objection, whatever. And if it
13 wants, constitutional issues, statutory issues,
14 factual issues, whatever.

15 I think you would just have to leave it
16 up to the people in that office or whoever it's
17 going to be to decide whatever approach they're
18 going to take. They have to be independent.

19 MR. MEDINE: Thanks. I think we have
20 time for another brief round, if we keep our
21 questions within our five minutes, starting with
22 Judge Wald.

1 MS. WALD: Okay. I've just got really
2 -- sorry. I've just got one question, and I'm
3 returning to the appeal question.

4 I recognize some of you haven't had the
5 chance to really research it or don't wish to
6 comment, but I want to raise this question. We've
7 been talking about the fact that the FISA Court is
8 a kind of unique animal. I mean it is, I mean I
9 think it's thought of or its conceptualists
10 thought of it as an Article III court, but as has
11 been pointed out it does have some sort of
12 auxiliary, whether it's preventive or approval
13 kinds of functions.

14 Here, as a former Article III judge, I
15 think I share with Judge Carr, the problem is that
16 this court inevitably must and has pronounced on
17 constitutional questions, questions of statutory
18 interpretation, which I think inevitably become or
19 have to become part our, to the extent they're
20 disclosed, have to become part of our
21 jurisprudence.

22 So I think the appeal question is so

1 important to me because not only, I think, some of
2 the FISC counsel have, you know, opined on it,
3 that there may be constitutional questions, so has
4 the Congressional Research Service.

5 They are applying, you know, absolutely
6 a typical, traditional Article III standing in a
7 situation where the court is deciding Article III
8 questions, but in its original conception it's
9 devoid of one of the most important points of
10 Article III courts, namely people who have an
11 interest in the proceeding not being able to have
12 any voice, for good reason. I understand the
13 secrecy that's involved in national security.

14 But I guess I'm trying to pick your
15 brains if there is any way to try to solve that
16 question, because to leave these, the highest form
17 of jurisprudence, namely constitutional questions,
18 sometimes questions of statutory construction at a
19 point where they can't be availed of the process
20 which every other part of federal jurisprudence
21 has, namely, you know, an upper tier, even to the
22 FISC, to the FISCR kind of thing.

1 Some people have suggested a kind of
2 certification but that's had its opponents too.
3 They think you can't do that constitutionally.
4 You've got any positive thoughts on how this --

5 MR. ZWILLINGER: I'll take a shot at
6 it. I hate to keep coming back to the 2008 court
7 of review decision, but the government argued in
8 that case that there wasn't standing for the
9 providers to challenge. And the court ruled that
10 since Fourth Amendment rights were at stake, the
11 question of whether the provider could litigate
12 those on behalf of users was a prudential standing
13 doctrine, not a constitutional standing doctrine
14 and Congress could waive the prudential standing
15 doctrine and it had done that by putting the
16 standing provision for providers in Section 702.

17 So I don't see the hurdle quite as
18 insurmountable. If we agree that there are U.S.
19 persons who have Fourth Amendment rights and they
20 would have standing and someone else can litigate
21 that issue on their behalf, it's a prudential
22 question which Congress can waive, not a strict

1 constitutional one. At least that's my
2 interpretation of that decision and my offer of
3 help.

4 MR. CARR: In less legalistic terms,
5 because I'm not sure I fully understand the
6 concept of prudential standing, but it seems to me
7 that there a couple of different circumstances.

8 One may be an instance where there in
9 fact is a target, a person who's named in the
10 order. And that's easy. You can obviously
11 appoint.

12 Or it seems to me that you could
13 appoint, that that person could be designated to
14 represent the interests of persons affected by
15 this, potentially affected by this order. I mean
16 I think that's what you're saying. They have bona
17 fide interests.

18 And there's a scrap of doctrine that
19 may not be applicable that you can comment on.
20 Judge, isn't there some doctrine that says where
21 you have a situation that is capable of repetition
22 but will be evading review unless you go ahead and

1 decide it, even though arguably the particular
2 circumstance is now moot.

3 I mean, I hadn't thought about the
4 Constitution issue but it does seem to me -- and
5 also Congress gives courts its jurisdiction.

6 MS. WALD: Congress created the
7 original FISC and in a sense you might say decided
8 that this body of people, for good reason I'm
9 saying, couldn't be informed and become a regular
10 participant certainly if they have terrorist, you
11 know --

12 MR. CARR: I think the more serious and
13 unanswered constitutional question is can a court
14 play any role in overseeing Article II activities?
15 Congress, the courts and the Executive have all
16 agreed, yes, the FISC is a good thing and FISA is
17 a good thing and we don't want to push it one way
18 or the other, which is something I would suggest
19 to the people proposing what I would suggest may
20 be fairly radical changes, keep in mind all it
21 would take would be the Executive saying, no,
22 we're not going to go along with this. Go to the

1 FISA Court of Review, whatever it says, and
2 ultimately the Supreme Court. And the Supreme
3 Court might well say the whole structure
4 collapses. Who knows? I mean that's never been
5 tested and I don't think we want it to be tested.

6 MR. MEDINE: Mr. Dempsey.

7 MR. DEMPSEY: Jim Baker, you said in
8 your opening remarks, hopefully I'm not misquoting
9 you, but I think you said something along the
10 lines of, we've gone as far as we can go with the
11 FISA Court as, my words, quasi-regulatory body.
12 Would you expand upon what you were referring to.

13 MR. BAKER: Well, I was referring
14 mainly to Section 702, but I think it also applies
15 to Section 215 as well, which is really, I think,
16 I said the outer limits of what we can reasonably
17 expect a court to do, and to not, we shouldn't
18 think of them as some sort of super inspector
19 general that's, you know, conducting oversight,
20 free-ranging oversight of the activities of the
21 intelligence community.

22 I just think there are significant

1 constitutional issues with that. I think there
2 are a lot of practical issues with that. The
3 court's just not resourced to do that. The judges
4 are not trained to do that in that way. They just
5 play a different role.

6 And so I just, I'm trying to set
7 expectations, I'm urging you to set expectations
8 in a realistic way with the American people about
9 what you can reasonably expect the court to do.

10 The same applies to Congress. I mean,
11 what can the members of Congress and their staff
12 reasonably be expected to do when it comes to
13 conducting oversight of these agencies.

14 And in my opinion it's primarily the
15 responsibility of the President of the United
16 States to conduct effective management control and
17 oversight of the intelligence community. That's
18 what I was trying to drive at.

19 And I think if you, to go back to the
20 original point, if you look at the structure of
21 702, you've got the court approving these
22 procedures, several different types, looking at

1 the certification, but not really engaging in
2 review of individual determinations and so on.
3 And then you have sort of after the fact review of
4 things that have happened. I just think you've
5 gone pretty far in terms of what you can ask a
6 court to do to conduct oversight of the
7 intelligence community.

8 MR. DEMPSEY: I actually have no other
9 questions on this round, so I'll yield. I
10 appreciate the witnesses being here. It's been
11 very helpful. Very helpful.

12 MS. COLLINS COOK: I did want to take
13 you up, Judge Carr, on an invitation you had given
14 us earlier, which was to talk about the legal
15 advisors and what role they play, because I think
16 there's definitely a sense, and I mean no offense,
17 having been a law clerk, but that these are junior
18 attorneys who are law clerks. And I'm wondering
19 if you would talk a little bit more about who the
20 legal advisors actually are and what role they
21 serve.

22 MR. CARR: When I started in the court

1 in 2002 there was one legal advisor. When I left
2 I think there were four or five, I can't remember.

3 These are, they are neither law clerks
4 nor magistrates, okay. It's a unique role that
5 they perform. I think I can speak for myself when
6 I say, and I'm the author of a treatise on
7 electronic surveillance so I know more perhaps
8 than most FISA judges going into it, but they know
9 more about FISA, FISA law and national security
10 law, the workings of the agencies than any
11 individual judge can. And we rely upon them and
12 their judgement to assist us in making decisions.

13 To give you an example, they get by
14 FISA rule, FISC rule, seven days before we get an
15 application, and they review it carefully. It's
16 called the read copy. And Jim will confirm, I'm
17 sure, there's a lot of push back between the legal
18 advisors on behalf of the court and OIPR.

19 I know from personal experience there's
20 a lot of push back between OIPR and the agencies.
21 As someone said this morning, they don't want to
22 present junk because if they do, we're going to

1 lose confidence in it, and it's going to be much
2 more difficult unless they are straight up with
3 us.

4 But the legal advisors, and not
5 infrequently I would come in and let's say I would
6 have X number of cases set on my docket, and that
7 number grew substantially when I was there. But I
8 would be told this case, that case, the other case
9 and another case are off docket.

10 And it's my distinct sense that it was
11 off docket, in other words would not be formally
12 presented to me for review because of the
13 interaction between the legal advisors and the
14 OIPR attorneys and the agencies, whom I believe
15 the legal advisors called them directly with
16 questions and problems.

17 That was a core part of their job was
18 rigorously to vet the applications. And one of
19 the things that I think should be considered would
20 be that the number of instances, the instances in
21 which an application is submitted for review by a
22 legal advisor but never presented to a FISC judge

1 for consideration, that those two should be
2 registered, recorded and published because I think
3 there would be -- I mean was it a large
4 percentage? No, but it was a, Jim, would you
5 agree with me, fairly regularly cases would come
6 off docket.

7 MR. BAKER: Or they'd be, they'd either
8 come off completely or they'd be postponed to
9 another week because we were trying to resolve
10 some question that the legal advisor had raised,
11 yes.

12 MR. CARR: Right.

13 MR. BAKER: It would take us some time
14 to finish that analysis.

15 MR. CARR: But I do think it would not
16 be that difficult to give every read copy a number
17 and then that keeps that number and when it comes
18 off docket, it never comes back, they decide not
19 to present it, and there are instances like that,
20 I assume because of push back from the legal
21 advisors. And that would, if nothing else, show
22 that the rate of rejections in terms of the

1 overall operation of the court is higher than the
2 simple turndown by a judge.

3 But I mean to say that these are law
4 clerks, they occupy a unique role. And then we
5 have great confidence in them. They work for the
6 court, but in a very important way they help
7 ensure that we make the decisions we should.

8 Very often they would write a
9 memorandum for us about some aspect. And then, of
10 course, we would sit down and read these things.
11 And they're not two page search warrant
12 applications. They're 40, 50, 60, 80, 100 pages.
13 Very thorough, like Title IIIs, every bit as
14 lengthy and thorough as a Title III.

15 And we would often have questions, and
16 I would call an OIPR attorney and say, look, can
17 you give me this or that.

18 And on occasion I would actually have
19 hearings. I would question the agent and the
20 lawyer under oath, always on the record, even
21 though it would never be public. And I'd make a
22 finding and I would determine that my questions

1 had been answered, so.

2 MS. COLLINS COOK: Thank you, all three
3 of you for being here today. I appreciate part of
4 what we're doing here is attempting to educate
5 ourselves, part of what we're doing is attempting
6 to educate other people who might be thinking
7 about this, so I appreciate the thought and the
8 time that you've put into your answers.

9 MR. CARR: And certainly speaking for
10 myself, if there are other questions that the
11 agency has, feel free to communicate with me. I'd
12 be glad to answer them.

13 MR. MEDINE: Thank you.

14 Ms. Brand.

15 MS. BRAND: Thank you. I wanted to
16 follow up on something that I asked the government
17 witnesses about this morning and there wasn't a
18 full, we didn't get to do a full answer on that
19 panel, which is going back to the 215 bulk
20 metadata collection and the RAS standard.

21 Jim, I think you were in the audience
22 for this discussion about if there were a

1 requirement that the government submit to the FISC
2 after the fact the RAS selectors.

3 So this phone number is now a selector
4 and here's the paper trail that is the basis on
5 which the selector was established.

6 What would the court do with that? I
7 mean first of all, do you think that the court
8 could do something useful with that? Would this
9 be an actual check on the system, or would it
10 overwhelm the court? Can either of you speak to
11 how that would work in practice.

12 MR. BAKER: I don't see how it would
13 overwhelm the court and --

14 MS. BRAND: How it would or would not?

15 MR. BAKER: Would not.

16 MS. BRAND: Would not, okay.

17 MR. BAKER: I don't see how it would
18 overwhelm the court. You just have an Excel
19 spreadsheet, you write down the selector, you
20 write down the basis, the little field off to the
21 side, date, time, all this kind of stuff, and you
22 submit it to the court on a regular basis so it's

1 not too onerous for the government to comply with
2 because I think that is a real issue.

3 And then I would imagine that the court
4 would look for patterns to see if things were
5 going along in a way that they, that was
6 consistent with their understanding of what they
7 were thinking when they approved this thing. And
8 it would be an additional check.

9 To me, I have to say I don't see that
10 as that onerous of an additional obligation. And
11 I do think it would be useful for the court to
12 have additional transparency. And it seems like
13 it's something that would give the American people
14 additional confidence that what's going on is
15 legitimate and appropriate.

16 MR. CARR: I would think to do that you
17 would have to first of all, the analogy is to the
18 periodic progress reports that all Article III
19 judges get with a wiretap, review, minimization.
20 Again, it's all in the record, ex parte. Put them
21 under oath, how is the investigation going, are
22 you getting anything. I make a renewed finding of

1 probable cause for the Title III tap. Necessity,
2 you're doing a good job at minimization or you're
3 not.

4 So it does seem to me that this is a
5 function that Article III judges would be familiar
6 with performing in a similar way.

7 The one thing that occurs to me though
8 it seems to me for it to be useful you would have
9 to go back to the particular judge who issued the
10 PRISM order, whatever the order was.

11 MR. BAKER: This is 215.

12 MR. CARR: Pardon?

13 MR. BAKER: This is 215.

14 MR. CARR: 215, yeah. To go back to
15 that judge because that's the judge who gave the
16 original authority, rather than whatever judge
17 happens to be there that week.

18 Again, I don't know. But I suppose in
19 time any judge would develop enough familiarity to
20 have enough handholds to evaluate the reasonable
21 articulable suspicion in this context.

22 MS. BRAND: And Jim, just quickly for

1 you that there was some discussion during Beth's
2 question about the back and forth between the
3 court's lawyers and the government.

4 Can you talk about the back and forth
5 that happens within the government? I mean is
6 there a quasi-adversarial process within the
7 government before an application ever gets to the
8 FISC? Who's involved in the application? Can you
9 talk to that?

10 MR. BAKER: So it depends what kind of
11 application, whether it's from the FBI or NSA,
12 you're going to have different levels of review.

13 With the FBI you have review within the
14 field office, you would have review at FBI
15 headquarters. It would come over to the Justice
16 Department. You would have review there. And
17 then it would go to the FISC.

18 At NSA you're going to have similar
19 type of review. Obviously there's no field office
20 in that sense.

21 But look, I mean the review and the
22 meticulousness and the care that people put into

1 these things is substantial. There is a lot of
2 dialogue back and forth between every level, among
3 every level of this. There's back and forth
4 between FBI headquarters and the field. There's
5 back and forth between DOJ and FBI, or DOJ and
6 NSA. There's a huge amount of back and forth.

7 And I always took it as a huge amount
8 of my responsibility to make sure that I
9 maintained at all times the credibility of the
10 Justice Department in front of the FISA Court so
11 that we were transparent with the court about what
12 was going on so that the court knew that we cared
13 deeply about the accuracy of these applications.
14 That when we made mistakes, as we did, we brought
15 them to the attention of the court. That we tried
16 really hard not to make mistakes.

17 And so it was really, you know, the
18 Justice Department, again in my opinion, doing its
19 job, executing its responsibilities under the
20 Constitution as delegates of the President to help
21 him take care that the laws are faithfully
22 executed. Congress passed this law, it's our job

1 to enforce it. We're going to do our best to make
2 sure that it's enforced in the right way. And if
3 we think that the agency hasn't met the standard,
4 then we're going to tell the agency they haven't
5 met the standard yet and they've got to do X, Y
6 and Z to do that.

7 So I mean I think that this system has
8 worked extremely well so far, but it's clear now
9 and it's painful to me to see that some percentage
10 of the population of the United States doesn't
11 think that, and so we need to take that seriously
12 and figure out how to deal with it. And that's
13 your job.

14 MR. MEDINE: Thanks. In the interests
15 of keeping, because I just want to ask one final
16 question, which is the point was made earlier that
17 this outside party, advocate, amicus might have a
18 role in compliance reviews. What role would that
19 be and how would that play out?

20 MR. CARR: Well again, in my thinking
21 about it, I mean once again, I mean many times
22 compliance, a noncompliance notice is really quite

1 straightforward and quite simple. But in the
2 event that you had something that was more complex
3 and you wanted to be really sure that the problem
4 had been identified and addressed and would not
5 recur, again I think at the very least the FISA
6 judge should have the opportunity to have this
7 independent counsel participate in an adversary
8 mode with the government prosecutor and conduct a
9 hearing the way we do with a suppression hearing
10 or whatever, and then make a decision.

11 One would hope that the decision
12 ultimately would be okay, things weren't as bad as
13 they looked and it was good faith and it's been
14 fixed.

15 But I do think that there would be a
16 role for the attorneys whom I envision
17 participating in the process from time to time.

18 MR. MEDINE: Other panel members have a
19 comment on that?

20 MR. CARR: It's not a career enhancing
21 move for somebody in an agency to make a mistake,
22 to get it wrong. And one of the things that

1 impressed me as a young magistrate about the FBI
2 and DEA and so forth, and I had the same kind of,
3 I grew up politically in the 60s. I had
4 apprehensions about the government and FISA secret
5 court. And one thing I can assure you has
6 impressed me from day one and throughout my
7 activities in the FISA Court is the people who do
8 this work want to get it right. Not just the
9 lawyers in the Justice Department, but the agents
10 out in the field.

11 And the other thing I want to say is, I
12 alluded to this before, I know that at least the
13 FBI on frequent occasion was not happy with them
14 because they were not going forward to present
15 something that the bureau very much wanted it to.

16 It's not an adversary relationship but
17 it's not a hand in glove relationship, or it
18 certainly was not when I was on the court. One
19 did not have that sense that they were just
20 presenting anything that the agency wanted.

21 MR. ZWILLINGER: Just to comment
22 briefly, I would just be very careful about using

1 the independence of this office to start getting
2 involved too far in what might lead them to be
3 captured by Executive Branch activity.

4 That is, if we believe there's some
5 role for an adversary in this process, some role
6 beyond what the legal advisors who sound like
7 they're both brilliant and helpful play, then that
8 person should be, should retain some of the
9 independence, and they shouldn't play too many
10 roles or positions in this so that they can both
11 challenge from an independent point of view and
12 convey that independence to the American public.

13 MR. MEDINE: I want to thank the panel
14 for giving us a unique insight into the operations
15 of the Foreign Intelligence Surveillance Court.

16 We'll take a break and resume at 2:45.

17 MR. CARR: May I just say one thing
18 that occurred to me this morning?

19 MR. MEDINE: Sure.

20 MR. CARR: And also before the Senate
21 Judiciary Committee, let's all keep in mind what a
22 remarkable country we live in where we're having

1 this kind of conversation about these issues, and
2 what a remarkable institution we have in the
3 Foreign Intelligence Surveillance Court, because I
4 don't think any other country has anything like
5 it. Can you imagine this conversation occurring
6 anywhere else in the world? And I think we should
7 all keep that in mind and take pride in that.

8 MR. MEDINE: Excellent point while we
9 go on our break. Thank you.

10 (Off the record)

11 MR. MEDINE: All right. We'll be
12 starting the final panel which involves academics
13 and a former member of Congress.

14 We're pleased to be joined by Jane
15 Harman, who's the Director, President and CEO of
16 the Woodrow Wilson Center and a former Member of
17 Congress, Orin Kerr, who's a Fred C. Stevenson
18 Research Professor at George Washington University
19 Law School, Stephanie K. Pell, who's the Principal
20 in SKP Strategies, a former House Judiciary
21 Committee Counsel and Federal Prosecutor, Eugene
22 Spafford, Professor of Computer Science and

1 Executive Director, Center for Education and
2 Research in Information Assurance and Security at
3 Perdue University, and Stephen Vladeck, Professor
4 of Law and the Associate Dean for Scholarship at
5 American University Washington College of Law.

6 To the panel members, I understand
7 you're free to make a brief statement and then
8 we'll do another round of five minute questioning
9 on the panel.

10 So Congresswoman Harman, if you'd like
11 to start.

12 MS. HARMAN: My apologies for being a
13 few minutes late, but I'm delighted to be here. I
14 consider myself one of your grandmothers. I was a
15 principal co-author of the Intelligence Reform Law
16 in 2004, which established you.

17 And one of the tragedies I think
18 history will record is that you were not fully
19 functioning until May of 2013. That is about
20 eight and a half years lost of a very, very
21 critical mission.

22 And let me just say that the goal in

1 the law, and certainly my personal goal, was to
2 have a group inside that would make certain that
3 privacy and security, or that liberty and security
4 were reinforcing values in the policies and
5 practices that we established under the law.

6 And if ever that function were needed
7 it is right now. It is unfortunate, at least to
8 me, that you are one of the best kept secrets in
9 Washington. I know you're making a massive effort
10 to get out there and I commend you for it, but I
11 think the need is urgent.

12 And you uniquely, among the different
13 groups now looking at some of our policies and
14 practices, I think are in a position to make sure
15 from the inside that we are doing the right
16 things.

17 Let me just make two other points.
18 One, I was in Berlin, Germany this week, no, last
19 week, a week ago today at a dinner of top policy
20 types and think tank leaders and business people,
21 all of whom were shocked and horrified by the
22 revelations in European newspapers.

1 When I told them that there was a
2 Privacy and Civil Liberties Board in the United
3 States and it is now holding hearings and I'm
4 testifying next week, they looked stunned, and
5 said, gee, that's wonderful. I hope that a group
6 like that will also be in touch with foreign
7 governments.

8 And so I put that out there. I'm not
9 sure whether that's in the mandate or it isn't,
10 but it might be interesting to think about
11 connecting to those folks and maybe forming some
12 common cause about ways to look at the practices
13 and procedures of different countries.

14 And finally, I would just offer my own
15 observation about all of this, which is that we
16 need, this isn't maybe your mandate, but our
17 government needs crisis management 101. It seems
18 to me as a recovering politician that when bad
19 stuff is coming your way, when, let's just imagine
20 some guy named Snowden has taken a lot of stuff
21 from the government and it's dribbling out, you
22 get ahead of it, and you figure out a frame, and

1 you figure out a context, and you talk about what
2 else could come out and what it means.

3 And this is just free advice again from
4 somebody who spent 17 years in the United States
5 Congress. Some crisis management function at the
6 highest level of our government I think could be
7 helpful, along with a very robust Privacy and
8 Civil Liberties Board.

9 So I'm delighted to be here. I don't
10 know that my testimony will be as technical as my
11 well-qualified colleagues, but I have been in this
12 game for a long time and I passionately hope that
13 things turn out well for our country and that we
14 have both security and liberty to look forward to.

15 MR. MEDINE: Thank you, Congressman.
16 Professor Kerr.

17 MR. KERR: Thank you for the invitation
18 to testify here this afternoon.

19 The FISA statute is premised on a
20 search warrant model, putting Article III judges
21 in the position of judges evaluating search
22 warrant applications. And that model isn't

1 working because the search warrant model is
2 premised on the judge serving essentially a
3 ministerial function.

4 When a judge reviews a search warrant
5 application the judge is looking for probable
6 cause, looking for particularity, but is not
7 trying to conduct a comprehensive review of
8 whether the statute is being applied correctly,
9 how the statute should be interpreted and what the
10 constitutional implications might be of the
11 warrant, if issued.

12 That doesn't work in the high
13 technology area because technology is simply
14 changing too quickly.

15 Judges are therefore being asked to
16 resolve difficult issues of interpretation which
17 they are just not competently equipped to answer
18 in the context of an ex parte application such as
19 a search warrant application.

20 And the various proposals that were
21 discussed earlier this afternoon at the FISC panel
22 were really about various ways that the FISC could

1 be restructured to make amendments to the warrant
2 model.

3 The special advocate approach is one
4 approach, encouraging disclosure of
5 interpretations is another approach. And both of
6 those are I think, are interesting and important
7 and promising ideas for how to reform the Foreign
8 Intelligence Surveillance Act to deal with new
9 technologies.

10 Let me suggest two other approaches.
11 One, which has been discussed and implemented, and
12 the other which has not been.

13 One approach is that of sunset
14 provisions, having the government's authority
15 lapse for a certain number of years and then
16 expire, putting the burden on the government to
17 seek renewal of that power. I think sunset
18 provisions which were originally designed to have,
19 sort of act as a testing time to see if the
20 government still needs that power a few years
21 later.

22 Today instead, in light of new

1 technologies is really a way of ensuring that the
2 government can go back to Congress, or rather has
3 to go back to Congress to seek approval for any
4 new interpretations of the law.

5 So combining the sunset authority with
6 disclosure of interpretations that the FISC is
7 taking is, I think, one important step.

8 Another approach which has not been
9 suggested so far would be a rule of lenity for
10 foreign intelligence surveillance law. You may be
11 familiar with the rule of lenity in the criminal
12 context. The idea is that when interpreting a
13 criminal statute judges should adopt the narrower
14 interpretation of the criminal law, and that
15 requires if the government wants to adopt, have a
16 broader interpretation of the criminal law they
17 have to go to the legislature and have the
18 legislature enact it. The idea being that the
19 laws are ultimately up to Congress, not up to the
20 courts.

21 A rule of lenity for surveillance law
22 would serve a similar function. The idea would be

1 if the government goes to the FISA Court and says
2 here's an interpretation of the law, if it's a
3 close call the default should be for the FISA
4 Court to reject the interpretation and to tell the
5 Executive Branch that they have to go to Congress
6 to get Congress's approval for that interpretation
7 of the statute.

8 This would force the Executive Branch
9 to go to Congress and not try to seek approval of
10 new programs from courts that are poorly equipped
11 to analyze the questions here, especially
12 involving the normative desirability of these
13 programs.

14 Effectively the sunset provisions and a
15 rule of lenity working together with disclosure
16 would force the Executive Branch to keep going
17 back to Congress as technology changes to have
18 Congress whether to approve or disapprove any new
19 surveillance programs. Thank you.

20 MR. MEDINE: Thank you, Professor Kerr.

21 Ms. Pell.

22 MS. PELL: Thank you to the members of

1 the board for inviting me to testify today. It's
2 quite an honor.

3 Putting on my hat as a former
4 congressional staff member, I'd like to raise two
5 process or transparency points that I think relate
6 to some of the discussions on both of the earlier
7 panels.

8 We heard on the prior panel the idea
9 that the FISC having had or currently having a
10 mechanism to seek review of outside technical
11 experts.

12 I think that is an excellent idea but
13 it is an equally important resource for staff
14 members and members of committees. In my
15 experience working on reform of the Electronic
16 Communications Privacy Act, which was not done
17 under essentially working with classified
18 information, myself and my colleagues were able to
19 contact outside experts, professors at
20 universities, people who had worked in the
21 telecommunication industries for decades, in order
22 to get a view of current technology and its

1 capabilities and where that technology was going
2 in the future.

3 Now, of course, we heard from the
4 government also and it shouldn't surprise anyone
5 to hear that the government's views often did not
6 a hundred percent comport with the views of these
7 outside experts.

8 What I'm saying shouldn't be either
9 surprising or seen as a criticism. The government
10 of course is an advocate. It has a very important
11 mission to do and it's going to present the views
12 of technology in a way that best represents its
13 positions.

14 But what these outside experts could do
15 in addition to often getting a different view from
16 government, was help the committee look towards
17 the future to understand where the technology and
18 its capabilities were going so that in the course
19 of trying to write statutes that wouldn't become
20 obsolete with the next new iPhone model, we had
21 the necessary information for forward projection.

22 Secondly, and this point goes more to

1 the discussion on 215 and something, Judge Wald,
2 you raised on the first panel about things that
3 have been said in different press outlets by
4 different experts regarding the fact that the
5 government's interpretation viz-a-viz bulk
6 collection and relevance was perhaps novel or a
7 little idiosyncratic, certainly not something that
8 even people who perhaps were experts in
9 surveillance law could read that statute and say,
10 oh, I could see how the bulk collection authority
11 would be operating under this statute.

12 What I'd like to raise is a problem
13 that occurs from a process level, as a committee
14 staff member especially on the Judiciary Committee
15 where certainly we hear classified information and
16 we often need briefings, to have briefings behind
17 closed doors, but committee staff members and
18 members interact with nongovernmental stakeholders
19 who have real interests in how these statutes are
20 written and how they affect the privacy interests
21 of the general public.

22 When you have a situation that a

1 government's legal interpretation essentially is
2 hidden from public disclosure, the dialogue that
3 must occur between the staff and the committee
4 members and these nongovernmental constituencies
5 frankly can be very dysfunctional.

6 Because when you discuss why you want
7 to make a change to a statute but are not able to
8 talk about what you think that change will do, it
9 can have the effect of having those
10 nongovernmental constituencies ironically argue
11 for changes in the law or reject proposals that
12 are not in their interests.

13 I think that raises a very problematic
14 process question, calls into question the
15 integrity of the legislative process with respect
16 to legal interpretations of statutes that must
17 remain essentially hidden from public disclosure.
18 Thank you.

19 MR. MEDINE: Thank you, Ms. Pell.
20 Professor Spafford.

21 MR. SPAFFORD: I'm not a scholar of the
22 law but of systems and I studied systems for many

1 years and find ways where they can be exploited or
2 where they can be bolstered. And I'd like to
3 present to you two high level thoughts about
4 systems viewing this.

5 The first is we've heard from many
6 people today and over the past many months about
7 how carefully this is controlled. It's vetted.
8 The requests are scrubbed. The information is
9 closely guarded. And we can perhaps take that as
10 given and realize that we do have a number of
11 people who are working very hard in the nation's
12 defense and the nation's interest.

13 The concern with privacy however is
14 that if those systems are constrained and
15 controlled within a very small private, closely
16 held group then it is possible that under
17 political circumstances or stress they can swing
18 out of control beyond what we intended.

19 And this is by no means unusual given
20 the country's history. We look at things like the
21 Alien and Sedition Act, the Japanese internment in
22 World War Two, the COINTELPRO investigations, the

1 McCarthy hearings, and President Nixon's enemy's
2 list is just a few where government systems were
3 then used for political aims or for aims that were
4 then later ruled unconstitutional.

5 So what we need to do is look at where
6 are the points at which this can be controlled,
7 where are the points at which we should observe to
8 make sure that this system cannot be subverted.

9 And we're lacking in the transparency
10 and the openness necessary. We don't have the
11 adversarial capabilities. The fact that people
12 who have these orders served against them cannot
13 talk about them, cannot bring them up before a
14 court are all considerable problems in terms of
15 righting any wrongs or oversights. That should be
16 addressed.

17 In particular we have heard how some of
18 our elected representatives are unable to hear all
19 of the information about these programs, to engage
20 their cleared staff and to have conversations with
21 each other about some of the issues involved.

22 To my knowledge we have not elected any

1 terrorists to Congress, at least not of the kind
2 that we're looking for. We are not in a position
3 where we have terrorists in the judiciary, or
4 terrorists operating our ISPs. To prevent those
5 individuals from helping to safeguard our privacy
6 and our constitutional rights is really
7 counterproductive to the interests of the nation.

8 So I would suggest that you look at
9 that as one thing that might be considered. In
10 general I believe that classification is over-
11 used. Anything that's classified should be
12 classified only to protect the safety of a party
13 or for operational efficacy.

14 It should not be used to hide things
15 from the American public. Things that are
16 classified when they come out, the American public
17 should say it's too bad we lost that capability
18 but they shouldn't be ashamed of what our
19 government is doing. And we have seen instances
20 of that I believe in the last few months.

21 The second comment that I'll make very
22 briefly about systems is more technical. I

1 circulated to you a set of fair information
2 privacy practices that have been put together by
3 the U.S Public Policy Council of the ACM.

4 These help govern good privacy and
5 databases. I would ask that you look at those as
6 you consider possible changes. The more of those
7 that are upheld the better we protect the privacy
8 of information.

9 And the more information we collect the
10 more likely we are to collect noise, particularly
11 if we have that information stored for a long
12 time. In any system the more we try to avoid
13 false negatives, that is missing cases of things
14 we're looking for, the more likely we are to
15 generate false positives.

16 And there is a concern as well for the
17 American public that in the process of trying to
18 be sure that we stop every terrorist threat we
19 cast a net that is too likely to engage those
20 individuals who are involved in unusual but not
21 illegal behavior.

22 And I'll be happy to answer your

1 questions later. Thank you.

2 MR. MEDINE: Thank you, Professor
3 Spafford.

4 Professor Vladeck.

5 MR. VLADECK: Great, thank you,
6 Chairman Medine, members of the board. It's a
7 pleasure to be here. You know, given the lateness
8 of the hour and the far more interesting nature of
9 your questions I'm going to try to be very brief.

10 We've heard a lot already today about
11 the idea of a special advocate and so I thought
12 I'd focus my short opening remarks on that
13 proposal.

14 I suspect the members are familiar with
15 a Congressional Research Service report that was I
16 think disclosed last week about constitutional
17 concerns with the special advocate. And I thought
18 I'd briefly address the three major ones that the
19 report raises.

20 First the report suggests that a
21 special advocate would raise Article II problems
22 with regard to the appointments clause and how

1 that office is set up. I actually think this is
2 perhaps a non sequitur.

3 I don't really think there's any
4 current proposal, including the Leahy-
5 Sensenbrenner bill that would actually constitute
6 the special advocate as anything remotely
7 resembling what the Supreme Court referred to as
8 an officer of the United States in Buckley versus
9 Valeo. I'm happy to elaborate on that but I
10 actually think this is a bit of a red herring.

11 The second bucket of issues that the
12 CRS report raises is concerns about adverseness in
13 the FISA Court and in FISA proceedings. Of course
14 this has been a structural concern in FISA since
15 long before the current controversies. Indeed
16 Judge Silverman when he testified about FISA in
17 1978 raised this exact concern as a constitutional
18 objection to FISA.

19 I'm happy to elaborate more on why I am
20 not convinced that this is a problem. I think the
21 only relevant point for now is that a special
22 advocate would not exacerbate any adverseness

1 concerns that currently exist.

2 That is to say there may be adverseness
3 concerns under 702, under 215 with FISA as
4 currently constituted, having an adverse party
5 only should ameliorate those concerns and not make
6 them worse.

7 Instead I actually think the hardest
8 issue raised by the CRS report and the one that I
9 do think is the biggest head scratcher for the
10 special advocate is the appeal question. So the
11 Supreme Court just said this summer in the
12 Proposition 8 case that a party must have a direct
13 stake in the outcome in order to appeal an adverse
14 decision by a lower court, as within the Article
15 III system. And I for one am pretty confident
16 that the FISA Court is part of the Article III
17 court system. And obviously I think some of the
18 current proposals would not invest the special
19 advocate with such a direct stake in the outcome.

20 So it seems to me that there are two
21 responses to the problem posed by the Perry
22 decision. The first is to create a direct stake

1 in the outcome. That is to say to actually have
2 the special advocate not just representing some
3 amorphous undifferentiated interest, but to
4 actually represent U.S. persons whose
5 communications might be intercepted pursuant to
6 the surveillance being authorized.

7 That might raise policy questions that
8 are difficult to think about. Certainly we have
9 precedent in our legal system for such sort of
10 separated representation, Guardian Ad Litem are a
11 good example, class counsel under Rule 23(b)(2)
12 class action, even for example, the habeas lawyers
13 for the Guantanamo detainees, who routinely have
14 access to classified information that cannot be
15 shared with their clients.

16 So one possibility around this problem
17 is simply to create that direct stake. The other
18 is to avoid it. And so I suspect there's been
19 some discussion among the board about the idea of
20 certification.

21 That's one possibility where you could
22 have the FISA Court certify particularly difficult

1 legal questions to FISCR. This could be modeled,
2 for example, on the Supreme Court certiorari
3 statute 12542, which allows for circuit courts
4 right now to certify questions for the Supreme
5 Court, quote, at any time, unquote. And whether
6 or not a party is asking for such certification.

7 Another possibility would be to borrow
8 an example from the bankruptcy context and
9 actually bifurcate the FISA Court's decisions into
10 those that the FISA Court is allowed to render as
11 a final matter. Those could be sort of cases not
12 presenting novel questions of law or
13 reauthorization cases, in which case the FISA
14 Court would be empowered to act finally, and those
15 in which it could actually only issue a
16 provisional report and recommendation that
17 actually had to be confirmed by the FISA Court of
18 review on appeal. That's how the bankruptcy court
19 system works right now with regard to core and
20 non-core proceedings. I think that's another way
21 to sort of get around the problem.

22 The larger point, and then I'll stop,

1 is that I think the appeal question shouldn't
2 distract from the advantages that having some kind
3 of adversarial participation in the FISA Court
4 itself would bring, even if we can't ultimately
5 solve how we allow them to appeal if and when they
6 lose.

7 Thank you very much.

8 MR. MEDINE: Thank you, Professor
9 Vladeck.

10 Ms. Cook.

11 MS. COLLINS COOK: Thank you all for
12 joining us today. All right, I'm having the same
13 problem that one of our panelists had earlier
14 today.

15 I wanted just to go back to something
16 that the first three panelists discussed and
17 that's the issue of congressional oversight. I
18 think you've seen an evolution over time in terms
19 of congressional oversight. You see it both with
20 respect to the addition of the Judiciary Committee
21 as receiving reports, exercises an oversight
22 function in addition to the intel committees.

1 I think you also see it in a movement
2 away from a traditional, fully-informed standard
3 up to the hill to specific reporting requirements,
4 a whole range of specific reporting requirements.

5 And my question is a general one, which
6 is, do you think that we're in the right place
7 right now in terms of congressional oversight?

8 And I would separate between an ongoing
9 oversight function and the need to legislate or
10 reauthorize in a sunset situation. Or should
11 Congress be taking a fresh look at how it
12 exercises its oversight capabilities?

13 And I guess just going left to right
14 might make sense at this point, my left to right.

15 MS. HARMAN: Your left, so that would
16 be me?

17 MS. COLLINS COOK: Yes.

18 MS. HARMAN: Okay. It took me awhile.
19 I think it's a great question and I think it's
20 something that has to be revisited, but I was
21 there. I was working in the Carter White House
22 when FISA was passed in 1978. I wasn't part of

1 the hardy little band that on a bipartisan basis
2 that crafted the law. But I was impressed by the
3 fact that the basis of FISA is a robust
4 functioning of all three branches of government,
5 Executive Branch policy reviewed by the FISA Court
6 and overseen by the Congress. That was the deal.

7 And that worked very well, my
8 impression until 9/11. And then the event of 9/11
9 but also the fear of ongoing 9/11s caused the Bush
10 Administration to feel that we need a dramatically
11 enhanced response or aggressive, an aggressive
12 approach, not just a response.

13 And they ignored FISA for a couple of
14 years, which I only found out afterwards, although
15 I was a member of the Gang of Eight. And Congress
16 pushed back and amended FISA to catch up to
17 technological change. And FISA and other laws,
18 PATRIOT Act and other things that have been
19 mentioned, certainly Executive Order 12333,
20 although it's not a law, are in place now.

21 So what is my basic answer to you? I
22 think robust oversight is crucial. I think it

1 should extend beyond the intelligence committees,
2 although I think they have a special role because
3 they have a special understanding, or are supposed
4 to, and I hope I did, of what the challenges are.

5 But I think because of the reach of
6 these programs all members of Congress should have
7 some role in oversight. That's number one.

8 I think the challenge is the changes in
9 technology. Others on this panel know a lot more
10 about that than I do. But it is very hard to
11 craft either a law or an oversight regime that can
12 anticipate, you know, what iPad or iPhone 6S is
13 going to look like and what capabilities it might
14 have that iPhone 5S doesn't have. And I don't
15 mean to limit it to one manufacturer.

16 But what else is going to be out there
17 that we can't imagine, or I can't imagine?
18 Remember, I'm the grandma, these kids can probably
19 imagine it.

20 MR. KERR: Just briefly, because this
21 is a great question although, in large, outside of
22 my expertise. But one issue that I think matters

1 a lot is whether, what is the reference point that
2 Congress is looking at the question from?

3 So if there is a sunset provision or if
4 the FISA Court is taking a conservative
5 interpretation of the law, the Executive Branch
6 has to go to Congress and has to get something
7 from Congress. It has to persuade.

8 And when the Executive Branch is in a
9 position of needing to persuade, that is going to
10 lead to better oversight than the opposite. So if
11 the FISA Court is taking an aggressive
12 interpretation of the law, it's relatively
13 difficult I think for the legislative branch to
14 give the kind of oversight that it needs when it's
15 effectively trying to say, okay, what might be
16 going wrong that nonetheless has been approved by
17 the FISA court? It's a difficult position, I
18 think, for the legislative branch to be in.

19 So one of the benefits I think of the
20 sunset provisions and the rule of lenity idea is
21 it effectively means that the Executive Branch has
22 to go to the legislative branch and make the case

1 affirmatively. And I think that's just going to
2 lead to better oversight.

3 MS. PELL: And I'll sort of take the
4 end of what Professor Kerr said and when the
5 Executive Branch has to come to the legislative
6 branch, the legislative branch has to stay
7 engaged.

8 If there are continual reasons to be
9 viewing things because they are sunseting or the
10 Executive needs to ask Congress for something on a
11 regular basis, the staff are going to stay
12 engaged, the members are going to stay engaged.
13 It's going to be a priority. And I think it needs
14 to be a priority. Thank you.

15 MR. MEDINE: Thank you.

16 Ms. Brand.

17 MS. BRAND: Thank you. Just to follow-
18 up on Beth's question about congressional
19 oversight. Those of you who were here for the
20 previous panels heard me ask about the proposals
21 to have a return requirement to the FISC where the
22 government would have to go and tell the FISC what

1 it was doing after the fact. So it's not
2 congressional oversight, it's judicial oversight.

3 And I have a somewhat cynical view that
4 sometimes reporting requirements are a fig leaf
5 and not particularly effective oversight because,
6 you know, they impose massive, massive personnel
7 burdens on the Executive Branch and then it goes
8 into a black hole and no one ever looks at it.

9 So that was the reason for my questions
10 earlier. And I would have the same question I
11 guess about congressional oversight. If, you
12 know, very granular, there is already a lot of
13 congressional reporting under FISA, and if it were
14 increased even beyond what it is now to include
15 some very granular reporting, what would Congress
16 do with that information and does it actually
17 enable a greater level of oversight than already
18 exists?

19 So I guess maybe for Congresswoman
20 Harman and Stephanie.

21 MS. HARMAN: Well, if I weren't an
22 optimist I wouldn't have served in Congress for

1 seventeen years. I think Congress is capable, I
2 think members are capable, not equally capable. I
3 think committees are capable and it's a tragedy
4 that we seem to be basically ignoring the regular
5 order, the committee process in at least this
6 Congress and the prior one.

7 But I think the intelligence committees
8 and other committees of jurisdiction could staff
9 up to do this well, even the granular stuff.
10 There are very smart people that are sitting right
11 here who could be hired with the focus on this,
12 and there are members who really care about
13 getting it right in both parties. And obviously
14 the public is now intensely clued in. And once
15 the Privacy and Civil Liberties Commission becomes
16 a household word, you're going to keep attention
17 focused.

18 So I think this is doable. Yes, it
19 will take a commitment of resources, and not just
20 financial resources but brain cells to do it
21 right.

22 And I think the challenge is going to

1 be that the goalposts keep moving, that it is
2 going to change because the capabilities of both
3 our technology and what the bad buys can do are
4 evolving and keeping on top of that and
5 understanding what that means and then
6 understanding what the requirements are, not just
7 what does the law say, but who should we be
8 focused on and how should we be doing this?

9 And again, it might just, in two years
10 or ten minutes, not just be bad phone numbers and
11 bad email addresses, it could be something in the
12 cloud that I can't even imagine, or something
13 beyond the cloud.

14 MS. BRAND: Okay, thank you.

15 Stephanie.

16 MS. PELL: Obviously you want reporting
17 requirements or information to be useful but
18 without it what can Congress do?

19 I found one of the most challenging
20 aspects of reform of criminal investigative
21 authorities was just getting accurate information
22 about how technology functions, about how often

1 the government was using certain types of
2 authorities.

3 Those kind of metrics for dedicated
4 staff and members, and they are there, is very,
5 very useful, but if it's not there, you know,
6 where is your starting point?

7 MS. BRAND: Do you have a view, any of
8 you, on what type of information is not currently
9 provided that could be provided that would be
10 useful?

11 MR. SPAFFORD: I wanted to add to that
12 that reporting is not sufficient because with the
13 technology and with the complexity I can craft a
14 report that says everything and means nothing to
15 the people who read it because they don't have the
16 background.

17 Unless we allow those with expertise in
18 the area and time in office, and this is largely
19 staff function, the ability to ask questions to be
20 brought out to either the court or to elected
21 representatives, they aren't going to actually be
22 able to understand what's going on with some of

1 the very complex technical issues.

2 And so again, I come back, I have this
3 concern that reports have kept staff from being
4 able to even be briefed or aware of these things
5 or to discuss it with members. And many of the
6 members have backgrounds in law, or education, or
7 other issues, where they don't understand the
8 technology and they really depend on the staff to
9 help them to get to those bits of information.

10 MS. BRAND: Professor Vladeck.

11 MR. VLADECK: I mean, I think there's
12 also an incentives problem, right. So I think,
13 you know, I mean we can all, I think, agree that
14 everyone's working on what they see as the best
15 interests of their constituents.

16 But the problem is that when this is
17 all happening in the dark, you know, I don't know
18 what the incentive is for members to go down in
19 the skiff and spend hours and hours going through
20 materials that they may not even understand.

21 You know, I think last Tuesday's
22 HPSCI's hearing we brought this out quite sharply.

1 I mean, I think when you have the Chairman of the
2 House Intelligence Committee saying it's not a
3 violation of our privacy if we don't find out
4 about it, you know. I mean the question is how do
5 we change that mentality, not just among, you
6 know, the popular discourse, but among the members
7 who are tasked with this oversight function.

8 And then part of that is not just
9 better reporting and better opportunity to
10 actually engage the reporting, but also some
11 mechanism through which it's more in their
12 interest to exercise the oversight, as opposed to
13 just sort of keeping things under the rug.

14 MS. HARMAN: Could I just add one thing
15 because I thought your question wasn't just about
16 reports, I thought it was about oversight.

17 MS. BRAND: Where the reporting enables
18 oversight.

19 MS. HARMAN: All right. But oversight
20 is much more than reports. Oversight is, it can
21 be offensive too. It can be asking questions,
22 requiring people to come up and report, reviewing

1 materials.

2 I mean, back in, you know, in the
3 antediluvian days I'm told that Mike O'Neill, who
4 was the Chief Counsel of HPSCI for years in the
5 80s, read every single FISA application, read
6 every single FISA application. Now that to me is
7 pretty darn good oversight, assuming he knew what
8 he was reading, and he's a very smart guy. He's
9 still around.

10 Yo, I mean that would be impossible
11 now. There's too much going on. But it seems to
12 me that the right people motivated the right way
13 with adequate resources, and part of that is the
14 determination to focus. And I think, don't sell
15 members short. Of course, why wouldn't I defend
16 members? But don't sell them short.

17 Some members are keenly interested in
18 this and can make it a priority to focus on this.
19 And I think we need a staffing pattern that
20 enables those members to do that. But I think
21 there are members who have been and are and will
22 be very conversant with intelligence and know how

1 to do oversight.

2 MR. MEDINE: Professor Spafford,
3 earlier you said that there was a concern that the
4 more information you collect to avoid false
5 negatives, the greater the risk of false
6 positives.

7 One could read that as an implicit
8 critique of the haystack model that the
9 administration has advanced for Section 215. If
10 that's the case do you have an alternative for
11 accomplishing the same goals without the haystack?

12 One option that was discussed earlier
13 today is to access information at the provider
14 level, using I guess a federated search model or
15 something similar to that.

16 What are your thoughts on potentially,
17 I guess, technological solutions that avoid the
18 problem that you seem to be concerned about?

19 MR. SPAFFORD: It's difficult to give
20 specific examples without delving into specific
21 systems.

22 I will say that in general from what I

1 have seen in the open press, the theory is collect
2 all of the information in case it's useful and
3 then mine all of that.

4 And the problem there is it's possible
5 to collect huge amounts of information that have
6 no bearing or lead to false results. In fact, it
7 can obscure the results because it introduces
8 noise.

9 An example of this is the analysis that
10 uses the three hop collection for contacts. What
11 I have seen, and I do not have personal experience
12 with this, but what I have seen mentioned is that
13 a two hop analysis is much more accurate. A three
14 hop analysis begins to pull in people at car
15 rental agencies and hardware stores and pizza
16 places and actually introduces more noise.

17 It would reduce the amount of
18 searching, the amount of data necessary and some
19 of the concerns to have a more tailored approach.

20 But fundamentally at its heart it's a
21 question of, where are our values here? Is this
22 such an existential approach that we have to

1 collect every bit of information that goes across
2 every communication line in hopes of catching
3 every last person who has harbored an inimical
4 thought?

5 Somewhere there needs to be a little
6 bit more balance where we're willing to use
7 traditional police and intelligence methods for
8 safeguarding ourselves and not try to head
9 everything off in regards for helping with
10 privacy.

11 MR. MEDINE: Thank you. Professor
12 Vladeck, earlier you talked about one potential
13 model to get appellate review and the Foreign
14 Intelligence Surveillance Court of the bankruptcy
15 approach, which is that the lower decision is not
16 really final until reviewed.

17 How would you square that with the
18 exigencies of surveillance needs where having a
19 non-final order if it doesn't permit the
20 government to engage in surveillance could
21 actually delay critical surveillance activities
22 while the review process goes forward?

1 MR. VLADECK: Sure. I mean I think it
2 actually wouldn't be that difficult. I mean you
3 could analogize it to a preliminary injunction but
4 just sort of reverse it, right.

5 So the idea would be that an interim
6 order by the FISA judge would be sufficient to
7 allow the government to act on an interim basis
8 pending review and finalization by the FISCR.

9 And then, you know, I think the idea
10 would be that would sort of solve both problems.
11 It would allow the government to act once they
12 make the initial prima fascia showing to the FISA
13 judge, and then it would allow for subsequent
14 retrospective review by FISCR without running into
15 the problem.

16 And that, you know in the bankruptcy
17 context, I mean the bankruptcy court has the power
18 to issue interim orders pending confirmation of
19 their report. And so I think you could just
20 borrow that analogy and work it all the way out.

21 MR. MEDINE: And when would you have
22 this apply? I mean we've heard that there are,

1 the vast majority of what the FISC does is routine
2 requests that don't raise novel legal or
3 technological issues.

4 Would you have these bankruptcy model
5 approach in every single request to the FISC, and
6 if not, how would you determine which requests it
7 applied to?

8 MR. VLADECK: Well, see the whole point
9 of the bankruptcy model is to actually divide
10 classes of cases, right, and so the bankruptcy
11 model divides what are called core proceedings
12 from non-core proceedings.

13 And in core proceedings, which might be
14 analogous to the sort of non-interesting FISC
15 cases, the bankruptcy court does have the power to
16 act finally and without any appellate oversight.

17 And then it's only in the non-core
18 proceedings in the bankruptcy context that you
19 have that review.

20 So it seems to me you could have some
21 trigger, so some of the proposals include any
22 decision turning on a significant question of law

1 or a significant departure from prior.

2 I mean there are ways to sort of make
3 that threshold work, and it could be whether it's
4 a novel interpretation. It could be whether it's
5 application of an existing precedent to a new set
6 of facts.

7 I mean, you know, I think the devil's
8 in the details but I think you could find a way to
9 agree on a sort of a trigger that would sort of
10 sort cases into one of those two categories.

11 MR. MEDINE: And I guess because if you
12 get to the FISC review on that basis, which I
13 understand, how do you get to the Supreme Court?
14 I mean the Supreme Court does seem to raise a case
15 in controversy question of going from the FISC
16 review up to the Supreme Court because you don't
17 have that lack of finality that you would have had
18 from the lower court.

19 MR. VLADECK: Yeah, I mean I think the
20 Supreme Court issue is still a problem. You could
21 presumably solve it the same -- not the same way
22 but sort of an analogous way. I mean so it's

1 already the law under 28 U.S.C. 1254(2) that all
2 of the circuit courts can certify questions to the
3 Supreme Court at any time. It would be, you know,
4 a four word amendment to 1254(2), right, in
5 parentheses, including the FISA Court of Review.
6 All right, that was more than four words. Right.

7 And then you know, presumably that
8 wouldn't provide for mandatory review. It
9 wouldn't provide for automatic review, but it
10 would also allow FISCR, if there were cases where
11 FISCR thought it was a sufficiently important
12 question to raise it to the justices' attention,
13 FISCR could then send it to the Supreme Court.
14 And the Supreme Court say we don't care. I mean
15 that's, you know, the Supreme Court hasn't
16 answered a certified question since 1981, you
17 know. I mean I think it's their prerogative to
18 ignore FISCR, but at least FISCR would have the
19 ability to try to get their attention.

20 MR. MEDINE: Thank you.

21 Judge Wald.

22 MS. WALD: Okay. There's been a lively

1 debate on some of the outside commentator on 215
2 as to whether or not it is sufficient to have,
3 let's say, the representative democracy model for
4 big, bulk programs like 215.

5 You know that is, we have elected our
6 members of Congress, if they set up a system for
7 review, be it the Gang of Eight, Jane, or be it
8 something broader, then that's it and, you know,
9 the people just have to live with that.

10 Of course, one problem with that always
11 is that even if you adopt this, theoretically the
12 peoples' resort is not to elect the same people if
13 they don't like the same people, but if they don't
14 know about the program that's in there, that
15 particular exit strategy is not worth that much.

16 But the deeper thing is, is that the
17 right model or is the model which some people have
18 written about that when you get to a program, not
19 the individual warrants, but when you get to a
20 program that really encompasses a large portion,
21 you know, of people and inevitably a large portion
22 of innocent, people who won't have any terrorist

1 implications afterwards, is it not necessary, even
2 at the cost of a little risk to the possible tight
3 security, for that to be disclosed, not in its
4 operational details, but in the fact that, yes, we
5 do have the bulk program that goes to X, Y, Z?

6 I'm wondering about your thoughts,
7 Jane, Representative Harman. We've known each
8 other a long time. And Stephanie, and anybody
9 else that wants to.

10 MS. HARMAN: Well, first of all, Pat,
11 Judge Wald, let me salute your decades of service
12 to our country. You are certainly for women
13 lawyers, the gold standard.

14 I was teaching a course at Harvard Law
15 School about a week ago and a young woman, we were
16 talking about this, she said, well, why should we
17 trust NSA or any government agency to put the
18 technical side of this together? Why should we,
19 and then why do you trust them?

20 And I said, well, I start with this,
21 there are bad guys out there trying to attack us,
22 let's just talk about the terrorist piece of this,

1 and I want to know who they are and disrupt them
2 before they do that. My assumption is most of
3 them are in some foreign place and are not U.S.
4 persons, but at any rate some of them could be.

5 So Congress tried to design a system,
6 and I think did so pretty well, building in
7 safeguards and court review and congressional
8 oversight.

9 Now the system got a lot bigger since
10 9/11. Is it the right size? I don't know. I
11 don't know if it's the right size. But I know I'm
12 not the person, or if I were a member of Congress
13 now, or even as, you know, the lowly, beat up
14 President and CEO of the Wilson Center, just
15 kidding, I'm not the right person to decide what
16 the size is. I'm much better at designing the
17 safeguards so that whatever size it is, there
18 aren't abuses.

19 And I'm pretty persuaded we've got to
20 have haystack. Again, I don't know what should be
21 in it. If the question is should everything be in
22 it? No, everything shouldn't be in it. The right

1 things should be in it. What are the right
2 things? Somebody, again, with more technology
3 knowledge should decide that, subject to review by
4 the court, the FISA Court and maybe the Supreme
5 Court ultimately, depending on how we structure
6 this. And I am for Supreme Court review so there
7 has to be standing and that has to be provided for
8 somehow.

9 And the congress. Congress after all
10 writes the laws. So I mean maybe that's an
11 oversimplified version of it.

12 But back to that Harvard Law School
13 student, I trust our government, subject to
14 safeguards, to do the right thing to keep our
15 country safe.

16 MS. WALD: Let me just clarify or just
17 follow-up, okay. And that is, for instance in 215
18 one of the criticisms, even by some isolated
19 members of Congress is we didn't even know that
20 215 was meant to encompass a bulk selection.

21 And so the question -- but then one
22 answer is, ah, but some people in Congress did. I

1 don't know whether, you know, an inner group was
2 told that this was a contemplated use. And so
3 they knew it, etcetera, but maybe not until the
4 thing was passed and you began to get --

5 I know later on re-authorization, memos
6 were sent up from the Department of Justice
7 explaining it, but apparently not everybody read
8 them even though they could have read them,
9 etcetera.

10 So I guess, yeah, I'm getting to this
11 question. I only raised it because it is a
12 philosophical question. I think of whether or not
13 there are what some people call secret law that
14 when it's being passed --

15 MS. HARMAN: Oh, what? I think I
16 missed that.

17 MS. WALD: When it's being passed
18 everybody doesn't debate in the public debate
19 about what's really involved. And I understand
20 the security risks. They can't obviously debate
21 about a lot of security.

22 But the question of whether or not

1 there's some level at which they should know that
2 something that you don't read the ordinary meaning
3 into could encompass a very novel and extensive
4 program to be in the debate.

5 MS. HARMAN: Well, I don't want to
6 dominate this, and again, there are very competent
7 people here.

8 But what did I know and when did I know
9 it? As we were debating the PATRIOT Act a lot of
10 it was controversial, and what the White House
11 requested, the Bush White House requested, was cut
12 back by Congress and several sections were
13 sunseted, as you've just discussed. Whether
14 sunset is the best mechanism, I don't know but it
15 requires congressional review.

16 And 215 was one of those. And there
17 were also controversies about the so-called
18 library provision about whether grandma taking out
19 a library book was subject to some kind of
20 scrutiny.

21 But at any rate, this stuff was
22 debated. It was re-debated. I don't know how

1 many members paid attention. I didn't view this
2 as secret law. What precisely was the process to
3 get the information I think was discoverable by
4 members of Congress. I don't think it was hidden.
5 And I think somebody not on the Intelligence or
6 Judiciary Committee who really wanted to figure
7 out how 215 works could have found out.

8 And again, in defense of Congress, a
9 lot of stuff going on, people get distracted and
10 this wasn't the public issue that it has become in
11 recent time.

12 And that again is why there needs to be
13 a robust Privacy and Civil Liberties Commission.
14 This is the kind of issue this commission, had it
15 been fully functioning in -- well, you weren't
16 there when PATRIOT passed, but when PATRIOT was
17 re-authorized, or the controversial provisions
18 where you were there, you could have, if you had
19 been there, focused attention, held hearings, done
20 more to educate Congress and the public about what
21 was at stake and influenced how the changes were
22 made.

1 MR. MEDINE: Mr. Dempsey.

2 MS. WALD: Ms. Pell, I just wondered if
3 she had anything to add to this quickly.

4 MS. PELL: So I'll try and narrow down
5 a little bit to your specific question about an
6 interpretation of a statute like 215 that
7 authorizes a type of bulk collection that would
8 not be readily apparent, even to a surveillance
9 expert who read the statute.

10 Sort of putting on my former national
11 security prosecutor hat, so much of intelligence
12 oversight does, and it probably does have to
13 happen behind closed doors.

14 That being said, I think we really need
15 to push ourselves and the Executive Branch needs
16 to be pushed, which we saw you doing this morning,
17 to figure out how it is possible not to hide
18 interpretations of a law that are perhaps
19 idiosyncratic or novel.

20 And when I was thinking about this
21 issue in preparing to testify today what bothered
22 me in terms of dialogue and exchange between staff

1 members and their constituencies back in the 2009
2 timeframe was the inability to explain to those
3 constituencies, nongovernmental stakeholders why,
4 what would happen to language if it was amended in
5 a certain way so that there wasn't really
6 meaningful dialogue going on and you have the
7 potential for constituencies who are very
8 interested in these issues, lobbying or supporting
9 language that wasn't necessarily in their
10 interest.

11 And I think that's a bit of a broken
12 process but a hard problem to cure because the
13 Executive Branch is going to say there's going to
14 be harm to national security if this legal
15 interpretation tells people that we're collecting
16 bulk, collecting metadata. And there's the rub,
17 but I think we need to push.

18 MR. MEDINE: Okay. Mr. Dempsey.

19 MR. DEMPSEY: Thanks very much to all
20 of the witnesses for coming today and trying to
21 work these issues through with us.

22 Professor Kerr, do you have any

1 thoughts on this question of review or call it
2 appeal?

3 You've written extensively on appeals
4 in the criminal context of court orders for
5 surveillance. In the FISA context here where
6 there's some interest in creating some process for
7 getting from the judge to the FISA Court of Review
8 and at least making issues available to the
9 Supreme Court, should they take them or not, what
10 are your thoughts in terms of what would be the
11 best way to structure that, or could that be
12 structured that's at least as constitutional as
13 the rest of FISA?

14 MR. KERR: It's a good question and a
15 difficult one, in part because the constitutional
16 questions hinge in large part on an understanding
17 of the search warrant application process and the
18 ex parte application process, which is almost
19 entirely unexplored in the case law.

20 How should we think about an
21 application for an ex parte court order? Is that
22 like a case in which case it's an exercise of the

1 judicial power and we need to think of it in the
2 traditional Article III ripeness, case in
3 controversy way, or is that just some sort of an
4 extra issue that goes before a judge that does not
5 require the traditional Article III strictures to
6 be followed.

7 We don't really know. So just thinking
8 from a constitutional standpoint it's really
9 difficult to know what the constitutional
10 parameters are here in terms of what is
11 permissible. There's just a tremendous gray area
12 and I don't think there's going to be a lot of
13 certainty one way or another.

14 I tend to be somewhat skeptical that
15 the Supreme Court specifically could serve a
16 useful role here, in part because everything the
17 Supreme Court's doing is on the record, all in
18 open court. It's difficult for a court of nine
19 justices to have an oral argument where they're
20 sort of, you know, bandying about hypotheticals on
21 an area where there's a lot of classified issues.
22 I just don't know how procedurally that might

1 work.

2 And in part my idea of the rule of
3 lenity playing a significant role here as a way of
4 avoiding this problem entirely. I think if you
5 have the initial court decision --

6 MR. DEMPSEY: Although wouldn't your
7 rule of lenity, that allow the government, the
8 government would have the right to appeal still so
9 actually you end up with a situation in which you
10 in a way are perpetuating the current system where
11 if your rule is applied, it's not like you
12 immediately go back to Congress, you go to the
13 FISCR and then you go to the Supreme Court.

14 MR. KERR: Well, I suppose you could
15 have the process end at the FISCR rather than go
16 to the Supreme Court. So you could have more
17 equality there, where it's not that one side sort
18 of can do more than the other side.

19 So, yes, I think you have the same
20 problems with the Supreme Court trying to step in.
21 And, of course, one reason we've never had this
22 issue is the FISCR has only handled a few cases,

1 so the Supreme Court has never been in a position
2 to review that.

3 But I'm more optimistic about the idea
4 of having public disclosure of the FISC or FISCR
5 interpretations of the law combined with some sort
6 of sunset provision that forces this to be hashed
7 out in Congress than I am having nine justices of
8 the Supreme Court try to answer these questions,
9 so.

10 MR. DEMPSEY: Professor Vladeck.

11 MR. VLADECK: I was going to say, I
12 mean I think it's very important to not
13 generalize. I mean I think, you know, I would
14 draw a very sharp distinction between original
15 FISA, in which I think there is the strongest
16 analogy to the warrant context, and 215 and 702,
17 which look nothing like warrants of any
18 conventional understanding.

19 And in the context of 215 and 702, I
20 think it is telling that Congress actually
21 expressly provided for adverseness, right, that in
22 both statutes the recipient of a 215 order, the

1 recipient of a 702 directive is given the, you
2 know, express right to participate adversarial
3 before the FISA Court, to appeal adverse
4 decisions, including to the Supreme Court.

5 So, you know, I think the adverseness
6 in the 215 and 702 context is actually, you know,
7 satisfied until you get to the appeal question,
8 which I was talking about before.

9 And in the warrant context, I guess I
10 just, I'm less circumspect I think than Professor
11 Kerr, only because I have a hard time seeing how
12 the issuance of a search warrant is what the
13 Supreme Court called an extrajudicial duty. It
14 strikes me as a quintessentially judicial duty. I
15 mean if the warrant clause of the Fourth Amendment
16 requires a neutral magistrate and not just a
17 neutral government officer of some vague
18 description to sign off on a warrant, it seems to
19 me that a warrant is part of the judicial process
20 and that the adverseness is sort of justified,
21 whether you buy it or not, by the fact that
22 there's a subsequent proceeding in many cases that

1 will allow for --

2 MR. DEMPSEY: But could you even go so
3 far as to say, I mean I'm not a constitutional law
4 scholar, which will become apparent in a second.
5 Is it possible to say that because of the Fourth
6 Amendment that actually the case and controversy
7 concepts are quite different in the warrant
8 context?

9 Because we've said even though there's
10 no party judges do this. This is appropriate for
11 judges, even in the absence of a traditional case
12 or controversy. And it's right there explicitly
13 in the Constitution. No one's ever, FISCR, no
14 one's ever really asked how do we get warrants
15 before judges in the first place? Is maybe that's
16 the answer, that it's right there in the Fourth
17 Amendment?

18 MR. KERR: I don't think so. In part
19 because the case law of the Supreme Court, at
20 least in talking about the neutral magistrate
21 requirement, has suggested that it doesn't, the
22 neutral magistrate doesn't need to be a judge,

1 doesn't need to be a lawyer. It could actually be
2 somebody who's a court clerk, could in theory,
3 there's been some suggestion in the cases, be
4 somebody inside the Executive Branch who could
5 count as a judge for Fourth Amendment purposes
6 issuing search warrants.

7 And this goes back to the difficulty of
8 just trying to figure out how to categorize search
9 warrant applications. Is it a traditional case?
10 Is it something that's just another duty? The
11 fact that you could have a non-judge issue a
12 search warrant, to me takes it somewhat, at least
13 from a constitutional standpoint, outside of the
14 traditional sort of tripartite system and suggests
15 it may not be a judicial function. But it's
16 really a gray area.

17 MR. VLADECK: And it's usually
18 appealable. I mean, I think, right, I mean at
19 least in the federal context, right, if the
20 government's, you know, there are extraordinary
21 contexts where you can pursue, right, where you
22 can seek to challenge the denial of a warrant

1 application.

2 MR. KERR: Actually traditionally the
3 understanding has been no, that denials of
4 applications are not appealable.

5 Now there's been some disagreement in
6 the Title III setting. They've said that you can
7 appeal it. That's another murky area, so it's
8 just, again, just a gray zone.

9 MR. DEMPSEY: We've zoomed off into
10 speculation.

11 MR. MEDINE: Ms. Cook.

12 MS. COLLINS COOK: I'd like to turn to
13 a slightly different topic. Our statute requires
14 us to consider the need for specific actions taken
15 by the U.S. government to protect against
16 terrorism and balance that need as against privacy
17 and civil liberties concerns.

18 And one thing I think is very difficult
19 to articulate is what makes a program effective.
20 It can't simply be that a program is effective if
21 it has thwarted five plots, if it's thwarted ten
22 plots. And I would throw open to the panelists

1 what other types of metrics or concepts we should
2 be looking to and to determining whether specific
3 actions or programs are effective.

4 MS. HARMAN: Well, I don't think
5 thwarting plots is the only metric. I don't know
6 how you measure deterring plots.

7 But having that program, the right
8 sized program, whatever that means, in effect and
9 a lot of oversight of that program. Oversight
10 also adds value. In addition to curbing abuses,
11 it could help enhance the program in some way. It
12 could point out some deficiencies and lead to
13 amendments imagining the oversight is from
14 Congress. So I think the metrics have to be more
15 complex than this.

16 But I superimpose over this something
17 I've said a couple of times. One is the changing
18 technology, which is very hard for any of the,
19 Congress, or the courts, or the Executive Branch
20 to keep on top of, but which is something the bad
21 guys plotting against us are keeping on top of.
22 So it's an imperative to factor in changing

1 technology.

2 And the other part of it is, and again
3 this is not directly to your question but it
4 relates to your question, the need to be sure that
5 the public supports what we're doing. And that
6 again is the role you have.

7 I do not think that privacy and
8 liberty, that privacy and security are a zero sum
9 game. I think you either get more of both or less
10 of both. I've said this repeatedly. You probably
11 know that. And that's your job is to make sure
12 that we get both.

13 And I think unless it's perceived that
14 we're getting both there's going to be constant
15 anger and second-guessing and drastic remedies
16 proposed, which at some point might take hold and
17 then we lose both.

18 MS. PELL: I'm not an intelligence
19 analyst so I do hesitate to answer this question.
20 But this morning I believe Raj De, the General
21 Counsel from NSA, made a very interesting
22 statement which I doubt the government will want

1 to elaborate on publicly, but that was that the
2 Internet metadata bulk collection program was
3 ended.

4 And I thought, well, and that had been
5 public. But he seemed to indicate that it was
6 ended because it wasn't seen as effective or
7 providing a level of intelligence that the
8 telephony metadata program was.

9 And so I was very curious, and again, I
10 don't expect the government to talk about this in
11 public, but what was that metric? Are they
12 getting bigger pictures of terrorist groups or
13 cells or activities because of what this telephony
14 metadata program is doing versus what the Internet
15 program was doing? Probably something you could
16 inquire about behind closed doors.

17 MS. HARMAN: Could I just -- I don't
18 think that's -- I thought the change in collection
19 had to do with the FISA Court saying that the
20 incidental collection that was going on was
21 outside the scope of the law and that's why it was
22 cut back and, in fact, what had been collected was

1 destroyed.

2 And I think it is very important that
3 the law be as precise as possible. And I thought
4 this was a great victory for the worried public
5 about how oversight works. So I obviously didn't
6 hear his testimony but I think that's what I
7 imagine he was talking about.

8 MR. SPAFFORD: There are things that
9 can be measured such as the cost of all of the
10 storage necessary to hold this five year haystack
11 that's being built-up, the cost of all the
12 equipment, the personnel to do the collection, to
13 do the maintenance, to do the searching.

14 There can be other kinds of costs that
15 are calculated for protecting all of that. For
16 instance, the NSA has spent a lot of money to
17 build a very large data center in Utah. How much
18 of that is for this purpose, they can perhaps
19 answer in a classified setting. That's one thing
20 that can be measured.

21 You can measure the number of
22 successes. You can measure the number of

1 failures. And hopefully they can produce some
2 measure of the number of false incidents that they
3 have investigated and spent time and effort on,
4 how much has gone into that.

5 From that, you can draw some
6 calculation as to the cost per success and the
7 cost per failure. Thereafter is a policy decision
8 as to are we spending enough, are we spending too
9 much for one of these incidents?

10 And that requires getting a full
11 accounting of what things have been prevented.
12 Apparently this collection is largely being or
13 totally being directed towards anti-terror
14 activities and the accounting that we've seen of
15 the number of thwarted terrorist activities in the
16 U.S. seems to be small relative to the investment
17 involved. But that's a decision, you have to get
18 the values and that's a policy decision that's
19 well, certainly beyond my pay grade.

20 MR. VLADECK: I'd also just add very
21 briefly, I mean you know, in the due process
22 context the Supreme Court has said efficacy is not

1 just a function of the government's success rate,
2 right. Efficacy is also a function of the cost to
3 the government of providing additional process.

4 And I think it's impossible to divorce
5 efficacy of particular surveillance programs from
6 any attempt to actually figure out what the actual
7 downside would be of adding additional safeguards,
8 of adding additional protection. You know,
9 because I think that's part -- I mean efficacy is
10 not just sort of accuracy, it's also sort of a
11 lack of false positives on the individual right
12 side as well.

13 MR. MEDINE: Ms. Brand.

14 MS. BRAND: Thank you. I have a policy
15 question that may have, may or may not have
16 constitutional implications for Professors Kerr
17 and Vladeck and anybody else who wants to weigh
18 in.

19 With respect to the advocate, or
20 amicus, or whatever you want to call it, in the
21 FISC there is an appeal to that. There's
22 something I like about it. But I think it's much,

1 much more complicated in its implementation than
2 most of the bills or proposals recognized.

3 And as I've been thinking through the
4 many, many levels of detail about how the thing
5 would be implemented, to my mind a lot of sort of
6 sub-questions turn on whether the advocate is
7 someone with procedural rights in the process or
8 someone who is called upon to give their view of a
9 question of law for the court's benefit.

10 So Orin, do you have a view about
11 whether the advocate, or Professor Vladeck about
12 whether the advocate is somebody who should, as it
13 would be in a true adversarial process, have a
14 right to participate in every single aspect of the
15 proceedings, to see every single piece of paper
16 presented to the court?

17 You know, there was some discussion
18 about the back and forth that goes on between the
19 FISC's lawyers and the government. Should the
20 advocate be privy to all of that communication
21 like they would in a regular litigation context,
22 or what?

1 And do you think whether the person has
2 procedural rights or not dictates whether or not
3 there's an Article III question here?

4 MR. KERR: So on the policy question
5 it's not obvious to me that the details of
6 procedural rights would make a major difference.
7 And in part that depends on what the role is of
8 this special advocate, when they're brought into
9 the case.

10 I assume we're thinking of, you know,
11 once in a while there would be a particularly
12 significant issue on which we would want the
13 special counsel or however you --

14 MS. BRAND: Let's just posit that it's
15 the person is only involved in novel or
16 significant cases.

17 MR. KERR: Right. As long as, I think
18 it's important that they be given the full factual
19 picture, so they would be given access to all of
20 the underlying facts.

21 And in Marc Zwillinger's earlier
22 testimony he talked about those challenges. But

1 once that, once all the facts are out there, at
2 least for that counsel, it's not obvious to me
3 that there is that much of a need for the
4 procedural rights, as long as the issues are fully
5 litigates.

6 That may just be a question though that
7 Marc Zwillinger would be in a better position than
8 I would to answer, but. And it's also not clear
9 to me that giving procedural rights would make a
10 difference from the Article III standpoint in
11 creating adversariality.

12 MS. BRAND: Well say, for example, that
13 the government did not give access to the special
14 advocate on some piece of information, does that
15 person have a right to it?

16 Does the person have a right to object
17 if the court goes and talks to the government
18 without including the person?

19 I mean those are the kind of rights
20 that a party in litigation would have. But, you
21 know, would all of those same rights apply here or
22 would the person really just be called upon to

1 provide their expertise but not to necessarily
2 participate in a truly adversarial way? That's
3 sort of one of the basic questions.

4 MR. KERR: Yeah, I mean, I suppose
5 there's questions of once you have the right to
6 access the information do you have litigation over
7 whether that right was fully complied with. Sort
8 of thinking in the criminal setting, you know,
9 like a Brady violation or something like that
10 where the litigation over the major issue leads to
11 litigation over all of the sub-issues.

12 And that I would think is just a
13 practical question of how likely is that to be
14 something that interferes with the core function
15 of the special counsel.

16 So I don't have a strong sense of what
17 the right answer is, just given how -- I think
18 really it boils down to would the judges of the
19 FISA Court take this as a priority and make sure
20 that the special counsel is receiving the
21 information, or is it something where that would
22 not be a priority.

1 And I would imagine establishing in a
2 statute that this is an important priority, that
3 this is something that the counsel is entitled to
4 might make sure that the FISA Court judges do that
5 without a need to require litigations on all these
6 sub-issues, but that's just, I think, a practical
7 issue that may just depend on how it works.

8 MR. VLADECK: And I would just add
9 briefly, I mean, I think the closest Supreme Court
10 case I can think of on point is FEC vs Akins,
11 right. In Akins you have the court saying that
12 informational injury in that case suffered by
13 voters, right, was sufficient to confer standing
14 because they couldn't undertake their
15 responsibility as voters without the information,
16 right.

17 So it seems like a sort of similar kind
18 of procedural injury without sort of a direct
19 personal stake. I mean, I'm not the first to
20 suggest the Supreme Court's stand on jurisprudence
21 isn't exactly a straight line.

22 But I do think, I mean, I do think

1 there are procedural issues to work out, and much
2 of them I think would depend on whether, whatever
3 you call this position, is in fact invested with
4 specific representational obligations viz-a-viz
5 those whose communications are intercepted, in
6 which case I think all of these issues become much
7 more joined, right.

8 I think there would be no question in
9 that case that they would have procedural rights,
10 that they would be able to appeal, for example,
11 denial by the FISA Court. Or if you don't, if
12 they have abstract interests in the proceedings, I
13 think that would get harder.

14 But I share Orin's view that I think
15 most of the work would be done just by having them
16 in the room. And then Congress could presumably
17 create the disclosure obligations, not to the
18 opposing counsel, but to the court. And then it
19 would be the court's responsibility and the
20 court's ability to hold the government to account
21 if they failed to comply with those disclosure
22 obligations.

1 MS. BRAND: Thank you.

2 MR. MEDINE: I wanted to return to
3 Congresswoman Harman and Ms. Pell on the question
4 of going forward.

5 The challenge that Congress has in
6 enacting legislation that authorizes secret
7 activities, I mean, it seems almost like a
8 contradiction. How do we write laws that
9 authorize programs that we don't want to talk
10 about in public?

11 And assuming it's an entirely
12 legitimate function and it's a democratic function
13 and assuming the government will fully comply, but
14 how do we write an authorization for a program
15 that we can't talk about?

16 MS. HARMAN: Well, we can talk about
17 part of the program. We can talk about the
18 purpose of the program. We can talk about the
19 framework for the program.

20 Certainly I recall very specifically in
21 the debate on the FISA Amendments in 2008 that's
22 what we did. Maybe a number of members of

1 Congress weren't paying much attention, but it was
2 out there on the airwaves what the issues were.
3 Certainly the telephone metadata program had been
4 disclosed by the New York Times and then partially
5 declassified by President Bush in late 2005, and
6 there was conversation out there.

7 So Congress can do that. That it, that
8 should happen. There should be public hearings,
9 as there now are public hearings about competing
10 versions of some potential fixes for the laws that
11 we have.

12 Yes, a portion of this is classified.
13 Exactly how it works is classified. Why do we
14 want to tip our playbook to the bad guys? And I
15 think that can be explained publicly too. I think
16 if you poll people, and probably we have but I
17 just can't remember what the polls showed, I think
18 Americans want two conflicting things, but they're
19 really not conflicting.

20 One, they want their privacy protected.
21 Well, good luck with that. I mean the private
22 sector knows more about Americans' privacy than

1 the public sector does.

2 But they also want to be secure and
3 they want laws that will catch these bad guys and
4 prevent or disrupt plans to hurt us.

5 So I think that debate about purposes
6 and framework is properly in the public domain.
7 It should be made clear in the public domain that
8 some of the innards, you know, how the watch works
9 will be kept classified because we don't want to
10 tip our hand.

11 But again, if there's adequate
12 safeguards and if there's transparency in
13 disclosing, as has been proposed, how many
14 searches have been made, how many Americans were
15 involved, what were the outcomes in sort of a bulk
16 way, not compromising individual privacy, I think
17 people will be comforted or should be comforted.

18 And just one last point, if we don't do
19 this, if we blow up the bulk collection program
20 totally and we say we're going back to the law
21 enforcement model and only after something happens
22 are we going to go after folks, as soon as

1 something really bad happens, and oh, by the way
2 it could happen even with this program, the
3 pendulum is going to go the other way and we're
4 going to start collecting and at our disadvantage
5 at that point, all kinds of stuff, possibly
6 without the safeguards that we could build in
7 properly now.

8 MR. MEDINE: Ms. Pell, do you have any
9 additional thoughts?

10 MS. PELL: One additional thought, and
11 I'll borrow from criminal investigative
12 authorities. In the ECPA context it took a long
13 time I think to be able to have a good
14 conversation about how to amend statutes to deal
15 with location data.

16 And part of that challenge was there
17 weren't a lot of opinions by courts at various
18 levels discussing how the government sought, under
19 what authorities the ability to collect location
20 data.

21 Over time more of those opinions, most
22 of them at the magistrate level, but nevertheless

1 with anylisis, came out. If in fact we're able to
2 get to a place where, for example, there are FISA
3 Court opinions that are declassified or
4 summarized, we have the basis of a conversation,
5 facts and legal analysis to have a dialogue that
6 members can talk about without worry of disclosing
7 classified information, where interested
8 constituencies or stakeholders can bring concerns
9 based on what they see in those opinions. It will
10 take a little while but that's one way forward.

11 MR. MEDINE: Thank you.

12 Professor Vladeck, earlier you
13 mentioned 702 and providers' ability to come in to
14 court. One can read the statute to say the
15 providers can only challenge the program but not
16 the specific tasking orders.

17 Is that your view, and if so do you
18 view that as a shortcoming of the statute?

19 MR. VLADECK: To be frank, I think
20 because it's never been litigated, you know, I
21 think it can be argued both ways. And I would
22 have hoped that a provider would have tried to

1 litigate it in the other direction.

2 You know, we learned from the letter
3 from Judge Walton to Chairman Leahy that in fact
4 no recipient of a 702 Directive has ever
5 challenged it.

6 You know, I do think any opportunity
7 for more presentation of adversarial argument and
8 briefing in the FISA Court, at least after the
9 government has been able to obtain the authority
10 ab initio is worth pursuing.

11 And I actually think we didn't hear
12 anything to the contrary from the government
13 witnesses this morning. You know, whether you
14 would need that on top of a provision for some
15 kind of special advocate, I think, is an
16 interesting question because you'd have maybe
17 potentially a redundancy problem. But in the
18 absence of that, certainly, I think, you know, it
19 would be a relatively easy sell to Congress to do
20 that.

21 I think the harder sell is getting the
22 recipients to actually use it. And I think that's

1 a question worth pursuing as well.

2 MR. MEDINE: All right, thanks.

3 We have eight or ten more minutes if
4 people have a couple of more questions.

5 MS. WALD: Yeah.

6 MR. MEDINE: It looks like Judge Wald
7 is ready and eager.

8 MS. WALD: Okay. My first question is
9 for Professor Kerr. I wonder if you think, given
10 the present status of 215 was originally not known
11 to us. It was in operation for many years before
12 it became publicized. Now there's a great deal,
13 we know it's there and there's a lot of people
14 going back and forth. There are several proposed
15 reforms, in quotes, on the hill.

16 And the question is still there, at
17 least one of the bills says stop the program, you
18 know, the Leahy bill, move to a different way of
19 doing it.

20 I'm wondering if you think your two
21 precepts that you laid out earlier, namely sunset
22 and a rule of lenity have any application, if so,

1 what to the present status and debate over what to
2 do with 215 right now?

3 MR. KERR: Well, there is no rule of
4 lenity right now so --

5 MS. WALD: No, I know that, but I mean
6 there should be or there's some principle there
7 that could be applied to what do we do with 215
8 right now, that we know about it.

9 MR. KERR: Yeah, and certainly my
10 understanding is that Section 215 sunsets in 2015,
11 I think. So that provision will be, you know,
12 that will have to lead to a debate at some point
13 over the next two years over whether this program
14 is desirable or not. And the government's going
15 to have to make its case.

16 You know, we could wish that it was
17 something that happened in the next few months
18 rather than two years from now, because the
19 debate, of course, is current now and who knows
20 what the picture will be then.

21 But so the sunset provision, I think,
22 does play a very important role over the next two

1 years in figuring out, ultimately Congress
2 answering this question of whether to approve the
3 bulk collection program or not, and if not, what
4 are the alternatives.

5 MS. WALD: Well, your original
6 explanation of the rule of lenity was that if the
7 FISC Court got something that appeared to be a
8 novel interpretation or that appeared to be at the
9 extreme edges of an interpretation they should
10 tell the government to go to Congress and get a
11 specific authorization. Does that have any
12 application to the present situation?

13 MR. KERR: Yeah, well, if there had
14 been a rule of lenity in place that the court had
15 considered at the time I would think that the
16 answer would be that they would not have approved
17 the bulk collection program under Section 215.

18 I think they should not have approved
19 it, at least based on the arguments that have been
20 made so far, even without a rule of lenity, just
21 considering it as a fifty-fifty question.

22 So we would not have been in the

1 situation that we're in with the FISA Court having
2 already approved the program, sort of putting the
3 difficult burden on those that are trying to amend
4 the statute in the other direction, if there had
5 been some sort of a rule of lenity in place.

6 MS. WALD: But as it comes up for
7 re-authorization, which it does apart from the
8 sunset every, I forgot what the period is, but do
9 you think that's the point at which the rule of
10 lenity might apply?

11 MR. KERR: So I'm thinking of, just to
12 be clear, the rule of lenity being Congress
13 instructing the FISA Court to interpret the
14 Foreign Intelligence Surveillance Act in that way,
15 sort of by default adopting a narrow
16 interpretation of the statute rather than a broad
17 interpretation.

18 MS. WALD: Yeah, but I thought you had
19 suggested that when it came to FISC in the
20 beginning, and I'm just saying would that have any
21 application when you're having re-authorizations
22 they would say this is sort of an extreme and

1 novel interpretation, go back, go to Congress and
2 get a specific authorization.

3 MR. KERR: Yeah, so it certainly could
4 enable the FISC to back off of an earlier
5 interpretation if that's in place.

6 MS. WALD: I still have one second?

7 MR. MEDINE: Yes.

8 MS. WALD: One question, a quick one to
9 Professor Vladeck.

10 I want to make sure, 702 is kind of a
11 complicated program and if you can speak for
12 yourself or for any of the NGOs that you may have
13 had contact with, how would you characterize the
14 main concern of outside groups about the way 702
15 operates? Because I think we're all agreed they
16 had congressional authorization to begin with so
17 it's not a 215.

18 MR. VLADECK: So I wouldn't dare speak
19 for anybody other than myself, and even then --

20 MS. WALD: Okay, that's good enough.
21 That's good enough.

22 MR. VLADECK: And that's subject to my

1 wife's overruling.

2 But I'll just say my biggest concern
3 about Section 702 is the volume of communications
4 of U.S. persons that are at least ostensibly
5 available to be picked up, quote, incidentally,
6 unquote, right, that 702 bars targeting but seems
7 to contemplate, based upon my understanding of our
8 technological capacities, the collection of data
9 on a scale that makes the incidental acquisition
10 of U.S. persons communications not just likely,
11 but certain, and a very large number of those
12 communications.

13 So my biggest concern is that this sort
14 of intentional targeting requirement is a bit
15 disingenuous.

16 MS. WALD: So how would you correct
17 that?

18 MR. VLADECK: I mean, I think, there
19 are a couple of possible ways to do it, but they
20 all get to the same place.

21 One is to not allow the government to
22 file for a directive if they have reason to

1 believe that a certain percentage of the
2 intercepted communications will actually involve
3 U.S. persons.

4 One is to not just require minimization
5 requirements but actually to provide what the
6 baseline minimization requirements are.

7 I mean think there are, you know, there
8 are a number of different ways to attack that
9 problem. I think the threshold issue is that it's
10 just too likely that communications are being
11 accidentally picked up or incidentally picked up,
12 even when the government can't go after them
13 specifically. And so I think there are any number
14 of ways to scale that back.

15 MR. MEDINE: Mr. Dempsey, any final
16 questions?

17 MR. DEMPSEY: If I could.

18 So Professor Kerr, did I hear you
19 correctly to say that you do not think that
20 Section 702 bears the weight that's been put upon
21 it in terms of authorizing the bulk collection
22 program? Is that what you were suggesting? Did I

1 catch that?

2 MR. KERR: No, I was referring to
3 Section 215.

4 MR. DEMPSEY: 215, yeah 215. That's
5 your view?

6 MR. KERR: I think the arguments that
7 have been put forward and are found in Judge
8 Eagan's opinion are not persuasive based on just
9 an understanding of the current statute.

10 And I could say that when news was
11 disclosed that the bulk collection program had
12 been authorized under Section 215, I scratched my
13 head and wondered how on earth did they get there
14 based the on the statute that was written, which
15 was sort of understood as a grand jury subpoena
16 power, and on its face requires that the authority
17 be limited by the grand jury subpoena powers, only
18 a grand jury subpoena for documents, if it would
19 have been issued, that is a requirement of the
20 Section 215 authority.

21 And I imagine a prosecutor going to,
22 trying to defend a grand jury subpoena for every

1 telephony metadata piece of information in the
2 entire United States and not getting very far, to
3 put it gently, before a judge in a case if there
4 was a motion to quash file.

5 So I just don't think it's a persuasive
6 interpretation of the statute, at least based on
7 the arguments that have been put forward so far.

8 MR. DEMPSEY: Let me ask you a question
9 about minimization. You've written about issues
10 about minimization in the context of government
11 acquisition of stored data in the ECPA context.

12 Do you have thoughts about minimization
13 in the FISA context, focusing on content
14 collection, particularly where in the context of
15 where there have been reports, we alluded to them
16 this morning, that the government collects stored
17 data in transit as it's being moved from server to
18 server.

19 What are your thoughts about sort of
20 building a minimization structure that would be
21 constitutionally sound for the FISA side
22 addressing stored content, either stored content

1 that's actually in storage or stored content
2 that's captured while it's in motion?

3 MR. KERR: Yeah, I think it's a
4 difficult question in part because the meaning of
5 minimization in the national security context, it
6 strikes me as a different idea than the meaning of
7 minimization in the criminal setting.

8 Where in the criminal setting you're
9 really worried about making sure that information
10 is not ever possessed by the government, never
11 held, and certainly never disclosed in public.

12 And in the national security setting
13 it's a totally different set of concerns. It's
14 more than just is this going to be part of the
15 database, how long is it going to be retained?

16 And we're more comfortable with the
17 idea of it sort of being in a database somewhere
18 subject to certain requirements as to when the
19 database is going to be queried.

20 So one perhaps non-answer to the
21 question is it strikes me as such a different
22 question that it's not clear to me that the same

1 principles should apply.

2 And I would also point out that, for
3 example, in Judge Bates's opinion on some of these
4 issues in Section 702, his constitutional analysis
5 was one possible way of approaching it, but it
6 struck me that there's a lot of other ways that I
7 can imagine other courts interpreting the same
8 issues.

9 So there's a complicated issues raised
10 by how broad is the surveillance, how broad do you
11 take the foreign intelligence exception to the
12 Fourth Amendment, assuming that that is an
13 established exception, how broadly do you take
14 that?

15 It's a lot of murky questions that
16 would regulate that. And it's much more
17 complicated, I think, than the similar criminal
18 setting.

19 MR. DEMPSEY: Would you say it's
20 possible we're bumping up against constitutional
21 limits if there is such a different --
22 minimization in the criminal context is

1 constitutionally premised. I mean, it flows from
2 the scope and particularity requirements. So if
3 it's constitutionally-based, could we be running
4 up against, without robust true minimization in
5 the foreign intelligence field, could we be sort
6 of running up against constitutional -- certainly
7 constitutional issues, but I don't know if you
8 would go so far as to say constitutional problems?

9 MR. KERR: Yes, absolutely. So there
10 are a lot of different constitutional issues that
11 are implicated here. There's, you know, obtaining
12 contents of people's communications which is
13 obviously going to raise Fourth Amendment
14 questions.

15 There's the reasonableness requirement,
16 how that would apply in the national security
17 setting.

18 But there's not only the rights of
19 those that are U.S. persons communicating with
20 other U.S. persons, which has been the primary
21 focus in the statute so far, but there also may be
22 constitutional issues raised when a U.S. person in

1 communicating with a non-U.S. person. That half
2 of the communication was presumably a
3 constitutionally protected communication, and that
4 has not yet received much attention at all.

5 So there are a lot of important issues
6 that are complicated that are certainly in play.

7 MR. MEDINE: Any other final questions?

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

10 MR. MEDINE: Thanks to the witnesses on
11 this panel and all the witnesses today, as well as
12 the board staff that made today's hearing
13 possible.

14 The board encourages all interested
15 parties to submit comments at regulations.gov
16 relating to the topic of today's hearing.

17 A transcript of the hearing will be
18 posted on our web site at pclob.gov.

19 And I now move that the hearing be
20 adjourned. All in favor say aye.

21 (Aye)

22 MR. MEDINE: Unanimous motion, the

1 hearing is adjourned at 4:20 p.m. Thank you very
2 much.

3 (Whereupon, the hearing was adjourned)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

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

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the within-named witnesses personally appeared at the time and place herein set out, and after having been first duly sworn, according to law, was examined by counsel.

I further certify that the examination was recorded by me stenographically; that this transcript is a true record of the testimony given by said witnesses.

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 _____, 2012.

Lynne Livingston

Notary Public

My commission expires: December 10, 2014

A				
ab 295:10	278:10	acm 235:3	acute 157:7	adjudicatory
abilities 17:6	academic	acquired 70:10	ad 239:10	181:15
ability 19:21	114:10	70:17 73:20	add 21:7 22:11	administration
40:20 70:21	academics 3:14	132:13	35:8 37:14	31:8 73:4,9
86:3,4 90:7	9:5 219:12	acquisition	38:10,18 48:17	80:21 85:1
100:13 110:4	accept 73:4 75:1	301:9 304:11	51:1 59:17	118:5 123:4,7
119:8 125:17	118:6	act 1:8,10 2:10	75:2 76:2	243:10 254:9
167:2 174:17	acceptance	2:11 6:4 7:8,9	80:12 81:2	administrative
177:12 178:14	117:1	9:1 11:16 84:7	83:20 93:10	7:2
181:15 193:16	access 26:1	94:3 144:7,8	95:14 167:5	admitted 166:13
250:19 260:19	27:14 120:15	154:2 162:17	170:10 189:20	adopt 226:13,15
289:20 293:19	159:2 163:2	167:12 170:13	250:11 252:14	261:11
294:13	165:6 170:7	187:3 225:8,19	268:3 282:20	adopting 299:15
able 19:6,8,14	195:14 239:14	228:16 232:21	288:8	adoption 52:20
19:17 20:15	254:13 285:19	240:14 243:18	adding 37:15	advance 62:4
29:9 102:4,12	286:13 287:6	257:7,11	160:4 167:3	188:22
103:13 144:2	accidentally	258:16 266:9	283:7,8	advanced 254:9
144:17 152:2	302:11	299:14	addition 22:12	advances 174:16
153:9 160:17	accompanying	acting 2:17 10:8	22:16 24:12	advantage 91:15
163:7 166:7,11	90:17	action 25:4	43:11 50:14	advantages
186:8 193:21	accomplish	158:5 239:12	229:15 241:20	241:2
198:11 228:18	73:22	310:15	241:22 278:10	adversarial
231:7 250:22	accomplishes	actions 6:7,9	additional 23:4	123:2 126:9
251:4 289:10	81:13 123:14	25:2 277:14	81:17 183:1	130:7 155:22
293:13 294:1	125:19	278:3	211:8,10,12,14	157:11 158:17
295:9	accomplishing	activities 12:19	283:3,7,8	180:15,17,22
abolish 13:12	16:10 88:17	46:10 57:20	293:9,10	181:7,17
abroad 133:15	254:11	67:17 80:16	additionally	182:21 183:22
139:17	account 25:20	84:19 132:5	19:17	233:11 241:3
absence 73:7	72:15 74:7	144:19 147:11	address 11:5	274:2 284:13
121:12 275:11	88:7 112:13	154:10 201:14	81:21 94:17	287:2 295:7
295:18	119:16 289:20	202:20 217:7	142:14 236:18	adversariality
absent 88:22	accountability	256:21 280:13	addressed 216:4	286:11
89:1	130:10	282:14,15	233:16	adversaries
absolutely 16:7	accounting	290:7	addresses	54:14 74:16,20
34:17 104:16	282:11,14	activity 31:18	249:11	87:17 91:14
153:11 179:16	accuracy 214:13	45:3 51:10	addressing	93:1,4
198:5 307:9	283:10	153:22 154:1	74:11 304:22	adversary
abstract 76:1	accurate 249:21	177:1 218:3	adds 278:10	151:10 216:7
101:22 102:1	255:13	actual 46:17	adequate 190:2	217:16 218:5
115:13 289:12	accustomed	105:10,15	253:13 292:11	adverse 238:4
abuses 263:18	151:9	108:12 112:8	adjourned	238:13 274:3
	acknowledgm...	173:10 210:9	142:17 308:20	adverseness
	57:5	283:6	309:1,3	237:12,22

238:2 273:21 274:5,20 advertently 133:10 advertised 122:6 advice 156:13 223:3 advisable 86:9 86:18 advisor 205:1 206:22 207:10 advisors 153:10 185:6 204:15 204:20 205:18 206:4,13,15 207:21 218:6 advisory 6:17 advocate 124:19 124:22 125:2 147:13 159:2 159:11,15 160:4,8 162:6 162:7 165:9,16 166:6 167:21 172:1 180:1 183:1 190:18 215:17 225:3 229:10 236:11 236:17,21 237:6,22 238:10,19 239:2 283:19 284:6,11,12,20 285:8 286:14 295:15 advocates 161:5 affairs 154:13 affect 60:12 82:13,16 230:20 affidavit 18:8 affiliated 148:22 169:5	affirmatively 71:6 124:14 246:1 afoot 45:3 afternoon 8:21 143:1,2 148:5 179:20 223:18 224:21 age 40:1 117:18 117:22 agencies 8:16 38:4 62:12 67:19 137:13 153:21 176:17 203:13 205:10 205:20 206:14 255:15 agency 2:16 6:2 10:7,17 36:10 58:2 209:11 215:3,4 216:21 217:20 262:17 agent 80:15,16 80:19 208:19 agents 217:9 aggressive 243:11,11 245:11 agile 17:9 20:4 agility 63:2,6 167:1 ago 39:6 68:8 118:21 136:18 136:18 165:10 178:21 221:19 262:15 agree 65:11 96:5 188:16 199:18 207:5 251:13 259:9 agreed 7:5 167:10 201:16 300:15 agreeing 6:21	ah 264:22 ahead 59:16 143:16,20 174:10 200:22 222:22 aims 233:3,3 airwaves 291:2 akins 288:10,11 al 29:4 alarm 34:8 alert 185:7 alien 232:21 allegations 10:12 allow 22:18 27:17 86:8,21 87:7 102:4 108:19 109:10 119:18 241:5 250:17 257:7 257:11,13 260:10 272:7 275:1 301:21 allowed 82:1 114:12,16 240:10 allowing 123:9 allows 10:16 18:2 22:15,19 42:5 99:6 240:3 alluded 95:9 153:18 217:12 304:15 alluding 51:17 alternate 48:10 48:11 88:20 alternative 19:2 88:16 125:20 254:10 alternatives 177:13 298:4 ameliorate 238:5	amend 293:14 299:3 amended 243:16 269:4 amendment 23:18 69:17 101:5 110:14 111:16 113:3,9 116:10 151:1 158:12 172:19 172:22 178:17 199:10,19 260:4 274:15 275:6,17 276:5 306:12 307:13 amendments 7:9 144:7 225:1 278:13 290:21 american 4:7 20:7 92:21 93:3 96:3 117:3 193:1 196:8 203:8 211:13 218:12 220:5 234:15 234:16 235:17 americans 18:21 47:17 125:13 144:14 291:18 291:22 292:14 amicus 123:9 124:18 160:17 161:19 167:22 172:2,8,13 173:21 180:2 183:1 186:17 190:19 215:17 283:20 amorphous 239:3 amount 13:6 57:6 59:9 60:13 83:16	85:12 90:5 103:9,13 104:5 104:6 214:6,7 255:17,18 amounts 13:1 113:13 255:5 analogies 103:22 104:2 analogize 162:10 257:3 analogous 79:22 258:14 259:22 analogy 31:13 171:5 177:9,19 178:2 211:17 257:20 273:16 analysis 22:19 85:16 95:12 113:1 134:1,5 186:6 187:13 207:14 255:9 255:13,14 294:5 306:4 analyst 279:19 analysts 140:20 analytic 135:21 analytical 41:5 41:6 83:10 analyze 6:7 17:6 40:22 227:11 analyzed 135:18 analyzing 33:7 anger 279:15 animal 197:8 announced 5:10 75:4 122:2 annual 75:5 anonymous 51:15 answer 31:10 54:6 80:22 91:3 116:13 117:2 120:7,19 120:20 163:15
--	--	---	--	--

178:11 189:18	162:8 163:7	223:22 276:9	approaching	150:14,15
192:20 209:12	164:14 165:2	277:4	88:18 306:5	154:11 194:22
209:18 224:17	179:15,16	applied 48:11	appropriate	224:13 250:18
235:22 243:21	180:7 197:3,22	127:19 224:8	78:1 79:19	271:11,21
264:22 273:8	238:10,13	258:7 272:11	124:8 193:17	276:16 277:7
275:16 279:19	240:18 241:1,5	297:7	195:13 211:15	areas 95:17
281:19 286:8	270:2 272:8	applies 121:8	275:10	arent 47:3 73:15
287:17 298:16	274:3,7 277:7	136:1 155:21	appropriately	102:1 114:12
answered 21:21	283:21 289:10	202:14 203:10	6:12 33:20	140:14 250:21
182:17 209:1	appealable	apply 83:22	79:4,14 193:7	263:18
260:16	276:18 277:4	98:17 127:5,15	approval 61:11	arguably 201:1
answering	appealing	135:20 136:13	61:12 62:6	argue 173:20
298:2	151:15	257:22 286:21	63:7 66:1 73:8	192:14,15
answers 53:5	appeals 270:3	299:10 306:1	95:18 99:11	231:10
110:19 129:21	appear 190:20	307:16	100:1,10	argued 199:7
209:8	appeared 9:1	applying 79:4	139:19 179:10	294:21
antediluvian	298:7,8 310:6	79:14 128:20	180:19 181:14	argument 31:12
253:3	appearing	129:6 198:5	181:18 182:19	125:9 159:8,12
anticipate	142:11 157:20	appoint 164:15	197:12 226:3	174:1 193:17
100:20 244:12	appellate 152:2	200:11,13	227:6,9	193:22 271:19
antiterror	152:4 180:10	appointed	approve 27:4	295:7
282:13	193:19 256:13	161:19,19	51:12 62:3	arguments
anybody 53:22	258:16	169:1	142:6 182:16	125:19,20
153:12 169:5	apple 155:10	appointing	183:9 227:18	191:4,5,6,7
180:20 262:8	applicable	121:16	298:2	192:5 193:12
283:17 300:19	134:19 200:19	appointment	approved 12:10	195:12,20,20
anybodys 47:16	application	162:2 169:14	27:17 58:12	298:19 303:6
anylsis 294:1	82:17 124:1	appointments	72:17 100:16	304:7
anymore 175:8	128:8 149:17	236:22	106:21 121:2	arises 106:3
anyway 80:22	162:12 172:10	appreciate	127:21 128:1	armed 132:3
apart 37:21 38:5	181:21,22	142:11 144:3	128:17 134:1	arms 96:6,9,10
161:18 299:7	205:15 206:21	204:10 209:3,7	138:9 178:15	96:17 97:9
apocryphal 91:1	213:7,8,11	apprehensions	182:3 189:14	arrest 44:17
apologies	224:5,18,19	217:4	189:14 211:7	47:8
220:12	253:5,6 259:5	apprized 61:16	245:16 298:16	arrests 32:8
app 155:8	270:17,18,21	approach 127:6	298:18 299:2	article 11:6,9
apparatus 55:7	277:1 296:22	130:9 135:3	approver	12:22 124:22
146:20	298:12 299:21	196:17 225:3,4	180:14	127:4 152:6
apparent 268:8	applications	225:5,13 226:8	approving 31:4	154:3,4 161:13
275:4	104:11 127:20	243:12 255:19	203:21	161:14 167:8
apparently	128:1,16 129:1	255:22 256:15	arbitrary	183:16,17
265:7 282:12	130:17 148:7	258:5	119:16	197:10,14
appeal 152:2	148:20 206:18	approaches	arduous 137:13	198:6,7,10
161:11,14,20	208:12 214:13	225:10	area 56:22	201:14 211:18

212:5 223:20 236:21 238:14 238:16 271:2,5 285:3 286:10 articles 12:17,20 56:11 139:12 articulable 27:6 28:4 31:16 44:2 45:1,8 61:14 79:9 212:21 articulate 28:14 35:10 37:7 72:5 85:9 277:19 articulated 64:5 67:11 86:20 93:15 123:8 articulates 37:3 articulating 86:13 articulation 17:21 97:4 ashamed 234:18 aside 86:15 asked 39:21 90:2 91:2 107:19 114:19 117:7 136:17 136:18 140:3 150:21 156:10 195:18 209:16 224:15 275:14 asking 36:2,3,16 78:12 105:17 109:8 117:20 179:9 240:6 252:21 aspect 44:14,15 58:21 151:22 208:9 284:14 aspects 155:17 163:8 249:20 assess 8:9 40:5	64:14 88:20 130:15 assessing 78:17 assessment 25:22 50:1 79:3 89:21 118:11 assessments 89:19 assigned 181:5 assist 153:5 205:12 assistant 2:13 10:10 128:2 associate 4:7 220:4 associated 27:7 31:22 45:10,11 45:18 46:11 47:1,3 196:3 assume 53:4 207:20 285:10 assuming 61:20 184:7 191:3 253:7 290:11 290:13 306:12 assumption 82:20 263:2 assurance 4:4 220:2 assure 217:5 attack 39:5,8 262:21 302:8 attacks 16:2,11 20:7 38:20 40:14 attempt 283:6 attempting 209:4,5 attend 144:17 attention 39:15 122:14,15 149:12 150:5,7 194:3 214:15	248:16 260:12 260:19 267:1 267:19 291:1 308:4 attorney 2:13 3:10 10:10 12:11 121:2 128:2,2 137:22 143:13 164:16 164:20 190:19 208:16 attorneys 150:13 162:16 164:19 179:3 204:18 206:14 216:16 audience 209:21 audit 120:16 auditable 121:6 audited 27:1 auditing 121:4 audits 30:3 50:8 51:19,20 author 205:6 authorities 68:11 70:19 87:2,12 88:7 89:13 114:3 144:20 177:21 249:21 250:2 293:12,19 authority 71:7 71:18 82:4 84:3,4 87:8,8 99:8 111:5 154:6 156:20 157:3 167:8,17 179:8 182:2 189:17 193:16 212:16 225:14 226:5 230:10 295:9 303:16 303:20 authorization	61:19 126:17 138:2 290:14 298:11 300:2 300:16 authorize 290:9 authorized 24:22 27:10 63:13 66:16 108:2,7 144:10 178:15 239:6 303:12 authorizes 268:7 290:6 authorizing 35:10 302:21 automatic 260:9 automatically 110:4 auxiliary 197:12 availability 22:17 available 22:18 24:3,14 83:17 90:6 109:17 110:17 118:21 171:8 190:13 270:8 301:5 availed 198:19 avenue 1:17 5:8 avenues 48:15 48:16 avoid 45:20 54:14,15 88:11 91:14 175:2 235:12 239:18 254:4,17 avoiding 272:4 aware 40:10 52:19 58:11 75:3 135:5 144:18 148:1 169:6 251:4 awhile 242:18 aye 5:19,20	308:20,21 <hr/> B b 42:22 43:1 239:11 back 32:21 34:19 35:17 40:11,21 42:1 43:5 64:16 71:11 73:1 74:9 75:18 80:4,7 84:22 98:7,13 117:17 119:20 143:22 147:17 156:8 158:22 167:13 176:15 179:13 182:16 199:6 203:19 205:17 205:20 207:18 207:20 209:19 212:9,14 213:2 213:4 214:2,3 214:5,6 226:2 226:3 227:17 241:15 243:16 251:2 253:2 264:12 266:12 269:1 272:12 276:7 280:22 284:18 292:20 296:14 300:1,4 302:14 backend 128:6 background 120:22 186:7 250:16 backgrounds 251:6 bad 37:17 44:14 216:12 222:18 234:17 249:3 249:10,11 262:21 278:20
---	---	---	--	--

291:14 292:3 293:1 baker 3:4 143:6 143:20,21 147:16,18 149:10 166:17 166:20 170:10 171:12 175:7 178:4 179:15 180:5 185:22 186:15 187:2 189:20 196:2 202:7,13 207:7 207:13 210:12 210:15,17 212:11,13 213:10 balance 34:21 138:16 142:3 167:1 189:22 191:19 256:6 277:16 balanced 6:9 72:2,10,16 balancing 115:19 160:1 190:5 ballroom 5:7 baltimore 310:4 banc 189:15 band 243:1 bandying 271:20 bankruptcy 240:8,18 256:14 257:16 257:17 258:4,9 258:10,15,18 barely 157:13 bars 301:6 based 25:22 27:5 44:12 46:17 47:18 60:6 75:14	100:2,11 113:16,17,21 118:7 156:9 192:17 294:9 298:19 301:7 303:8,14 304:6 baseline 302:6 basic 112:11 113:5 161:22 243:21 287:3 basically 104:3 136:1 171:5 187:8 248:4 basics 14:13 139:8 basis 29:1,14 40:8 57:12 76:5,14 86:5 87:1,4,8 97:15 102:16 127:10 131:16 165:8 167:22 173:3 173:22 210:4 210:20,22 243:1,3 246:11 257:7 259:12 294:4 bates 152:20 batess 152:21 306:3 battle 157:12 bear 98:22 141:20 166:8 179:18 bearing 255:6 bears 83:4 302:20 beat 263:13 began 265:4 beginning 299:20 begins 255:14 behalf 127:1 149:1 155:13	199:12,21 205:18 behavior 235:21 believe 25:21 32:9 44:3 45:1 45:9 46:7 48:21 68:7,12 82:6 117:20 137:5 155:18 177:18 206:14 218:4 234:10 234:20 279:20 302:1 believed 132:14 believes 8:11 165:2 believing 40:8 belongs 113:6 beneficial 14:1 beneficiaries 67:2 benefit 26:6 284:9 benefits 8:10 151:6 245:19 berlin 221:18 best 8:12 30:21 34:5 85:8,18 115:12 118:10 119:1 190:15 215:1 221:8 229:12 251:14 266:14 270:11 beths 213:1 246:18 better 16:10 18:3 31:12 41:6 77:12 93:9 102:15 109:13 149:12 173:7 188:14 235:7 245:10 246:2 252:9,9 263:16 286:7	beyond 67:11 70:2 72:7 128:13 137:9 218:6 232:18 244:1 247:14 249:13 282:19 biannually 138:1 bifurcate 101:13 240:9 big 53:14 108:21 178:10 261:4 bigger 263:9 280:12 biggest 238:9 301:2,13 bill 57:1,8 80:10 81:5,10 237:5 296:18 billing 21:12,17 23:3,3 113:6 bills 284:2 296:17 binds 169:20 bipartisan 6:1 243:1 bit 41:10 56:11 94:18 107:18 131:7 157:17 160:21,22 167:4 183:22 194:13 204:19 208:13 237:10 256:1,6 268:5 269:11 301:14 bits 251:9 black 247:8 blind 157:18 blinded 54:5 blow 292:19 board 1:3 2:1 5:4,14,15 6:5 6:21 7:22 8:5,7 8:11 9:8 36:8	142:12 143:19 143:22 145:1 155:4 222:2 223:8 228:1 236:6 239:19 308:12,14 boards 6:6 7:1 bob 22:12 36:9 49:13 51:16 65:11 73:2 90:10 92:15 93:15 115:1 129:22 bobs 133:2 body 105:2 161:1,5 201:8 202:11 boiled 186:4 boils 287:18 bolstered 232:2 bomb 39:2 bona 200:16 book 266:19 books 111:18 borrow 240:7 257:20 293:11 bothered 268:21 bounce 194:20 brad 2:13 10:9 13:21 23:12 28:13 31:9 33:10 36:20 63:19 76:11,22 90:10 102:14 126:14 130:2 bradford 6:22 brads 77:9 brady 287:9 brain 248:20 brains 198:15 branch 6:2,7 58:16 75:9 93:20 127:18 131:20 147:9
---	---	---	---	---

154:9 182:16 218:3 227:5,8 227:16 243:5 245:5,8,13,18 245:21,22 246:5,6,6 247:7 268:15 269:13 276:4 278:19	196:20 220:7 236:9 briefed 251:4 briefing 137:5,6 137:10 295:8 briefings 131:17 230:16,16 briefly 65:15 177:10 217:22 234:22 236:18 244:20 282:21 288:9	buckets 62:18 buckley 237:8 budget 89:16 build 281:17 293:6 building 58:19 174:14 263:6 304:20 builds 63:21 built 37:17 101:17 builtin 37:12 builtup 281:11 bulk 13:17 53:15 60:5,12 81:10,12 82:16 83:22 84:3 100:4,5,21 101:3,20 102:17 104:11 104:12 105:10 106:19 108:20 129:14 159:13 180:18 181:5 192:9 209:19 230:5,10 261:4 262:5 264:20 268:7 269:16 280:2 292:15 292:19 298:3 298:17 302:21 303:11	10:8 217:15 bush 243:9 266:11 291:5 business 7:11 26:1 50:21 82:8 83:11 99:1,6 100:1 165:21 221:20 buy 274:21 buys 249:3	43:4 45:16 145:7 194:2 calls 14:16 18:21 21:16,18 42:21 105:1 150:12 231:14 cameras 190:8 cant 11:5 22:10 24:15 26:16 27:15 29:7 56:6,8 71:2,5 107:9 133:17 135:4 147:19 168:14,15 177:2 179:12 189:18 193:5 198:19 199:3 205:2 241:4 244:17,17 249:12 265:20 277:20 290:15 291:17 302:12
branches 92:16 243:4 brand 2:4 5:16 20:10,11 21:8 21:20 22:1,20 25:8 28:3,21 29:13 30:6,13 31:1 72:20,21 73:11 74:8 75:17 77:8,13 78:7,11 79:20 80:6 81:15,21 82:13 121:10 121:11 122:18 124:16 125:6 183:20,21 184:21 185:15 186:13,16 188:5 209:14 209:15 210:14 210:16 212:22 246:16,17 249:14 250:7 251:10 252:17 283:13,14 285:14 286:12 290:1	bringing 129:3 brings 141:11 british 10:17 broad 40:13 140:10,11 299:16 306:10 306:10 broader 84:8 226:16 261:8 broadly 103:9 103:12 145:2 145:17,19 186:22 306:13 broken 10:13 88:10 269:11 brought 15:10 106:4 158:5 178:5 214:14 250:20 251:22 285:8 brushing 130:20 bucket 237:11	bulwark 157:1 bumper 113:19 bumping 306:20 bunch 32:12 47:2 burden 76:19 119:21 225:16 299:3 burdens 56:6 65:9 74:3 247:7 bureau 2:18	call 5:18 16:21 16:22 17:1 56:18 77:5 86:3 113:9 126:11 150:4,6 160:17 162:7 163:22 170:5 179:2,22 181:15 185:7 196:5 208:16 227:3 265:13 270:1 283:20 289:3 called 10:16 19:15 121:1 150:20 151:22 195:19 205:16 206:15 258:11 274:13 284:8 286:22 calling 25:3 32:16 34:12	capabilities 55:10 87:10 229:1,18 233:11 242:12 244:13 249:2 capability 234:17 capable 200:21 248:1,2,2,3 capacities 301:8 capacity 108:17 108:20 135:7 175:6 capture 69:11 captured 218:3 305:2 car 84:12 113:18 176:19 255:14 cards 171:19 care 127:16,19 213:22 214:21
breadth 71:17 break 8:20 9:20 9:22 142:13 218:16 219:9 breakdown 87:8 brief 9:12 59:18 143:16 156:7 166:21 196:3			C	
			c 1:18 3:16 5:9 43:1 111:20 219:17 260:1 cables 10:19 cadre 150:13 172:5 180:3 calculated 281:15 calculation 282:6 call 5:18 16:21	

248:12 260:14 cared 214:12 career 216:20 careful 217:22 carefully 205:15 232:7 carr 3:6 143:8 147:17,18 154:18,22 156:15 159:5 160:19 161:3 161:11 162:9 162:14 168:19 171:16 172:17 174:4 176:14 178:20 179:16 180:15 181:20 183:4 184:3,11 185:1 188:11 188:15 193:15 197:15 200:4 201:12 204:13 204:22 207:12 207:15 209:9 211:16 212:12 212:14 215:20 216:20 218:17 218:20 carrier 74:13 carrs 180:12 carry 10:20 98:18 156:11 carter 242:21 case 26:2,3,17 27:15 33:13 39:3 44:13 47:11 51:14 68:17 84:10 91:17 111:15 111:20 112:21 125:18 158:4 165:9,13,18 166:9,13 168:4 168:15 170:13	170:19 172:6 173:10,21 181:6 186:14 186:17,19 187:12 188:2 190:15 191:9 199:8 206:8,8 206:8,9 238:12 240:13 245:22 254:10 255:2 259:14 270:19 270:22,22 271:2 275:6,11 275:19 276:9 285:9 288:10 288:12 289:6,9 297:15 304:3 casebycase 167:22 cases 17:13 38:21 50:11 103:19 108:9 112:7 117:20 117:22 123:10 127:7,7 128:12 129:18 155:7 159:13,14,14 162:17 165:17 166:11 185:13 187:17 192:4 193:1 206:6 207:5 235:13 240:11,13 258:10,15 259:10 260:10 272:22 274:22 276:3 285:16 cast 53:12 235:19 catch 243:16 292:3 303:1 catching 256:2 categories 81:22 139:1 259:10	categorize 276:8 category 100:7 138:3,17 cause 47:18 75:14 134:22 148:22 149:2 153:7 158:11 184:18 212:1 222:12 224:6 caused 243:9 causing 114:2 caution 97:13 cell 14:18 cells 248:20 280:13 center 3:19 4:3 219:16 220:1 263:14 281:17 centers 10:15,20 ceo 3:18 219:15 263:14 certain 13:6 66:19 73:2,5 90:16 91:18,18 103:9,18 105:6 148:7 221:2 225:15 250:1 269:5 301:11 302:1 305:18 certainly 25:7 30:17 33:11 57:6 59:12 62:9 94:1 97:1 105:18 111:17 114:1,10 116:18 134:18 138:18 150:16 152:5 161:3 164:4 165:8 177:3 179:18 189:3,8 192:9 193:15 201:10 209:9 217:18 221:1 230:7,15	239:8 243:19 262:12 282:19 290:20 291:3 295:18 297:9 300:3 305:11 307:6 308:6 certainty 271:13 certification 137:21 138:17 199:2 204:1 239:20 240:6 310:1 certifications 66:20 140:14 certified 260:16 certify 239:22 240:4 260:2 310:5,9,13 certiorari 240:2 chairman 2:3 5:3,12 6:5 20:11 79:2 81:7 125:10 236:6 252:1 295:3 challenge 156:21 157:5,7 157:10 159:18 166:12 181:7 182:22 183:2 199:9 218:11 244:8 248:22 276:22 290:5 293:16 294:15 challenged 295:5 challenges 244:4 285:22 challenging 187:11 249:19 chance 64:19 163:12 197:5 change 1:6 80:10 84:6	113:16 128:17 231:7,8 243:17 249:2 252:5 280:18 changed 112:12 changes 52:16 56:19 83:22 109:10 111:1 111:19 113:10 113:11,11 123:1,4 201:20 227:17 231:11 235:6 244:8 267:21 changing 83:13 224:14 278:17 278:22 channels 93:6 characterize 300:13 characterized 36:20,21 charge 190:22 charged 15:22 153:21 charges 177:12 check 158:22 210:9 211:8 cheese 186:9 chief 7:2,3 122:12 124:2 128:5 253:4 choice 180:6 choose 193:11 chosen 61:17 chris 12:3 cipa 170:11 171:6 177:9,10 178:5 circuit 111:21 240:3 260:2 circulated 235:1 circumspect 274:10
--	---	--	---	---

circumstance 64:8 119:2 150:6,20 151:20 154:8 201:2	178:9 186:5,11 188:19 190:1 195:14 228:17 230:15 234:11 234:12,16 239:14 271:21 281:19 291:12 291:13 292:9 294:7	151:14 227:3 closed 230:17 268:13 280:16 closely 122:12 146:8 232:9,15 closer 84:7 closes 122:5 closest 288:9 cloud 249:12,13 clued 248:14 clunky 176:19 coauthor 220:15	collecting 145:15 269:15 269:16 293:4 collection 7:11 7:17 12:1,6,7,9 12:13 13:14 53:16 61:7 66:8,15,17,18 67:7 68:11 71:6 72:3,6,8 72:11,16 81:10 81:13 82:16 84:1 94:9,10 94:22,22 95:4 95:7,11,16,18 100:1,3,11,21 101:3,20,21 102:17 105:10 107:5,22 111:5 129:17 132:11 133:22 136:2,3 136:19,22 144:12 145:22 153:20 159:13 174:6 178:16 180:18 181:5 192:10 209:20 230:6,10 255:10 268:7 280:2,18,20 281:12 282:12 292:19 298:3 298:17 301:8 302:21 303:11 304:14	41:8 42:6,11 84:21 86:1,15 88:13 90:1,13 94:6 126:3 130:5,22 174:14 176:12 177:8 204:12 209:2 241:11 242:17 277:12 combined 273:5 combining 226:5 come 34:22 60:6 74:8 75:17 101:18 116:16 118:14 126:21 149:11 150:19 157:19 159:16 160:3 179:13 182:16 195:1 206:5 207:5,8 213:15 223:2 234:16 246:5 251:2 252:22 294:13 comes 30:3 71:11 72:11 91:9 102:21 107:7 119:3 148:1 164:7 203:12 207:17 207:18 299:6 comething 245:6 comfort 130:6 comfortable 65:7 77:6 160:16 177:3 305:16 comforted 292:17,17 coming 33:4 127:12 131:5 147:17 195:17
circumstances 26:18 61:21 70:9 93:21 163:19 174:5 184:22 200:7 232:17	claus 157:18 clause 172:21 236:22 274:15 clear 8:4 21:13 42:7,13 99:7 100:14,15 106:16,18 113:16 130:8 173:19 183:12 196:7 215:8 286:8 292:7 299:12 305:22	codification 59:3 codified 58:18 102:13 150:1 codify 104:9 cognizable 111:16 cognizant 112:15 cointelpro 232:22 collapses 202:4 collateral 84:17 colleagues 15:18 15:19 223:11 228:18 collect 13:1 14:17 70:21 71:15 91:12,21 100:17 102:11 146:20 235:9 235:10 254:4 255:1,5 256:1 293:19	collections 136:6 collects 7:12 13:4 304:16 college 4:8 220:5 collins 2:7 5:16 33:3 35:16 36:15 39:19	clearance 73:8 158:2 168:13 176:6 clearances 161:6 169:19 cleared 158:13 162:20 233:20 clearly 44:19 52:6 93:14 172:19 186:2,3 186:17 clerk 204:17 276:2 clerks 204:18 205:3 208:4 client 9:3 150:21 155:13,14 192:17,21,22 193:4 clients 155:5,8 195:6 239:15 cloak 155:20 close 49:8 96:20
circumvent 11:15 cite 45:13 cited 103:21 citizen 66:1 citizenry 60:13 67:22 citizens 53:17 65:19 67:15 136:6 city 44:6,11 civil 1:3 5:4 6:10 23:8 24:22 103:7 116:22 121:20 122:12 127:7 222:2 223:8 248:15 267:13 277:17 cja 162:16 clarify 264:16 class 239:11,12 classes 258:10 classic 32:18 classification 165:4 169:21 234:10 classified 93:14 94:19 124:4 135:17 156:4 157:14 159:3 165:7 167:18 170:4,7,12 171:2 172:4	clearance 73:8 158:2 168:13 176:6 clearances 161:6 169:19 cleared 158:13 162:20 233:20 clearly 44:19 52:6 93:14 172:19 186:2,3 186:17 clerk 204:17 276:2 clerks 204:18 205:3 208:4 client 9:3 150:21 155:13,14 192:17,21,22 193:4 clients 155:5,8 195:6 239:15 cloak 155:20 close 49:8 96:20	collected 12:14 100:5 104:22 106:20 120:10 120:13 132:16 133:3,6,10 134:12 135:2,6 135:16 136:2,5 165:14 280:22	collecting 145:15 269:15 269:16 293:4 collection 7:11 7:17 12:1,6,7,9 12:13 13:14 53:16 61:7 66:8,15,17,18 67:7 68:11 71:6 72:3,6,8 72:11,16 81:10 81:13 82:16 84:1 94:9,10 94:22,22 95:4 95:7,11,16,18 100:1,3,11,21 101:3,20,21 102:17 105:10 107:5,22 111:5 129:17 132:11 133:22 136:2,3 136:19,22 144:12 145:22 153:20 159:13 174:6 178:16 180:18 181:5 192:10 209:20 230:6,10 255:10 268:7 280:2,18,20 281:12 282:12 292:19 298:3 298:17 301:8 302:21 303:11 304:14 collections 136:6 collects 7:12 13:4 304:16 college 4:8 220:5 collins 2:7 5:16 33:3 35:16 36:15 39:19	41:8 42:6,11 84:21 86:1,15 88:13 90:1,13 94:6 126:3 130:5,22 174:14 176:12 177:8 204:12 209:2 241:11 242:17 277:12 combined 273:5 combining 226:5 come 34:22 60:6 74:8 75:17 101:18 116:16 118:14 126:21 149:11 150:19 157:19 159:16 160:3 179:13 182:16 195:1 206:5 207:5,8 213:15 223:2 234:16 246:5 251:2 252:22 294:13 comes 30:3 71:11 72:11 91:9 102:21 107:7 119:3 148:1 164:7 203:12 207:17 207:18 299:6 comething 245:6 comfort 130:6 comfortable 65:7 77:6 160:16 177:3 305:16 comforted 292:17,17 coming 33:4 127:12 131:5 147:17 195:17

199:6 222:19 269:20 commencing 1:18 commend 221:10 comment 59:18 115:18 172:8 197:6 200:19 216:19 217:21 234:21 commentator 261:1 commented 160:15,20 comments 9:16 46:13 117:16 144:5 155:12 166:18 180:13 308:15 commercial 22:6 commission 6:4 248:15 267:13 267:14 310:22 commitment 248:19 committee 3:22 218:21 219:21 229:16 230:13 230:14,17 231:3 241:20 248:5 252:2 267:6 committees 59:22 61:2,4 131:14,22 132:1,3,4,6 228:14 241:22 244:1 248:3,7 248:8 common 222:12 commonly 19:15	communicate 32:9,10 209:11 communicating 307:19 308:1 communication 10:14,18 65:16 69:13 96:1 256:2 284:20 308:2,3 communicatio... 7:19 16:20 47:16,17 66:4 69:12 71:20 112:5,9 132:12 132:13,19 133:11 136:4 144:13 151:2 156:11 165:15 193:4 228:16 239:5 289:5 301:3,10,12 302:2,10 307:12 communicatio... 144:13 community 37:3 89:7 91:8 109:22 117:8 141:15 142:7 202:21 203:17 204:7 communitys 15:8 companies 10:21 23:14,21 24:13 25:6 86:13 87:7 96:3 99:5 155:9 175:21 company 18:19 23:22 86:5,5,8 86:8 87:3,3,13 113:4,7,8 compared 88:2	115:20 116:9 comparison 25:19 51:2,7 comparisons 46:14 compartment... 189:5 compelled 24:8 156:10 compelling 116:5 competent 266:6 competently 224:17 competing 174:20 291:9 competition 22:3 competitive 22:6 complement 15:11 complete 163:1 completely 162:19 178:5 207:8 complex 118:19 129:12 216:2 251:1 278:15 complexity 250:13 compliance 30:1 35:3 36:17 50:3,15 64:15 77:5,19 78:9 78:13,15 215:18,22 complicated 43:7,10 184:10 284:1 300:11 306:9,17 308:6 complied 287:7 comply 211:1	289:21 290:13 comport 229:6 composite 19:22 comprehensive 224:7 comprehensiv... 62:21 comprised 6:4 compromising 55:9 60:18 292:16 compulsory 159:18 computer 3:10 4:2 29:17 45:14 70:14 103:14,17 143:13 219:22 computerized 103:6 conceivably 24:10 concept 65:6 102:9,19 167:21 200:6 conception 198:8 concepts 101:16 275:7 278:1 conceptual 95:15 conceptualists 197:9 concern 22:9 24:11 25:10,10 42:15 63:4,22 64:3 65:18 88:9 121:11 232:13 235:16 237:14,17 251:3 254:3 300:14 301:2 301:13 concerned 93:1	125:4 130:7 254:18 concerns 6:11 13:13 22:21 23:5 24:7 26:7 64:18 71:17 89:4 104:13 116:22 117:2 123:11,13 124:21 170:3 178:12 236:17 237:12 238:1,3 238:5 255:19 277:17 294:8 305:13 concise 186:12 conclusion 54:9 concrete 45:12 concreteness 45:20 concurrences 111:21 condition 171:17 conduct 30:9 45:4 50:21 66:10 129:1 147:9 154:12 203:16 204:6 216:8 224:7 conducted 38:12 66:19 131:6 146:22 conducting 202:19 203:13 conducts 144:19 confer 288:13 confidence 58:18 59:5,7 63:21 148:8 149:21 169:18 190:4 206:1 208:5 211:14 confident
--	--	---	---	---

130:19 238:15	266:12 267:4,8	conscious 142:2	constituents	214:20
confines 194:15	267:20 272:12	consent 5:22	251:15	consultants
confirm 205:16	273:7,20	consequence	constitute	174:18
confirmation	278:14,19	47:11	111:15 237:5	consuming
257:18	289:16 290:5	consequences	constituted	124:11
confirmed	291:1,7 295:19	8:11 47:5,7	238:4	contact 48:22
130:11 240:17	298:1,10	141:21 177:15	constitution	80:18 180:20
conflate 115:3	299:12 300:1	conservative	116:12 129:19	228:19 300:13
conflation 51:4	congressional	245:4	151:1 154:4	contacting
conflicting	89:14 131:2,8	consider 7:22	166:3 191:18	17:19
291:18,19	198:4 228:4	116:21 148:4	192:14 201:4	contacts 34:13
confront 49:20	236:15 241:17	220:14 235:6	275:13	181:1,16
49:20	241:19 242:7	277:14	constitutional	255:10
confronted	246:18 247:2	considerable	129:13 133:6	contain 56:12
194:8	247:11,13	233:14	161:16,21	containing
confronting	263:7 266:15	considerably	165:1 170:9,22	156:5
145:4	300:16	46:15,18,21	173:15 174:1	contemplate
confused 59:9	congressman	47:6 48:7	191:6,19 193:8	301:7
confusion 57:7	223:15	60:22	193:13 196:13	contemplated
congress 3:20	congresss 227:6	consideration	197:17 198:3	265:2
7:6 9:5 37:14	congresswoman	1:6 52:19	198:17 199:13	content 14:15
37:18 50:5	220:10 247:19	53:10 55:13	200:1 201:13	16:19 110:15
53:19 57:1	290:3	74:6 110:16	203:1 224:10	110:18 112:4,8
58:15 59:19	conjunction	119:13 185:8	234:6 236:16	132:11 304:13
60:1,10 61:2	35:6 129:14	207:1	237:17 270:12	304:22,22
79:19 123:18	connect 10:14	considerations	270:15 271:8,9	305:1
131:4 147:9	16:8,9 19:20	25:6	275:3 276:13	contents 307:12
148:11 150:10	21:6	considered 6:12	283:16 306:4	contested 25:3
170:2,5 187:3	connected 19:13	60:20 110:1,8	306:20 307:6,7	context 17:7
199:14,22	connecticut 1:17	206:19 234:9	307:8,10,22	39:13 52:6,8
201:5,6,15	5:8	298:15	constitutional...	75:19 84:3
203:10,11	connecting 41:7	considering	163:7 173:12	85:4,11 89:13
214:22 219:13	83:5 176:2	65:3,13 67:9	constitutionally	89:14,15,18
219:17 223:5	222:11	69:3 89:2	154:11 162:8	94:13,16
226:2,3,19	connection	298:21	199:3 304:21	103:22 109:19
227:5,9,17,18	11:10 29:3	consist 8:15	307:1 308:3	113:12 114:1
234:1 242:11	83:15	consistent 61:18	constitutional...	123:14 128:15
243:6,15 244:6	connections	75:11 178:16	307:3	128:21 130:15
245:2,6,7	14:7 83:6,12	211:6	constrained	135:3,5 136:12
246:10 247:15	83:18	constant 279:14	232:14	157:9 170:21
247:22 248:1,6	connectivity	constantly 38:6	constraints 38:5	172:14 212:21
249:18 261:6	83:10	constituencies	construction	223:1 224:18
263:5,12 264:9	connotation	231:4,10 269:1	198:18	226:12 240:8
264:9,19,22	180:2,3	269:3,7 294:8	constution	257:17 258:18

270:4,5 273:16	275:6,12	42:10 64:19	countries	102:16 106:8
273:19 274:6,9	conventional	90:21 106:9	222:13	109:16 110:8
275:8 276:19	183:18 273:18	133:14 134:20	country 68:1	111:22 112:21
282:22 284:21	conversant	140:7 301:16	141:17 191:15	113:2 114:6,19
293:12 304:10	253:22	correctly 105:4	191:17 218:22	115:9 124:3
304:11,13,14	conversation	122:4 187:17	219:4 223:13	125:2,17 128:7
305:5 306:22	90:8 126:4	224:8 302:19	262:12 264:15	130:4,17 134:2
contexts 97:7	147:22 219:1,5	cost 262:2 281:9	country s 6:18	138:4,10
103:5 110:17	291:6 293:14	281:11 282:6,7	232:20	140:14 142:5
115:6 120:4	294:4	283:2	county 310:4	142:15 143:4,9
145:5 276:21	conversations	costs 8:10	couple 62:13	146:7,13,18
continual 246:8	233:20	281:14	65:17 72:1,9	147:1,5 148:7
continue 16:1	convey 218:12	couldnt 24:17	72:22 88:14	148:9,11,14
28:6 53:12	convinced	41:13 73:6	98:21 132:9	150:3,12 151:7
54:8 59:14	237:20	177:5 201:9	144:5 161:2	151:17,22
continued 53:6	cook 2:7 5:16	288:14	186:5 187:16	153:3,5,11,13
continues 36:18	33:2,3 35:16	council 235:3	190:12 200:7	155:2,11 157:3
continuing	36:15 39:19	counsel 2:15,17	243:13 278:17	157:12,16,21
30:11 137:15	41:8 42:6,11	2:19 3:22 10:6	296:4 301:19	158:4,18,21
continuously	84:21 86:1,15	10:8 57:19	course 24:13	159:16,21
50:16,20	88:13 90:1,13	97:2 148:13	27:21 44:5	160:3,9,16
contradiction	94:6 126:2,3	152:1,12	53:14 59:11	162:5 163:2,11
290:8	130:5,22	156:14 158:13	88:20 141:13	163:13 164:15
contrary 295:12	174:14 176:12	161:1 165:6	154:4 176:18	164:21 165:2
contributes 14:5	177:8 204:12	170:4 179:22	208:10 229:3	165:12 166:2
control 138:8	209:2 241:10	198:2 216:7	229:10,18	169:6 171:5
141:1 147:10	241:11 242:17	219:21 239:11	237:13 253:15	172:7,11
203:16 232:18	277:11,12	253:4 279:21	261:10 262:14	173:12 175:14
controlled 232:7	cooperation	285:13 286:2	272:21 297:19	175:19 176:16
232:15 233:6	86:5 92:6,6	287:15,20	court 3:2,7,8	177:20 180:14
controlling	copies 59:20	288:3 289:18	7:16,20 8:3 9:2	180:17,19
114:2	copy 10:19	310:8,14	18:9 26:21	181:10 182:20
controls 27:14	205:16 207:16	count 73:14,16	27:9 29:19	185:13 186:1,1
27:16 98:18	core 103:10,13	74:1 145:9,9	35:5,9 41:20	187:2,5,21
100:19 101:1	104:6 155:19	276:5	42:1,2,7 51:22	188:1 189:15
115:14	206:17 240:19	counterprodu...	55:3 58:13	190:13,20
controversial	258:11,13	234:7	61:15 62:3,7	192:1 193:19
44:8 266:10	287:14	counterterror...	63:7 64:13,14	193:20 197:7
267:17	corporate 97:18	6:18 7:7,14	64:19,22 65:9	197:10,16
controversies	97:21 98:5	17:11 26:15	66:1,20 76:3,7	198:7 199:6,9
237:15 266:17	120:9	36:19 37:9	76:9 77:17,18	201:13 202:1,2
controversy	corporations	40:12 107:14	78:9,13,14	202:3,11,17
51:3 84:20	96:13,18	115:8 146:2	80:2 81:2,16	203:9,21 204:6
259:15 271:3	correct 35:2	counting 73:15	100:7,16 101:1	204:22 205:18

208:1,6 210:6	114:6 150:5,6	108:7,8 125:13	63:20 67:5,9	117:18,21
210:7,10,13,18	160:6 161:14	127:7 155:7	86:11 90:5	118:1,2,3,8,20
210:22 211:3	183:2 194:2	162:17,17	119:6 126:9	119:7 120:13
211:11 214:10	198:10 201:5	168:4 170:13	228:9 238:1,4	120:15,21
214:11,12,15	201:15 203:3	177:12 226:11	250:8	121:6 132:18
217:5,7,18	213:3 226:20	226:13,14,16	curve 118:16	133:5,22
218:15 219:3	227:10 240:3,9	249:20 270:4	custodians 55:6	134:12,17
227:1,4 233:14	260:2 271:17	287:8 293:11	customer 155:6	135:2 137:2
237:7,13	278:19 284:9	305:7,8 306:17	cut 266:11	144:13 145:22
238:11,14,16	288:20 289:19	306:22	280:22	155:6 255:18
238:17 239:22	289:20 293:17	crisis 222:17	cyber 132:5	281:17 293:15
240:2,5,10,14	306:7	223:5	145:21 146:3	293:20 301:8
240:17,18	courtyard 92:3	criteria 62:14	cynical 247:3	304:11,17
241:3 243:5	cover 11:22 14:6	120:15		database 26:2
245:4,11,17	164:2,2	critical 16:7	D	29:17 120:17
250:20 256:14	coverage 11:13	110:12 145:22	d 1:18 5:9	165:13 305:15
257:17 258:15	11:20 12:5,11	220:21 256:21	111:20	305:17,19
259:13,14,16	13:6	critically 42:18	damage 91:10	databases 235:5
259:18,20	covered 11:21	122:11 145:14	dangers 154:14	datas 24:13
260:3,5,13,14	11:21 56:22	criticism 57:7	dare 300:18	date 16:22
260:15 263:7	covers 101:8	229:9	dark 251:17	210:21
264:4,4,5,6	crack 54:1	criticisms	darn 253:7	david 2:3 5:2
270:4,7,9,21	craft 244:11	264:18	data 10:15,19,20	12:3 143:21
271:15,18,18	250:13	critique 254:8	16:20 17:7	day 35:6 62:6
272:5,13,16,20	crafted 243:2	cross 92:13	18:20 19:21	63:14 89:18
273:1,8 274:3	create 23:4 24:2	crs 237:12 238:8	22:14 23:21	120:5 147:7
274:4,13	29:14 168:21	crucial 153:11	24:5,5,7,19	170:21 177:11
275:19 276:2	182:22 238:22	243:22	25:5,12,19	185:13,14
280:19 282:22	239:17 289:17	curbing 278:10	26:8,11,15	217:6 310:17
284:16 286:17	created 22:22	cure 269:12	27:1,4,14	days 26:20,22
287:19 288:4,9	201:6	curious 280:9	36:11 38:10	27:2 29:20,21
288:11 289:11	creating 124:12	current 25:22	40:1,2,6,21	30:2,6 36:14
289:18 294:3	270:6 286:11	26:4 30:21	43:5,12,15,18	37:1,12 42:1
294:14 295:8	creation 159:1	37:21 58:7	51:15 60:6	50:12 51:19,20
298:7,14 299:1	196:4	77:15 82:3	62:21,22 69:15	52:1,1 58:13
299:13	credibility 192:1	84:19 86:16	72:11,13 83:8	63:12,13 64:16
courtroom	214:9	90:9,20 111:13	83:12,16 97:20	73:21 76:5
190:9	credible 194:1	114:2 118:10	98:4 99:14	119:11,20
courts 23:19	crime 3:10 71:4	119:1 174:17	100:7,13	139:20 205:14
26:11 27:3,19	92:5 105:6	228:22 237:4	102:12 103:6,9	253:3
30:5 64:20	116:2,3 134:9	237:15 238:18	103:10,13	daytoday 48:1
99:11,22	143:13	272:10 297:19	104:5,6 105:2	131:8 152:5
100:10 103:11	criminal 23:9	303:9	106:3,9,13,19	de 2:15 10:6
103:16 113:12	31:18 45:2,4	currently 63:10	109:17 110:5	11:4 13:19

18:22 22:10 25:17 28:11 29:2,16 30:9 30:17 35:8 36:7 37:1 51:1 57:15,18 62:9 66:6 69:20 70:1 72:1 75:2 76:11 85:7 89:5 93:10 94:17 96:11,21 98:6 114:22 118:9 119:12 120:21 121:19 131:10 133:12 134:18 135:11 135:14 136:10 136:16 139:7 139:14 140:12 279:20 dea 217:2 deal 115:4 168:6 181:3 215:12 225:8 243:6 293:14 296:12 dean 4:7 220:4 debate 15:4,17 58:20 59:10 92:14,16 93:12 261:1 265:18 265:18,20 266:4 290:21 292:5 297:1,12 297:19 debated 53:15 53:19 140:8 266:22 debating 266:9 decades 228:21 262:11 december 310:22 decide 98:12 161:8 168:7	181:6 182:2 192:4 196:9,17 201:1 207:18 263:15 264:3 decided 201:7 decides 178:10 deciding 181:4 181:11 198:7 decision 121:21 140:1,5 142:2 142:6 157:6 170:16 186:2 187:15 189:3 199:7 200:2 216:10,11 238:14,22 256:15 258:22 272:5 282:7,17 282:18 decisionmaking 160:6 decisions 59:21 89:16 105:7 140:15,19 148:9 151:11 159:7,10,21 160:2 165:4 180:18 191:7,8 192:18 205:12 208:7 240:9 274:4 declaration 37:2 declarations 18:6 declaratory 158:4 declassification 184:6 declassified 55:2 129:11 136:11 159:20 291:5 294:3 declassifying 123:18	decrease 22:6 dedicated 250:3 deemed 79:19 deeper 261:16 deeply 214:13 default 189:1 227:3 299:15 defend 253:15 303:22 defendant 170:15,18 defender 169:2 defenders 194:18 defense 27:22 121:2 132:2 232:12 267:8 defer 18:22 76:11,22 deficiencies 278:12 define 46:6 definite 112:10 definitely 131:10 204:16 definition 166:4 definitions 41:3 definitive 46:10 degree 46:17 47:20 66:2 67:15 68:2 167:9 degrees 8:16 delay 256:21 delegates 214:20 delegating 167:16 deliberately 183:5 189:5 delighted 220:13 223:9 delineate 75:12 delving 254:20 demands 155:6	155:16 democracy 261:3 democratic 59:13 290:12 demonstrates 90:18 dempsey 2:6 5:16 10:1 43:20,21 49:6 49:17 50:22 52:9 54:3 95:20,21 96:12 97:16 98:9 99:12 101:7 102:6,20 104:17 132:9 134:13 135:9 135:12,22 136:14,17 137:8 166:16 166:17 171:4 171:14,21 174:3 202:6,7 204:8 268:1 269:18,19 272:6 273:10 275:2 277:9 302:15,17 303:4 304:8 306:19 308:8 dempseys 120:8 denial 276:22 289:11 denials 277:3 department 2:14 3:10 10:11 27:2,22 30:2 34:2 36:2 50:5,6,7 51:20 63:20 77:1,16 78:4 121:2 127:1 129:3 130:3,18,21	132:2 139:20 140:22 143:6 146:9 163:3 213:16 214:10 214:18 217:9 265:6 departure 259:1 depend 189:8 251:8 288:7 289:2 depending 74:17 145:9 264:5 depends 60:15 65:4 188:18 213:10 285:7 depth 62:22 deputy 2:13 10:9 derives 52:3 describe 131:15 described 166:8 description 274:18 deserve 52:19 53:19 deserves 39:14 53:6 design 263:5 designated 200:13 designed 34:8 65:21 156:22 225:18 designing 263:16 desirability 227:12 desirable 60:8 297:14 desire 47:16 despite 108:8 destroyed 24:13 281:1
--	---	---	---	--

detail 88:11 135:17 177:2 189:13 284:4	98:19 116:17 117:1 122:16	203:5,22 213:12 221:12 222:13 229:15 230:3,4 275:7 277:13 296:18 302:8 305:6,13 305:21 306:21 307:10	299:4 directive 157:4 173:12 274:1 295:4 301:22 directives 156:4 165:13 directly 189:19 206:15 279:3 director 2:20 3:18 4:3 7:1 18:8 122:1 139:21 140:20 219:15 220:1	227:15 231:2 231:17 273:4 289:17,21 disclosures 55:9 86:9 88:22 91:7 97:1 106:6 126:22 discontinued 18:17 discourse 94:2 252:6 discover 14:20 29:10 discoverable 267:3 discovery 14:20 29:10 48:13 72:4 103:7 discretion 148:12 149:5 150:10 153:4 161:7 163:21 164:8 discriminatory 44:10 discuss 11:11 135:4 144:2 147:6 231:6 251:5 discussed 82:11 97:22 99:4 144:16 145:20 167:4 224:21 225:11 241:16 254:12 266:13 discussing 26:17 121:18 126:6 177:9 293:18 discussion 8:13 9:6 15:4 38:11 43:22 60:10,21 74:21 75:20 86:2 90:4,19 92:20,21,22
detailed 71:1 131:16	developing 117:3	differently 72:13 160:3 165:4 difficult 16:15 18:11 20:1 38:19 63:5 64:14 73:15,22 74:22 83:18 118:17 124:4 124:11 157:15 169:9 173:22 181:2 188:22 189:8 194:9 206:2 207:16 224:16 239:8 239:22 245:13 245:17 254:19 257:2 270:15 271:9,18 277:18 299:3 305:4	disadvantage 293:4 disagree 135:4 disagreement 277:5 disappear 30:7 disapprove 227:18 discerned 115:5 disciplined 68:22 disclose 74:14 86:4 119:8 156:10,10 158:6 167:18 170:14 171:2 178:8 194:19 disclosed 54:17 60:18 111:12 197:20 236:16 262:3 291:4 303:11 305:11 disclosing 85:1 170:18 189:22 190:1 292:13 294:6 disclosure 54:13 54:20 56:20 60:22 92:19 93:2,17 158:11 225:4 226:6	
details 11:6 53:2 53:18 60:11 94:20 172:12 259:8 262:4 285:5	development 6:12 33:18	difficulties 156:1 difficulty 276:7		
detainees 239:13	developments 114:5	dignity 193:3		
determination 28:19 29:1,15 29:16,18 30:10 30:12,18,19,20 30:22 31:14,15 32:6 33:13 34:2,18 35:4 42:2 45:22 46:18 47:10 61:14 62:4 63:8 78:18 120:14 136:8 253:14	develops 109:20 device 113:18 113:19 devils 259:7 devoid 198:9 devoted 126:5 dialed 16:22 dialogue 214:2 231:2 268:22 269:6 294:5 diane 7:3 dichotomy 112:10 dictates 285:2 didnt 34:7 209:18 264:19 267:1 281:5 295:11	dinner 221:19 direct 122:1 148:12 238:12 238:19,22 239:17 288:18 directed 66:14 67:21 94:22 95:1 184:3 282:13 direction 55:4 64:20 295:1		
determinations 30:1,3,4 48:2,7 49:9 55:20 62:5 63:15,16 63:19 64:17 77:4,17 78:10 204:2	difference 47:19 111:1 159:4 183:5 285:6 286:10 different 15:10 16:3 40:17 42:12 43:5,6,8 47:6 79:22 81:17,20 101:19 104:12 109:11 114:18 136:13 140:18 144:20 145:5 145:10 168:17 180:2,3 181:8 181:17 182:3 182:14 186:6 190:12 200:7			
determine 20:21 54:22 66:10 115:11 118:1 156:14 208:22 258:6				
determined 68:10 102:17				
determining 31:6 278:2				
deterring 278:6				
develop 212:19				
developed 33:15				

93:6,12 115:2 144:6 160:8 196:1 209:22 213:1 230:1 239:19 284:17	divorce 23:8 25:2 283:4 dni 67:8 75:4 85:7,21 137:22 dnis 122:12 doable 248:18 docket 127:13 206:6,9,11 207:6,18 doctors 115:12 doctrine 199:13 199:13,15 200:18,20 document 67:9 124:12 documentation 76:7,8,13,14 76:18 79:10 139:22 documented 28:19 29:17 63:16 139:17 documents 99:21 157:16 170:7 303:18 doesnt 21:15 54:16 68:3 96:16 128:8 135:13 165:3 182:5 215:10 224:12 244:14 256:19 265:18 275:21,22 276:1 doing 25:15 34:3 37:15 42:3 54:15 65:1 91:20 95:6 127:6,13 167:11 209:4,5 212:2 214:18 221:15 234:19 247:1 249:8 268:16 271:17	279:5 280:14 280:15 296:19 doj 3:4 15:19 23:12 31:3,5 31:10 32:21 33:17 143:12 214:5,5 dollar 146:21 domain 124:9 292:6,7 domestic 14:8 14:21 dominate 266:6 dont 10:1 11:4 13:19 23:11,18 25:21 31:14 41:2,18 43:17 48:16 54:7 55:14 56:3,5 57:9 59:2 61:1 66:13 71:9 73:17 74:1 81:19 83:1,7 92:13,20 93:15 97:2,3 99:18 110:19 114:1 114:13 116:4 119:16 120:18 127:10 129:2 129:21 130:16 130:17 134:16 136:10 138:14 139:13 140:6 153:12 154:7 163:17,20 164:1,21 166:2 170:2,8,20,21 175:21 176:4 176:10,15 177:4 178:11 178:18,18 180:9 182:9 183:5,13,14 184:12,17	185:8,17 189:16 190:7,8 191:12 195:2,9 195:19 197:5 199:17 201:17 202:5 205:21 210:12,17 211:9 212:18 219:4 223:9 233:10 237:3 244:14 250:15 251:7,17 252:3 253:14,16 258:2 259:16 260:14 261:13 261:13 263:10 263:11,20 265:1 266:2,5 266:14,22 267:4 271:7,12 271:22 275:18 278:4,5 280:10 280:17 287:16 289:11 290:9 292:9,18 304:5 307:7 doors 230:17 268:13 280:16 dots 16:9,9 19:20 21:6 41:4 83:5,5 doublebarreled 53:21 doubt 53:12 58:3 279:22 downside 283:7 downsides 139:6 downwards 22:3 dozen 68:9 dozens 155:5 draft 150:2 dramatically	243:10 drastic 279:15 draw 54:7 125:17 273:14 282:5 dream 195:20 195:20 dribbling 222:21 drive 203:18 driving 111:4 dry 91:19 dual 183:2 due 156:12 282:21 duly 310:7 duty 57:19 274:13,14 276:10 dysfunctional 231:5
E				
				eagans 303:8 eager 296:7 earlier 35:17 39:20 62:20 63:19 89:11 90:2 99:4 114:17 117:18 120:8 152:22 204:14 215:16 224:21 228:6 241:13 247:10 254:3,12 256:12 285:21 294:12 296:21 300:4 early 16:16 earth 303:13 easily 173:5 easy 69:22,22 184:9 185:16 185:19 188:22

189:7,10 200:10 295:19 echo 114:22 ecpa 293:12 304:11 edges 298:9 educate 209:4,6 267:20 education 4:3 220:1 251:6 edward 25:22 effect 91:6 231:9 278:8 effective 20:6 36:4 83:3 92:5 109:18 122:17 203:16 247:5 277:19,20 278:3 280:6 effectively 28:16 54:12 149:21 158:16 227:14 245:15,21 effectiveness 36:16,22 37:19 38:1,17 39:9 56:9 75:12 118:8 effects 56:19 effectuated 93:18,19 95:2 139:19 effectuates 58:21 efficacy 234:13 282:22 283:2,5 283:9 effort 93:20 221:9 282:3 efforts 6:14,18 7:4 18:4 37:22 49:14 50:4 57:11 eight 145:8,10	178:21 220:20 243:15 261:7 296:3 either 8:6 11:20 41:11 44:16 61:15 79:16 124:12 134:7 139:13 148:11 150:9 182:21 190:9 192:22 207:7 210:10 229:8 244:11 250:20 279:9 304:22 elaborate 146:9 194:14 237:9 237:19 280:1 elect 261:12 elected 233:18 233:22 250:20 261:5 electronic 7:18 65:15 85:3 205:7 228:15 element 17:12 eleven 127:11 eliminate 55:14 56:4 81:10 elisebeth 2:7 5:16 email 38:12 249:11 emergency 64:6 emphasize 130:1 141:5 148:18 empirical 40:7 employed 169:1 employees 97:4 empowered 193:12 240:14 en 189:15 enable 54:14 88:11 194:7,16	247:17 300:4 enables 252:17 253:20 enact 226:18 enacted 167:11 enacting 290:6 encompass 264:20 266:3 encompasses 261:20 encourages 308:14 encouraging 225:4 ended 38:14 44:9 280:3,6 enemys 233:1 energetic 160:22 energies 18:3 enforce 78:1 215:1 enforced 68:21 215:2 enforcement 24:19,21 28:17 292:21 engage 191:3 233:19 235:19 252:10 256:20 engaged 46:9 115:2 246:7,12 246:12 engaging 204:1 enhance 148:8 278:11 enhanced 243:11 enhancing 216:20 enjoy 23:18 enlai 91:2 ensure 6:11 33:19 43:12 57:22 82:7	101:4 129:19 159:11 208:7 ensured 59:5 ensuring 6:9 153:6 226:1 enterprises 146:21 entire 126:5 304:2 entirely 54:17 81:14 155:12 156:5 161:7 162:3 270:19 272:4 290:11 entitled 69:17 288:3 entity 97:10,11 environment 21:17 40:12 envision 150:12 162:15 177:15 216:16 equality 272:17 equally 228:13 248:2 equipment 281:12 equipped 224:17 227:10 escalate 17:22 especially 75:18 144:21 154:21 227:11 230:14 essence 82:22 171:6 essentially 6:16 61:6 64:11 65:21 82:11 84:6 224:2 228:17 231:1 231:17 establish 81:16 139:16 established 6:2	76:15 93:6 101:3 210:5 220:16 221:5 306:13 establishes 81:18 154:5 establishing 288:1 etcetera 23:17 52:16 57:10,14 112:6,6 138:17 172:5 265:3,9 eugene 4:2 219:21 european 221:22 evading 200:22 evaluate 38:1 39:9 61:17 114:7 191:2,4 212:20 evaluating 145:2 223:21 evaluation 25:18 38:16 118:13 119:2 event 7:4 15:14 147:21 163:17 184:15 216:2 243:8 everybody 11:8 13:5 57:12 67:20 101:11 167:10 168:6 265:7,18 everyday 82:17 everyones 251:14 evidence 22:8 30:15,16 52:6 71:3 78:17 81:16 105:6 106:10,10 108:13 109:5
--	---	--	--	--

111:7 134:8 evidenced 14:22 evidentiarywise 109:4 evinces 96:22 evolution 241:18 evolving 249:4 ex 125:9 157:21 181:1,16 211:20 224:18 270:18,21 exacerbate 237:22 exact 237:17 exactly 41:15 48:22 49:3 65:5 72:6 76:2 76:3 78:12 186:15 288:21 291:13 examination 310:9 examined 310:8 example 17:17 17:20 19:8 24:18 25:4 27:11,15 28:8 28:21,22 29:2 29:5 32:5,19 40:17 45:13 46:5,10 48:20 50:10 52:22 67:20 73:14,17 73:19 76:5 94:10 102:6 136:21 145:6 165:12 173:10 178:6 185:22 205:13 239:11 239:12 240:2,8 255:9 286:12 289:10 294:2 306:3	examples 254:20 ex ante 63:7 64:6 exceeding 64:20 excel 210:18 excellent 219:8 228:12 exception 61:21 62:3 64:6,10 306:11,13 exceptionally 131:12 exceptions 105:5 109:2 exchange 9:13 268:22 exclusive 154:12 166:1 exclusively 108:5 executed 156:21 214:22 executing 50:17 214:19 executive 4:3 6:2,7 7:1 11:14 58:16 68:14 75:9 93:20 105:5 127:18 131:20 144:22 147:9 154:10 154:11 165:3,5 171:3 182:15 201:15,21 218:3 220:1 227:5,8,16 243:5,19 245:5 245:8,21 246:5 246:10 247:7 268:15 269:13 276:4 278:19 exemplary 146:14 exercise 70:18	150:9 252:12 270:22 exercises 241:21 242:12 exercising 87:12 exigencies 256:18 exigent 61:21 64:8 exist 40:15 152:3 238:1 existence 38:13 99:2 existential 255:22 existing 30:11 259:5 exists 24:19 247:18 exit 261:15 expand 202:12 expanded 108:18 expect 12:18 58:7 78:15 128:21,22 147:4 202:17 203:9 280:10 expectations 64:21 203:7,7 expected 62:8 64:22 203:12 expeditious 122:19 expeditiously 122:8 expenditure 38:9 expensive 38:7 experience 31:6 60:7 131:8 150:15 161:12 162:18 164:10 175:14 176:16	184:12 205:19 228:15 255:11 experienced 156:14 expert 170:11 175:15,20 268:9 expertise 182:18 244:22 250:17 287:1 experts 3:14 174:18 228:11 228:19 229:7 229:14 230:4,8 expirations 182:6 expire 225:16 expired 20:10 expires 310:22 expiry 37:22 explain 10:22 28:7 269:2 explained 65:11 113:1 128:6 291:15 explaining 265:7 explanation 298:6 explicit 101:15 explicitly 85:4 102:10 275:12 exploited 232:1 explore 8:9 expose 94:4 176:8 exposed 113:8 expost 65:12 express 274:2 expressly 35:10 273:21 extend 244:1 extended 91:16 extending 66:2	extension 156:2 extensive 266:3 extensively 270:3 extent 24:6 33:17 40:4 55:22 57:22 59:6,18 63:21 75:9 81:1 95:3 107:3 111:4 113:10 129:12 131:9 149:7 187:4 197:19 external 50:4,20 extra 271:4 extract 114:11 extrajudicial 274:13 extraordinary 70:5 127:16 141:9,16 276:20 extreme 298:9 299:22 extremely 14:1 16:7 18:14 153:14 159:13 215:8 eye 184:5 189:6
F				
face 57:9 303:16				
fact 18:12,12 29:10 33:20 35:1 40:9 43:11 53:1,4 53:11,13,17 54:8 55:9,20 57:7 62:2,5 63:11,12 64:2 64:13 66:8 67:6 68:19 72:13 79:3,12 85:14 90:14,15				

101:4 102:18 110:3 121:19 128:7 136:18 139:1 140:16 140:22 168:8 171:16 179:4 181:3 182:12 183:14 197:7 200:9 204:3 210:2 230:4 233:11 243:3 247:1 255:6 262:4 274:21 276:11 280:22 289:3 294:1 295:3 factbased 148:21 facto 110:4 factor 58:3 109:22 110:2 110:12 278:22 factors 12:2 52:4 109:15 110:7 facts 17:21 34:19 44:2 45:1,8 124:1,4 187:12 259:6 285:20 286:1 294:5 factual 76:14 173:22 187:18 191:6 196:14 285:18 factually 104:21 fade 120:5 failed 289:21 failure 282:7 failures 282:1 fair 57:6 88:15 235:1 fairly 71:1 152:19 201:20	207:5 faith 157:18 160:6 216:13 faithfully 214:21 false 235:13,15 254:4,5 255:6 282:2 283:11 familiar 133:19 133:20 161:12 212:5 226:11 236:14 familiarity 212:19 families 168:10 far 52:6,6 105:13 108:9 169:6 202:10 204:5 215:8 218:2 226:9 236:8 275:3 298:20 304:2,7 307:8,21 fascia 257:12 fashion 146:14 fashioned 111:6 favor 5:19 46:15 54:2 308:20 fbi 13:22 15:1 15:18 27:10 46:1 47:13 49:10 50:14 92:2,2,9,10 213:11,13,14 214:4,5 217:1 217:13 fbis 49:22 fcc 20:22 21:10 21:10,11,19 22:5 fear 67:18 92:20 243:9 feasible 52:8 86:9,18 95:5	184:4 186:18 fec 288:10 federal 2:17 3:6 4:1 5:11 7:7 10:8 24:20 26:5 38:4 143:8 169:2,14 194:17 198:20 219:21 276:19 federally 169:1 federated 254:14 feedback 79:18 136:20 feel 44:9 62:12 125:20 172:16 209:11 243:10 feelings 57:14 fell 108:1 felt 79:15 149:9 185:2 fewer 83:5,6 89:3 fi 66:16 fia 142:1 fiber 10:19 fide 200:17 field 171:19 210:20 213:14 213:19 214:4 217:10 307:5 fiftyfifty 298:21 fig 247:4 fight 108:9 115:22 158:21 figure 78:14 85:8 118:19 171:12 176:7 185:16 190:14 215:12 222:22 223:1 267:6 268:17 276:8 283:6 figuring 192:8	298:1 file 301:22 304:4 filed 18:6,8 86:12 files 103:15 filing 128:22 157:15 158:10 158:14 163:4 filings 157:13 final 94:6 115:18 120:6 130:22 142:8 153:17 215:15 219:12 240:11 256:16 302:15 308:7 finality 259:17 finalization 257:8 finally 9:4 27:19 132:5 152:10 163:18 195:18 222:14 240:14 258:16 finances 40:15 financial 103:19 248:20 find 15:14,20 34:13 35:3 44:16 45:15 49:1,3 112:3 154:7 180:7,10 181:1 182:11 189:21,22 193:10 232:1 252:3 259:8 finding 68:15 208:22 211:22 fine 51:2 finely 174:13 finger 175:9 fingers 123:20 finish 207:14 first 5:5 8:15,19	9:6,10 19:12 21:15 30:15 41:13 44:22 46:13 54:2,6 55:11 57:15,19 66:14 68:13 76:16 80:11 81:1 86:10 88:14 89:5 95:7 98:22 121:14 122:5 127:20 129:7 143:2 150:2 151:8 152:11 155:1,20 157:5 158:12 166:17 168:21 172:10 172:11 176:14 178:7 181:21 184:5,11 186:1 188:17 192:6 210:7 211:17 230:2 232:5 236:20 238:22 241:16 262:10 275:15 288:19 296:8 310:7 fisa 3:8 7:9 11:19,21,21,22 12:11 55:3 61:5 68:15,16 70:13 75:6,13 75:15,16,18 80:1,13 82:4 99:10,22 100:7 100:10,16,22 102:16 114:6 114:19 127:13 130:4,17 136:2 136:2,12 138:4 142:5 144:7 146:13,18 148:11,20 149:16 151:17
---	---	--	---	--

155:2,7,11,17 156:4 157:12 158:4 161:7 167:10 169:5,5 172:7 176:16 177:20 180:14 184:19 187:5 197:7 201:16 202:1,11 205:8 205:9,9,14 214:10 216:5 217:4,7 223:19 227:1,3 237:13 237:13,14,16 237:18 238:3 238:16 239:22 240:9,10,13,17 241:3 242:22 243:3,5,13,16 243:17 245:4 245:11,17 247:13 253:5,6 257:6,12 260:5 264:4 270:5,7 270:13 273:15 274:3 280:19 287:19 288:4 289:11 290:21 294:2 295:8 299:1,13 304:13,21	123:1,9 126:6 126:12,16,20 127:3,11 128:6 128:20 129:8 131:20 138:10 143:10 160:16 162:3 164:19 174:19,21 178:3 180:16 181:1,2 183:6 183:15 184:4 187:15 195:2 198:2,22 201:7 201:16 205:14 206:22 210:1 213:8,17 224:21,22 226:6 228:9 246:21,22 258:1,5,14 259:12,15 273:4 283:21 298:7 299:19 300:4	fiveyear 24:2 fixed 153:7,8 216:14 fixes 291:10 flawed 82:19 flexibility 84:9 flip 87:19 176:18 floodlight 54:4 flow 47:5,7,12 flows 10:19 307:1 focus 17:15 18:2 18:3 65:21 69:16 144:6 192:12 236:12 248:11 253:14 253:18 307:21 focused 20:5 89:20 122:14 248:17 249:8 267:19 focusing 304:13 folks 12:3 26:7 51:5 66:12 94:13 97:13 115:2 119:1 126:10 130:6 133:19 140:3 222:11 292:22 follow 33:9 50:17 67:12 92:1 120:7 126:3 177:10 209:16 246:17 followed 129:20 271:6 following 88:13 90:1 107:18 126:14 followup 20:12 28:3 49:7,22 56:10 72:22 75:20 86:2	264:17 force 165:3 171:1 227:8,16 forced 170:14 170:15 178:8 187:8 forces 273:6 foreign 1:9 2:11 3:2 7:15,18,19 8:2,22 11:15 14:7 26:20 27:7 32:1,7 58:12 65:18 66:10,21 67:3 71:2 80:15,16 80:17,19 105:8 125:12 129:1 134:2,7,15 140:13 142:15 143:3 146:2,6 149:1 150:2 153:3,19 154:1 154:13,13 163:10 218:15 219:3 222:6 225:7 226:10 256:13 263:3 299:14 306:11 307:5 foreignbased 149:1 forgetting 84:2 forgot 299:8 form 79:8 158:8 185:21 187:6 198:16 formal 123:7 formalizing 69:4 formally 206:11 former 3:8,9,19 3:22 8:22 9:5 59:12 143:12 152:20 155:3	197:14 219:13 219:16,20 228:3 268:10 formerly 3:4 143:6,10 forming 222:11 formula 108:1 forth 71:4 75:16 104:15 105:16 131:18 134:9 164:3 173:4 186:7 213:2,4 214:2,3,5,6 217:2 284:18 296:14 forward 40:20 42:5 55:1,4 117:3 122:7,17 154:15 160:7 186:8 217:14 223:14 229:21 256:22 290:4 294:10 303:7 304:7 found 77:4 78:13 243:14 249:19 267:7 303:7 foundation 57:2 112:17 founder 3:9 143:12 four 6:4 9:5 40:6 62:17 205:2 260:4,6 fourth 23:18 38:10 63:1 67:8 69:17 101:5 110:14 111:15 113:3,9 116:10 151:1 172:19,22 178:16 199:10 199:19 274:15
---	---	---	--	--

275:5,16 276:5 306:12 307:13 fraction 88:6 frame 222:22 framework 290:19 292:6 frank 294:19 franklin 7:1 frankly 88:1 89:17 157:16 168:2 231:5 fred 3:16 219:17 free 209:11 220:7 223:3 freeranging 202:20 french 91:3 frequent 131:12 131:16 217:13 frequently 36:1 41:21 64:8 124:2,3 fresh 242:11 friends 115:12 frisk 28:17 31:16 44:7 51:7,9,12,16 51:18 79:9 frisking 46:20 frivolous 129:1 front 34:4 51:17 95:5 126:12 127:3 128:4 181:13 195:1 214:10 frontend 132:20 full 17:22 18:10 39:15 49:16 58:15 157:3 165:6 188:8 209:18,18 282:10 285:18 fulltime 6:5 fully 200:5	220:18 267:15 286:4 287:7 290:13 fullyinformed 242:2 function 15:9 77:15 149:20 153:20 196:4 212:5 221:6 223:5 224:3 226:22 241:22 242:9 250:19 252:7 276:15 283:1,2 287:14 290:12,12 functioning 220:19 243:4 267:15 functions 6:17 122:10 152:5 197:13 249:22 fundamental 112:22 fundamentally 16:3 255:20 further 15:1 47:13,14 49:13 67:10 108:18 159:19 160:7 163:10,19 185:7 189:13 194:14 310:9 310:13 future 90:9,20 111:19 112:12 113:11 114:4 229:2,17 <hr/> G <hr/> gag 157:9 gain 162:18 164:10 game 168:9 175:10 223:12	279:9 gang 243:15 261:7 gather 18:19 gathering 66:14 gchq 10:18 gears 183:22 gee 222:5 general 2:13,15 2:17,19 10:6,8 10:10 11:7 12:8,11 27:20 28:1,2 30:5 48:1 50:7 52:12 57:19 66:7 68:6 70:16 72:2,3 82:4 94:18 97:2 99:20 106:22 121:2 122:21 128:2,2 137:22 146:19 165:11 202:19 230:21 234:10 242:5 254:22 279:20 generalize 273:13 generalized 137:20 generally 47:21 66:11 71:1 89:7 97:1 99:10,22 103:16 generate 235:15 generated 49:11 gently 304:3 george 3:17 219:18 germany 221:18 getting 54:5 63:2 71:7 78:12 108:4	129:3 134:22 136:20 140:2 192:2 194:13 211:22 218:1 229:15 248:13 249:21 265:10 270:7 279:14 280:12 282:10 295:21 304:2 give 18:6 28:8 28:21,22 36:11 45:19 51:5 52:21 64:19,21 74:16 87:9 94:10 130:20 148:11 160:5 161:18 163:9 163:11 164:4 178:13 179:8,9 190:13 205:13 207:16 208:17 211:13 245:14 254:19 284:8 286:13 given 33:15 34:16 46:1 58:1,7 64:7 83:8 87:11 93:17 95:6 97:14 132:5 150:11 155:14 157:3 162:8 164:1 204:13 232:10,19 236:7 274:1 285:18,19 287:17 296:9 310:11 gives 67:20 84:9 130:3,6 154:5 201:5 giving 44:3 45:1 45:8 218:14 286:9	glad 209:12 gleaned 118:12 glimpse 156:9 globalized 96:2 glove 217:17 go 19:14,18 20:16 27:15 35:16 42:1,5,7 42:20 49:18 59:16 71:6,11 74:1 92:12 98:13 108:9 117:3 119:19 128:3 135:17 137:9 143:16 143:20 145:11 151:17 177:2 180:8,10 182:1 182:10,11 189:4 191:10 194:12 195:17 200:22 201:22 201:22 202:10 203:19 212:9 212:14 213:17 219:9 226:2,3 226:17 227:5,9 241:15 245:6 245:22 246:22 251:18 272:12 272:12,13,15 275:2 292:22 293:3 298:10 300:1,1 302:12 307:8 goal 191:14,15 220:22 221:1 goalposts 249:1 goals 254:11 goes 97:20 131:4 140:13 227:1 229:22 247:7 256:1,22 262:5 271:4 276:7
---	---	--	--	--

284:18 286:17	269:13 271:12	119:13 126:11	governments	94:1 108:19
going 15:13	273:11 279:14	127:3 128:22	25:12 90:15	247:17 254:5
31:20 36:5	280:20 290:4	138:10,20	96:18 111:10	greatest 9:12
40:19 41:19,20	292:20,22	144:19 145:11	116:7 149:6	115:21 116:8
43:17 52:11	293:3,4 296:14	149:1,18 150:3	166:12 195:22	118:11,16
54:21 55:1	297:14 303:21	151:13 152:16	222:7 225:14	grew 206:7
57:13 60:21	305:14,15,19	155:6 156:8	229:5 230:5	217:3
73:1 74:8 83:3	307:13	157:2,21	231:1 276:20	group 45:11
84:22 85:1	gold 262:13	158:10,22	283:1 297:14	164:9 165:22
87:16,22 91:7	good 5:2 16:12	159:3,22	governmentwi...	166:4 168:22
91:10 98:9	20:19 22:1	160:14 165:18	87:1	194:17 195:15
108:12 109:3	24:15 31:20	167:2 170:8,13	governs 107:3	221:2 222:5
111:6 112:6	37:17 41:9	170:15 171:1	gps 113:18,19	232:16 265:1
117:5,17	43:21 44:14	175:8,16 177:4	grade 282:19	groups 221:13
120:19 122:17	67:13 74:16	177:5,11,14,16	grand 19:9	280:12 300:14
123:20 125:11	75:22 94:2,5	180:20 181:2	20:15 23:17	guantanamo
142:6,13 143:2	143:1 149:19	181:17 182:15	41:11,14 42:16	239:13
147:12 151:17	150:8 198:12	185:4 191:1,3	43:8 103:7	guarantee 43:17
165:5 166:4	201:8,16,17	191:13,15,16	108:9 109:2	guarded 232:9
167:5 168:12	212:2 216:13	194:3 195:13	303:15,17,18	guardian
171:10,18	235:4 239:11	196:11 199:7	303:22	239:10
174:6 176:7	253:7 270:14	209:16 210:1	grandma 244:18	guess 18:16 61:9
179:22 180:7	291:21 293:13	211:1 213:3,5	266:18	76:5 78:7
181:6,13 185:5	300:20,21	213:7 216:8	grandmothers	90:11 98:15
186:11 187:14	goodness 152:9	217:4 222:17	220:14	102:14 112:11
188:12 190:3,6	google 10:15	222:21 223:6	granted 128:7	119:15 149:5
196:5,17,18	gosh 152:8	225:16,20	granular 247:12	175:18 187:20
201:22 205:8	gov 9:15,18	226:2,15 227:1	247:15 248:9	198:14 242:13
205:22 206:1	308:15,18	229:4,9,16	granularity	247:11,19
209:19 211:5	govern 120:12	233:2 234:19	87:10	254:14,17
211:14,21	235:4	243:4 246:22	grasp 173:8	259:11 265:10
213:12,18	government	250:1 256:20	grassley 68:7	274:9
214:12 215:1,4	7:12 8:15 9:2	257:7,11	gray 271:11	guidance 117:10
217:14 227:16	10:18 13:15	262:17 264:13	276:16 277:8	guidelines 121:3
229:1,11,18	24:10 26:5	272:7,8 274:17	great 25:17	136:19 137:12
236:9 242:13	32:8,16 34:10	277:15 279:22	67:18 76:19	guides 191:8
244:13,16	53:2 70:18	280:10 283:3	80:7 115:4	guy 222:20
245:9,16 246:1	77:6 86:6,14	284:19 286:13	119:5 208:5	253:8
246:11,12,13	86:21 87:5,22	286:17 289:20	236:5 242:19	guys 33:4 101:9
248:16,22	88:5,7 92:17	290:13 293:18	244:21 281:4	262:21 278:21
249:2 250:21	95:22 96:7	295:9,12	296:12	291:14 292:3
250:22 251:19	97:6,11 98:12	298:10 301:21	greater 46:21	
253:11 259:15	103:20 105:16	302:12 304:10	55:21 67:14	
267:9 269:6,13	115:22 119:7,9	304:16 305:10	68:2 72:16	
				H
				habeas 239:12

hackers 24:15	292:21 293:1	hate 199:6	heart 255:20	highest 198:16
hacking 25:8,13	happy 146:3	havent 152:12	heavily 34:17	223:6
hadnt 162:22	147:5,11	178:4,20	111:13 173:13	highly 26:4,10
163:6 201:3	217:13 235:22	182:17 197:4	187:18	44:8 129:17
half 30:1 44:22	237:9,19	215:4	heightened	hill 242:3
45:2,8 220:20	harbored 256:3	haystack 108:4	95:17	296:15
308:1	hard 59:10 72:5	108:21 254:8	held 1:16 13:15	hinge 270:16
halt 142:7	72:12 131:15	254:11 263:20	24:8 232:16	hinges 101:12
hand 15:1 86:21	158:15 168:3,5	281:10	267:19 305:11	hired 248:11
86:22 97:12	168:11 169:10	head 171:15	help 14:6 139:10	hiring 122:3,8
156:7 158:21	170:16 178:19	238:9 256:8	156:14 159:11	historical 59:8
164:5 166:22	193:10 214:16	303:13	160:17 161:9	165:8 186:7
181:20 190:6,8	232:11 244:10	headnotes 188:3	166:7 200:3	historically
194:15 217:17	269:12 274:11	headphones	208:6 214:20	11:22 58:5
292:10 310:16	278:18	94:15	229:16 235:4	67:18 68:1
handful 172:5	harder 16:3	headquarters	251:9 278:11	118:17
185:10	19:22 187:14	10:18 92:2	helped 155:5,17	history 220:18
handholds	191:14 289:13	213:15 214:4	helpful 9:21	232:20
212:20	295:21	hear 76:8 229:5	15:21 16:8	hit 62:20
handle 76:21	hardest 238:7	230:15 233:18	18:14 33:5	hitting 90:4
133:22	hardware	281:6 295:11	37:8 72:4	hold 177:19
handled 272:22	255:15	302:18	92:14 126:13	279:16 281:10
handling 127:8	hardy 243:1	heard 22:2 31:2	126:18 142:10	289:20
157:14	harm 93:16	62:16 90:13	204:11,11	holding 99:16
hands 69:22	158:11,11	94:14 115:10	218:7 223:7	113:15 222:3
162:3	190:2 269:14	160:4 174:20	helpfulness 40:5	holdings 23:19
happen 89:10	harman 3:18	175:2 188:6	helping 234:5	hole 247:8
148:16 172:9	219:15 220:10	228:8 229:3	256:9	homeland 132:6
176:1 268:13	220:12 242:15	232:5 233:17	heres 210:4	honed 195:8
269:4 291:8	242:18 247:20	236:10 246:20	227:2	honor 144:1,1
293:2	247:21 252:14	257:22	herring 237:10	154:16 228:2
happened 15:6	252:19 262:7	hearing 1:4,16	hes 128:10	hop 41:13,15
51:13,21 60:7	262:10 265:15	5:5,10,18,19	253:8,8	255:10,13,14
93:17 148:2	266:5 278:4	6:20 7:21 8:8	hesitate 279:19	hope 148:8
158:3 165:12	280:17 290:3	11:3 13:10	hidden 231:2,17	150:16 153:9
204:4 297:17	290:16	90:15 125:10	267:4	153:14 216:11
happening 22:8	harms 93:15,18	158:18 159:7,8	hide 234:14	222:5 223:12
85:17 93:16	harvard 262:14	163:2 183:11	268:17	244:4
167:15 251:17	264:12	216:9,9 251:22	high 79:16	hoped 294:22
happens 30:8	hashed 273:6	308:12,16,17	130:10 224:12	hopefully 202:8
35:11 88:2	hasnt 128:8	308:19 309:1,3	232:3	282:1
89:12,18	215:3 260:15	hearings 208:19	higher 84:14	hopes 256:2
159:21 178:9	hat 228:3	222:3 233:1	128:14 135:1	hops 19:15 43:9
212:17 213:5	268:11	267:19 291:8,9	208:1	55:18

horrified 221:21	183:21 208:21	198:6,7,10	179:9,22	33:16 44:10
hotel 1:17 5:7	209:11 228:4	208:14 211:18	183:11 185:15	77:7 225:11
84:11 101:9,9	230:12 232:2	212:1,5 223:20	189:19 194:7	284:5
101:10,10	236:12,18	238:15,16	194:15 195:6	implementing
hour 99:17	277:12 282:20	271:2,5 277:6	197:2 198:14	6:3
236:8	idea 37:17,17,18	285:3 286:10	200:5 201:8	implicated
hours 251:19,19	48:14 64:5	iiis 183:8 208:13	202:8 203:6,7	307:11
house 3:22	65:12 75:22	ill 28:6,13 53:22	204:18 205:6	implication
17:20 131:14	79:2 113:5,17	76:11,22 92:1	205:16 220:13	11:12
132:6 219:20	124:7 160:16	138:2 166:20	222:3,8 223:9	implications
242:21 252:2	169:14 174:8	196:2 199:5	229:8 231:21	70:2 224:10
266:10,11	177:3 179:21	204:9 234:21	236:9 237:9,19	262:1 283:16
household	187:21 189:12	235:22 240:22	241:12 244:18	implicit 185:2
248:16	226:12,18,22	246:3 268:4	253:3 262:6	254:7
houses 60:1	228:8,12	293:11 301:2	263:11,15,16	implore 12:16
hpsci 253:4	236:11 239:19	illegal 94:3	263:19 265:10	important 17:12
hpscis 251:22	245:20 257:5,9	235:21	273:3 274:10	18:13 39:13
huge 109:3	272:2 273:3	illustrations	275:3 279:18	43:14 48:12
214:6,7 255:5	305:6,17	39:2	288:19 296:20	58:3 78:19
human 51:16	ideal 159:1	im 5:2,3 11:5	299:11,20	83:21 87:21
193:2,3	ideas 171:22	16:13 21:10	imagine 118:18	92:10 96:5
humiliation	194:20 225:7	31:9 36:9,16	158:15 211:3	110:8 114:9
44:18	identified 68:9	40:10 42:9	219:5 222:19	115:1 121:7
hunch 29:8	177:17 216:4	45:7 46:4	244:17,17,19	122:11 123:10
hundred 229:6	identifies 77:16	52:11,17 54:5	249:12 281:7	124:14 133:16
hundreds 39:6	identify 48:15	59:16 73:1,8	288:1 303:21	141:20 144:10
hurdle 199:17	identifying	74:5,8 76:1	306:7	145:14 152:6
hurt 292:4	14:16 82:9	77:6,9 78:7,11	imagining	152:14 153:14
hybrid 172:3,15	idiosyncratic	78:12 81:5,13	278:13	163:8 168:9,10
177:20	230:7 268:19	81:19 90:11	immediate 47:8	175:9 192:3
hypotheticals	ignore 260:18	98:7 99:19	immediately	194:22 198:1,9
271:20	ignored 243:13	105:17 109:8	44:16,20 45:4	208:6 225:6
	ignoring 248:4	111:2 117:5,19	46:3 272:12	226:7 228:13
	ii 3:1 154:3	120:19 135:5	immigration	229:10 260:11
	167:8 201:14	135:11 146:3	23:9 177:14	273:12 281:2
id 12:15,15 13:7	236:21	147:5,11,21	impact 11:1	285:18 288:2
14:10 15:18	iii 3:13 70:12	150:7 155:11	12:1 71:19	297:22 308:5
26:3 37:14	94:13 124:22	163:8,16	72:16 82:2	importantly
38:3,10 54:1	127:5,22	164:20 168:1	84:18	105:13 169:3,8
62:13 63:18	128:16 149:8	168:12,16	imperative 95:6	impose 56:3,6
66:22 72:9	152:6 161:13	169:6,7 170:11	278:22	74:2 247:6
76:7 80:4,22	161:14 174:11	171:9,10 173:4	implementation	imposed 100:12
117:13 126:3	183:16 184:19	173:5 174:6,12	6:13 284:1	105:14 133:5
143:22 161:2	197:10,14	175:1,7 177:2	implemented	impossible
169:22 182:8				

188:21 189:11 253:10 283:4 impressed 217:1 217:6 243:2 impression 172:10 243:8 improper 68:18 improve 31:2 148:6 inability 269:2 inaccurate 11:17 inadvertent 132:17 inappropriately 67:21 68:11 incentive 251:18 incentives 251:12 incident 77:19 incidental 95:4 280:20 301:9 incidentally 12:14 133:10 141:12 165:14 301:5 302:11 incidents 282:2 282:9 include 8:22 9:4 21:15 136:5 170:5 247:14 258:21 included 108:3 includes 35:14 39:16 42:4 66:17 105:1 including 39:2 92:5 133:21 138:14 144:21 237:4 260:5 274:4 286:18 incomprehens... 124:13 inconsistent	155:18 165:19 increased 62:10 247:14 increasing 141:21 indefinitely 101:11 independence 218:1,9,12 independent 6:1 47:14 148:13 179:22 182:2 196:8,18 216:7 218:11 independently 78:10 indicate 280:5 indicated 16:18 18:9 24:16 38:22 41:10,22 49:13 64:13 92:15 indication 18:7 indicator 74:16 indicators 20:3 indicia 58:6 individual 47:1 47:3 49:20 82:14 84:5 113:18 125:18 127:14 140:11 140:14,19 150:19 152:1,1 163:1 204:2 205:11 261:19 283:11 292:16 individualized 138:22 individually 19:20 93:8 individuals 82:9 130:11 193:5 234:5 235:20 industries	228:21 ineffective 54:18 inevitably 15:5 197:16,18 261:21 infinitely 43:7 influenced 267:21 informal 131:17 information 4:4 7:18 10:20 12:14 13:2,4 13:14 14:17,18 16:4 17:18 18:19 19:11 20:17,17 21:4 24:3 27:10,11 28:9 30:20 41:16 45:22 49:4,10,13 58:15 67:2 68:18 69:6,18 70:6,10,15,17 70:22 71:7,9 71:12,15 76:10 77:18 79:8 80:3,14 82:1 85:14 87:4,22 88:5,10 90:5 91:12,19 95:5 95:11,13 96:2 103:18 107:14 110:6,9,10,11 110:13,18 113:2,6 114:12 115:10 120:10 134:4,6,8 135:6 136:1 138:13 167:18 167:18 168:2 170:4,7,12,14 170:18 171:2,8 176:9 178:9 180:5,21	181:16 190:1 195:14 220:2 228:18 229:21 230:15 232:8 233:19 235:1,8 235:9,11 239:14 247:16 249:17,21 250:8 251:9 254:4,13 255:2 255:5 256:1 267:3 286:14 287:6,21 288:15 294:7 304:1 305:9 informational 288:12 informative 112:2 informed 20:4 59:19 159:10 177:1 201:9 infrequent 149:9 151:3 infrequently 148:18 164:11 206:5 inimical 256:3 initial 133:13 257:12 272:5 initially 161:3 initiates 157:5 initiation 162:2 initio 295:10 injunction 257:3 injury 288:12 288:18 innards 292:8 inner 265:1 innocent 261:22 input 160:1 194:10 inquire 280:16	inquiries 120:17 inside 136:3 139:19 221:2 221:15 276:4 insight 85:18 218:14 inspector 27:20 27:22 28:2 30:4 50:6 68:6 146:19 202:18 inspectors 48:1 instance 56:21 66:14 127:20 129:7 172:18 176:21 184:5 187:9 193:18 200:8 264:17 281:16 instances 68:9 152:17,19 153:1 187:10 206:20,20 207:19 234:19 institute 100:22 institution 59:13 219:2 institutional 58:6,8 166:10 institutionally 93:8 instructing 299:13 instruments 108:17 insurmountable 199:18 integrated 22:15 integrity 50:15 149:20 231:15 intel 131:14,14 131:21 132:1 241:22 intellectual 3:11 143:13
---	---	--	---	--

2:11,20 3:2,5 7:14,15,18,20 8:2,22 10:17 11:16 15:8,9 15:16 26:13,20 29:3 31:21 36:9,10 37:3 37:19 38:22 39:17 50:8 54:11 55:7 58:12 59:22 60:18 61:2,4,7 66:11,13,21 67:7,16,19 71:3 89:7 91:8 91:13 94:2 105:8 109:21 117:8 118:22 120:4 129:2 134:2,8,15 139:21 140:13 140:21 141:14 142:7,15 143:3 143:7 146:2,7 146:20 150:2 153:3,20 154:2 158:6 163:11 202:21 203:17 204:7 218:15 219:3 220:15 225:8 226:10 244:1 248:7 252:2 253:22 256:7,14 267:5 268:11 279:18 280:7 299:14 306:11 307:5 intended 11:22 14:6 72:15 232:18 intensely 248:14 intent 29:6 81:6 81:8,11 82:7 164:4	intention 82:10 intentional 132:17 301:14 intents 58:19 interact 230:18 interaction 206:13 interagency 66:9 73:8 intercept 47:16 intercepted 239:5 289:5 302:2 interest 17:2 71:22 111:16 115:21 116:7 119:5 122:5 151:15 164:13 166:10 193:2 198:11 232:12 239:3 252:12 269:10 270:6 interested 52:17 76:8 146:4 253:17 269:8 294:7 308:14 310:15 interesting 194:5 222:10 225:6 236:8 279:21 295:16 interests 26:7 116:6 123:3 150:22 158:12 165:21 166:3 200:14,17 215:14 230:19 230:20 231:12 234:7 251:15 289:12 interfere 64:18 interferes 287:14 interim 257:5,7	257:18 intermediary 78:5 intermingled 59:11 internal 37:12 50:4,19 64:4 121:6 139:14 internally 50:9 89:2 130:9 135:16 138:9 international 14:21 internet 98:14 98:17 99:9,13 155:16 280:2 280:14 internment 232:21 interpret 299:13 interpretation 108:6,11 160:18 197:18 200:2 224:16 226:14,16 227:2,4,6 230:5 231:1 245:5,12 259:4 268:6 269:15 298:8,9 299:16 299:17 300:1,5 304:6 interpretations 35:13 225:5 226:4,6 231:16 268:18 273:5 interpreted 96:19 106:8 224:9 interpreting 226:12 306:7 interrupting 140:7 intersection	174:9 intervening 47:9 interwoven 187:13 intimations 111:19 introduce 10:5 introduced 13:11 introduces 255:7,16 intruding 167:7 intrusion 46:16 46:17,21 48:8 113:22 invasion 115:20 116:9 invest 238:18 invested 289:3 investigate 48:19 investigated 282:3 investigation 2:18 10:9 15:2 17:11,17,22 18:1,12 47:13 47:14 48:15,16 49:5,15,16,22 67:4 80:13,17 84:13,16 100:4 104:7 108:2,7 108:12,14 109:6 211:21 investigations 18:10 70:11 82:2 120:4 232:22 investigative 17:4 18:4 19:4 49:14 50:11 119:21 177:22 249:20 293:11 investment	282:16 invitation 204:13 223:17 invited 172:7 inviting 143:22 154:20 228:1 involve 12:9 14:15,16 128:12 188:19 302:2 involved 27:12 33:17 34:17,17 57:10 68:13 115:10 124:10 181:4 192:5,12 192:13 198:13 213:8 218:2 233:21 235:20 265:19 282:17 285:15 292:15 involvement 31:3 141:18,22 142:3 involves 7:17 14:14 46:19 85:12 219:12 involving 144:12 191:9 227:12 ipad 244:12 iphone 229:20 244:12,14 ipso 110:4 ironically 231:10 irrefutably 91:11 isnt 97:9 102:13 140:10 188:8 191:14 194:3 200:20 222:9 222:16 223:22 288:21 isolated 264:18
--	---	--	---	---

isps 234:4	258:3 269:8,21	joining 241:12	260:21 262:11	junior 204:17
issuance 274:12	270:8 271:21	jointly 195:16	270:7 271:4	junk 205:22
issue 11:13	286:4 289:1,6	jones 111:20	275:22 276:5	jurisdiction
22:11 42:16	291:2 304:9	112:21 113:15	295:3 296:6	201:5 248:8
43:1 44:15	306:4,8,9	114:1	303:7 304:3	jurisdictional
124:22 125:4	307:7,10,22	judge 3:6,6,8	306:3	11:20
147:12 149:4	308:5	9:1 52:10	judgement	jurisprudence
152:14,15	issuing 181:9	57:16 79:5,10	32:22 42:4	28:13 197:21
158:18 167:7	183:7,8,17	79:15,17	158:5 205:12	198:17,20
168:11 170:9	276:6	104:19 115:4	judges 79:6	288:20
170:22 175:10	ive 24:18 80:8	115:17 124:2,2	127:5,11,12	jury 19:9 20:16
175:16 178:10	96:12 103:4	128:5,6 137:18	148:11 151:8	23:17 41:11,14
178:19 184:18	111:9 115:10	143:8,8,10	159:7 163:12	42:16 43:8
184:19,20	119:18 155:1,5	147:17 149:10	175:5,12	103:7 108:9
187:16,19,20	164:19 171:10	149:11 150:9	178:18 180:10	109:2 303:15
188:18 189:9	179:2,3 197:1	151:14 152:6	181:9,14	303:17,18,22
189:14 199:21	197:2 278:17	152:20,21	182:14 183:15	justice 2:14 3:10
201:4 211:2	279:10 284:3	153:2 154:7,18	183:16 184:4	10:11 26:22
238:8 240:15		154:22 155:2	184:13,13	27:2 30:2 34:3
241:17 244:22		156:15 159:5,5	186:4 188:16	35:12 36:2
257:18 259:20	J	160:11,19	203:3 205:8	50:6,6,7 63:20
267:10,14	james 2:6 3:4,6	161:3,8,11	211:19 212:5	76:22 77:16
268:21 271:4	5:16 143:6,8	162:3 163:10	223:20,21	78:4 127:1
272:22 276:11	jane 3:18 219:14	163:16,20,21	224:15 226:13	129:2 130:3,18
285:12 287:10	261:7 262:7	164:4,8 170:1	275:10,11,15	130:21 139:20
288:7 302:9	janosek 7:3	170:10 171:14	287:18 288:4	140:21 143:7
issued 75:6	january 148:3	176:16 178:22	judicial 47:9,18	146:9 162:17
212:9 224:11	japanese 232:21	179:14 180:6,9	61:11,12	163:3 213:15
303:19	jim 54:3 107:19	180:12,15	123:22 141:17	214:10,18
issues 44:4	147:18,21	181:4,10 182:1	141:22 142:3	217:9 265:6
103:4 129:13	149:10 153:17	182:1,5,12,20	247:2 271:1	justices 13:22
129:18 144:2	166:17 169:4	183:6,8,11,15	274:14,19	260:12 271:19
145:2,3,22	169:13 184:3	183:16,17	276:15	273:7
146:1 153:6	202:7 205:16	184:3 185:1,2	judicially	justification
156:1 158:19	207:4 209:21	188:6,11 189:3	144:11	47:15 111:11
159:16,22	212:22	196:22 197:14	judiciary 3:22	justified 78:17
160:9,18	jims 189:12	197:15 200:20	59:22 61:4	129:7 167:13
172:20 176:9	job 146:14	204:13 205:11	131:21 132:4	274:20
185:7 194:9	168:8 169:20	206:22 208:2	153:22 218:21	justify 158:10
195:1 196:3,13	183:15,16	212:9,15,15,16	219:20 230:14	
196:13,14	206:17 212:2	212:19 216:6	234:3 241:20	K
203:1,2 219:1	214:19,22	224:2,4,5	267:6	k 3:21 219:19
224:16 233:21	215:13 279:11	230:1 237:16	jump 10:3	keenly 253:17
237:11 251:1,7	joined 219:14	257:6,13	164:17	keep 9:12 20:22
	289:7			

21:1 23:14,21 25:19 43:17 63:1 65:8 76:13,18 99:5 136:15 153:19 169:12 175:7 196:20 199:6 201:20 218:21 219:7 227:16 248:16 249:1 264:14 278:20	303:2,6 305:3 307:9 key 12:2 110:15 116:11 188:2,3 keyed 108:16 kick 120:19 kidding 263:15 kids 244:18 killed 39:7 kind 23:10 29:14 32:18 34:8,9,21 46:2 52:12 53:16,21 62:17 74:6,21 84:17 104:3 123:8 124:17 138:15,22 139:4 148:18 161:8 176:8 177:1,6 179:4 179:5 187:19 189:12 195:4 197:8 198:22 199:1 210:21 213:10 217:2 219:1 234:1 241:2 245:14 250:3 266:19 267:14 286:19 288:17 295:15 300:10 kinds 87:11 91:18 105:6 106:6 112:4 144:2 169:19 176:7 197:13 281:14 293:5 knee 118:15 knew 149:19 214:12 253:7 265:3 know 11:18,19 13:10 23:11,13 24:4 31:21	32:7,16 34:11 39:6 41:18 44:1 46:7 52:14 53:8 56:13 57:3,10 57:19 62:11 65:17 67:8 71:1,10 73:17 82:21 83:1 86:12,22 87:21 91:15,17,21 92:3 93:15 94:12 99:18 101:7 103:15 109:8 110:19 112:7 117:6 118:4 119:4 120:20 123:22 127:10 129:3 129:21 131:19 133:18 136:10 137:14 138:11 140:2 146:11 146:21 163:17 164:1 165:10 165:17 167:14 170:2,9,11,11 170:20 176:2 176:15 178:18 178:18 184:12 187:22 189:16 190:11 191:20 192:5,22 193:1 195:21 198:2,5 198:21 201:11 202:19 205:7,8 205:19 212:18 214:17 217:12 221:9 223:10 236:7 244:9,12 247:6,12 250:5 251:13,17,17 251:21 252:4,6 253:2,22 257:9	257:16 259:7 260:3,7,15,17 261:5,8,14,21 263:1,10,11,11 263:13,20 264:19 265:1,1 265:5 266:1,8 266:8,14,22 271:7,9,20,22 273:13 274:2,5 274:6 276:20 278:5 279:11 282:21 283:8 284:17 285:10 286:21 287:8 292:8 294:20 295:2,6,13,18 296:13,18 297:5,8,11,16 302:7 307:7,11 knowing 105:20 knowledge 30:21 47:21 60:10 233:22 264:3 known 17:19 29:3 53:20 54:13 58:10 80:18 83:2,16 262:7 296:10 knows 57:12 155:4 180:9 187:2 202:4 291:22 297:19	82:6 85:9 269:4,9 lapse 225:15 laptop 32:7,9,11 large 59:9 60:12 83:11 87:14 113:13 138:22 155:9 169:7 170:12 192:7 207:3 244:21 261:20,21 270:16 281:17 301:11 largely 155:11 250:18 282:12 larger 104:5 110:10 240:22 late 16:13 220:13 291:5 lateness 236:7 law 3:17 4:6,8 6:13 24:19,21 28:17 50:18 60:3 102:21,22 108:7,8 114:5 121:8 124:1 172:8,13 173:6 174:10 183:12 189:14 204:17 204:18 205:3,9 205:10 208:3 214:22 219:19 220:4,5,15 221:1,5 226:4 226:10,14,16 226:21 227:2 230:9 231:11 231:22 240:12 243:2,20 244:11 245:5 245:12 249:7 251:6 258:22 260:1 262:14 264:12 265:13
---	---	---	--	---

267:2 268:18	leaders 221:20	258:2 269:14	88:10 127:22	limiting 27:14
270:19 273:5	leading 85:8,22	294:5	171:18 214:2,3	71:20
275:3,19	leads 14:21	legalistic 200:4	223:6 230:13	limits 41:11
280:21 281:3	110:6 111:8	legally 111:16	232:3 247:17	67:5 119:16
284:9 292:20	287:10	125:21 130:19	254:14 266:1	147:4 202:16
310:8	leaf 247:4	legislate 242:9	280:7 293:22	306:21
lawful 19:4	leahy 80:10	legislation 290:6	levels 24:19	line 12:21 13:3
57:20 94:4	237:4 295:3	legislative 13:11	130:10 139:18	79:11 92:12,13
132:17 181:5	296:18	37:15 57:3,5	168:17 213:12	256:2 288:21
lawfully 70:6,10	leak 168:7,12,14	57:12 89:1	284:4 293:18	lines 34:4 92:12
70:17 132:16	169:5,11	231:15 245:13	liberties 1:3 5:4	202:10
133:3,6 134:11	leaks 168:2,4	245:18,22	6:11 116:22	links 10:14
135:2,6 178:14	173:19	246:5,6	121:20 122:13	list 76:6 233:2
lawfulness	leaning 55:4	legislature	222:2 223:8	listening 43:22
157:4 173:11	learned 12:3	226:17,18	248:15 267:13	74:20 94:14
laws 214:21	295:2	legitimacy 58:2	277:17	listens 182:20
226:19 243:17	learning 150:17	58:6,21 59:3	liberty 6:11	litens 239:10
264:10 290:8	leave 13:7 32:3	112:18 160:5	221:3 223:14	literally 78:16
291:10 292:3	97:8 162:1	legitimate 115:3	279:8	124:17
lawyer 21:10	196:15 198:16	133:4 159:10	library 266:18	litigate 157:11
32:21 158:1	left 122:22	211:15 290:12	266:19	199:11,20
169:8 193:18	124:15 147:20	length 16:22	license 169:10	295:1
193:21 194:4	205:1 242:13	43:15 48:5	169:15	litigated 294:20
194:11 195:11	242:14,15	96:6,9,10,17	lies 138:8 141:1	litigates 286:5
195:12,19	legal 7:3 23:10	97:9 146:4,10	lifetenured	litigation 23:8
208:20 276:1	28:11 35:12	147:6	127:4	24:22 48:4
lawyers 9:1 24:4	36:18 43:12	lengthy 119:20	light 25:11	86:11 157:15
31:14 34:17,22	47:14 52:2,3	152:21 208:14	158:19 225:22	284:21 286:20
125:17 161:20	59:3 90:15	lenity 226:9,11	likelihood 21:3	287:6,10,11
164:9 172:4	95:18 99:8	226:21 227:15	181:22 189:2	litigations 288:5
175:4,12	111:10 112:15	245:20 272:3,7	limit 70:20	litt 2:19 16:13
192:16 194:8,9	112:17,18	296:22 297:4	80:14 244:15	21:7,9,22
195:5 213:3	115:14 123:11	298:6,14,20	limitation 81:22	46:12 54:1
217:9 239:12	123:12 124:21	299:5,10,12	99:20 134:16	59:17 60:14
262:13 284:19	153:10 155:19	lent 186:20	limitations	64:3 65:2
lay 37:9	185:6 186:6	lesser 46:16	55:17 97:22	67:12 69:21
layer 41:19	187:13,16,20	48:7	98:2 100:12	70:4 73:7,13
lead 48:2,21	196:9 204:14	letter 19:10	101:16 107:5	78:19 81:4
49:4 60:22	204:20 205:1	50:17 68:6	119:18 133:8,9	82:5 86:10,19
87:17 108:12	205:17 206:4	128:11 157:17	limited 83:2	90:11,22 95:14
109:4 111:6	206:13,15,22	295:2	114:14 134:20	98:21 99:18
218:2 245:10	207:10,20	letters 42:8,13	151:20 154:1	101:22 102:14
246:2 255:6	218:6 231:1,16	letting 165:1	156:16 166:5	105:9,12
278:12 297:12	239:9 240:1	level 50:10 72:4	303:17	106:12,15,19

107:2 114:8	55:14 142:10	137:2 179:18	166:6	making 7:4 11:7
117:5,11	168:11 223:12	203:22 221:13	low 79:17	31:14 32:22
119:15 120:8	235:11 237:15	224:5,6 234:2	132:20 148:21	33:12 56:19
120:18 123:6	262:8 285:17	235:14 245:2	lower 127:22	69:5 83:17
124:20 125:7	286:4 293:12	278:2	162:5 238:14	113:8 127:19
130:1,14 137:4	305:15	looks 247:8	256:15 259:18	148:4 159:7
137:11 141:4,8	longer 21:15	296:6	lowly 263:13	165:18 191:8
141:13	23:20,22 24:8	lose 112:16,17	luck 291:21	205:12 221:9
little 16:14	25:5 38:13	137:6 168:8,13	lump 123:3	270:8 305:9
34:16 41:9	39:11 53:1,3	191:22 206:1	lunch 8:20	management
54:4 56:10	82:3 91:20	241:6 279:17	142:13,17	147:10 203:16
64:9 76:1	99:15	losing 169:15	169:13	222:17 223:5
94:18 107:18	look 19:21 32:14	loss 126:11,18	lynne 1:22 310:3	mandate 150:10
131:7 157:9,17	34:19 39:10,11	128:19	310:20	170:2 222:9,16
160:21,22	40:11,13,20	lost 220:20		mandatory
167:4 169:22	41:5 49:18	234:17	M	260:8
183:22 204:19	79:6,10 94:12	lot 13:13 15:4	m 1:18 5:6 309:1	manner 55:22
210:20 230:7	101:1 102:22	20:6 33:14	machines 176:3	101:2 113:21
243:1 256:5	103:3 104:14	35:18 39:14	madrid 39:5	125:21
262:2 268:5	110:7 117:8	44:9 53:16,17	magistrate	manufacturer
294:10	119:22 126:18	65:18 86:2	181:9 183:7,17	244:15
live 218:22	127:17 128:18	87:10 97:2	217:1 274:16	marc 3:9 143:11
261:9	129:9 138:15	112:1,2,4	275:20,22	191:10 195:6
livelihood	151:18 154:3	114:10,11	293:22	285:21 286:7
169:11	154:15 159:19	116:17 127:19	magistrates	marcs 175:21
lively 260:22	160:7 163:12	128:3,22 133:8	205:4	maryland
livingston 1:22	166:11 179:2,3	150:17 157:18	mail 9:18	111:14,17,22
310:3,20	179:21 184:17	167:4 203:2	main 10:14	112:12,22
llc 3:21	203:20 208:16	205:17,20	168:1 300:14	310:4
lobbying 269:8	211:4 213:21	214:1 222:20	maintain 18:20	massive 221:9
local 21:15	222:12 223:14	236:10 244:9	62:15 99:5,14	247:6,6
24:20 116:2	229:16 232:20	245:1 247:12	169:21	material 26:1
located 5:8	233:5 234:8	263:9 265:21	maintained	80:12,13 81:2
133:15 139:17	235:5 242:11	266:9 267:9	214:9	83:14 111:12
location 12:5,5	244:13 273:17	271:12,21	maintaining	165:7
14:18 293:15	looked 92:3,17	278:9 281:16	62:19,20,22	materiality
293:19	109:16 129:14	284:5 293:17	maintenance	81:17
logic 159:20	131:4 216:13	296:13 306:6	281:13	materials 35:14
186:10	222:4	306:15 307:10	major 62:17	60:1 90:17
logical 90:21	looking 31:9	308:5	236:18 285:6	159:3 251:20
93:11	39:15 46:6	lots 15:10 56:13	287:10	253:1
logistics 157:14	50:16 78:16	116:5 141:14	majority 68:12	matter 12:8
long 20:21 33:14	91:8 103:11	196:3	68:17 128:17	29:22 43:12
41:4 43:12	129:15 132:19	love 165:22	148:20 258:1	60:9 66:7

86:11 108:13	260:17 264:10	139:4 228:10	9:5 219:13,16	60:6 98:14,17
109:5 127:17	273:12,13	252:11 266:14	228:4 230:14	98:17 99:5
171:16 184:9	274:15 275:3	mechanisms	243:15 263:12	100:3,18
196:10 240:11	276:18,18	95:2	members 2:1	101:17 102:7
matters 94:2	282:21 283:9	medine 2:3 5:2,3	5:14,15 6:5 8:5	104:22 105:1
244:22	286:19 287:4	5:21 10:2 13:8	9:8,16 58:11	105:20 106:10
mayflower 1:17	288:9,19,22	18:16 20:9	143:19 203:11	111:15 112:2,4
5:7	290:7 291:21	33:1 43:19	216:18 220:6	112:14 113:13
mccarthy 233:1	297:5 301:18	61:9 64:12	227:22 228:14	114:11,15,20
mean 24:5 26:9	302:7 307:1	65:14 69:8	228:14 230:17	115:5 209:20
28:15 31:14	meaning 266:2	71:13 72:19	230:18 231:4	269:16 280:2,8
45:19 51:8,11	305:4,6	95:20 104:19	236:6,14 244:6	280:14 291:3
51:14,20 54:16	meaningful	116:15 117:9	246:12 248:2	304:1
68:3 70:8 76:4	85:10 269:6	117:16 119:4	248:12 250:4	method 111:6
81:19 82:15	meaningfully	120:6 121:9	251:5,6,18	methods 60:19
84:2 85:6	157:11	126:1 132:8	252:6 253:15	61:1 174:6
91:17 93:13	means 21:11	137:17 142:8	253:16,17,20	256:7
99:12 102:14	28:7 51:6	143:1 147:16	253:21 261:6	meticulousness
103:2 104:9,13	85:18 88:16,20	154:18 160:10	264:19 267:1,4	213:22
107:3 113:15	89:3 95:1	166:15 183:19	269:1 290:22	metric 278:5
124:17,18	104:4,4 108:7	190:16 192:11	294:6	280:11
127:20 128:8	109:16 110:3	196:19 202:6	memorandum	metrics 36:6
135:17 137:11	127:10 135:9	209:13 215:14	208:9	250:3 278:1,14
140:10 148:17	135:12,14	216:18 218:13	memos 265:5	mic 103:3
166:22 169:4	158:17 162:22	218:19 219:8	mentality 252:5	microphone
170:2,5 175:9	223:2 232:19	219:11 223:15	mention 38:3	77:9
178:4,22 180:8	245:21 249:5	227:20 231:19	mentioned	microscope
181:8 183:9	250:14 278:8	236:2,6 241:8	23:16 35:7,17	126:21
184:12 187:1	meant 108:8	246:15 254:2	36:13 39:19	mike 253:3
188:20 190:6	161:13 264:20	256:11 257:21	47:20 63:19	mill 82:14
192:15 194:10	measure 58:19	259:11 260:20	79:2 89:11	mind 23:4 25:9
194:22 196:6	75:4 278:6	268:1 269:18	132:3 145:18	54:18 65:9
197:8,8 200:15	281:21,22	277:11 283:13	173:5 196:2	98:22 141:20
201:3 202:4	282:2	290:2 293:8	243:19 255:12	147:7 153:19
203:10 204:16	measured 281:9	294:11 296:2,6	294:13	169:12 174:5
207:3 208:3	281:20	300:7 302:15	mere 102:8	175:7 189:5
210:7 213:5,21	measures 59:1	308:7,10,22	156:9	201:20 218:21
215:7,21,21	79:18	meet 28:9 36:18	message 192:3	219:7 284:5
244:15 251:11	meat 138:7	56:6 84:13	met 29:9 31:7	mindful 167:15
251:13 252:1,4	mechanics	107:10	101:6 104:15	mine 255:3
253:2,10 257:1	139:8	meeting 38:16	215:3,5	minimal 115:20
257:2,17,22	mechanism	142:17	metadata 7:13	116:9
259:2,7,14,19	37:12 64:16	mega 187:16	14:11,14 16:18	minimization
259:22 260:14	76:20 78:3	member 3:19	38:12,13 51:10	12:10 94:8,11

95:15 120:22	38:5 50:17	253:12	127:2 128:3	83:11,18 85:21
133:21 135:15	177:21 220:21	move 21:16	139:21 140:20	89:1,16 92:9
135:20 136:11	229:11	167:2 216:21	146:13 198:13	93:7 102:4
136:22 138:5	missions 6:6	296:18 308:19	205:9 268:10	120:3 123:13
173:13,18	mistake 216:21	moved 21:14	269:14 305:5	125:16,19
211:19 212:2	mistakes 214:14	304:17	305:12 307:16	135:7 140:18
302:4,6 304:9	214:16	movement	nationality 12:4	145:21 151:16
304:10,12,20	mix 124:17	242:1	nationals 67:3	159:19 171:7,9
305:5,7 306:22	mode 55:5 216:8	moving 33:7	67:16	182:17 185:2
307:4	model 83:7	249:1	nations 67:14	215:11 221:11
minimize 12:12	223:20,22	mueller 18:8	232:11,12	222:16 230:16
95:3,3	224:1 225:2	multiagency	natural 38:1	233:5 242:9
minimized	229:20 254:8	140:4	89:12 194:11	243:10 253:19
135:6,9,12	254:14 256:13	multibillion	nature 58:1	268:14 269:17
minimum 37:11	258:4,9,11	146:21	60:15,17 64:7	271:1 275:22
140:3	261:3,17,17	multiple 42:19	110:11 137:21	276:1 277:14
ministerial	292:21	43:3,8,9	236:8	277:16 279:4
224:3	modeled 240:1	139:18 166:11	necessarily 8:5	286:3 288:5
minuscule 88:6	modest 148:4	multipoint 80:1	36:17 78:5	295:14
minute 9:9,10	modification	mundane 25:2	269:9 287:1	needed 221:6
13:20 28:13	128:13	murky 277:7	necessary 59:3	needing 245:9
60:5 99:17	modified 128:9	306:15	59:13 62:14	needs 37:7
116:16 220:8	modify 13:12	muscular 10:16	102:11 103:12	38:17 59:5
minutes 9:20,22	moment 22:22		103:14 104:5	85:20 104:15
122:22 136:15	164:18 184:7	N	107:21,22	142:5 191:20
143:18 153:15	money 281:16	nail 104:20	108:2 110:9	222:17 225:20
178:21 196:21	month 68:7	name 15:4 47:2	118:2 134:7	245:14 246:10
220:13 249:10	months 21:1	47:3 152:13	148:19 151:4	246:13 256:5
296:3	40:1,2 136:18	named 200:9	161:15 162:12	256:18 267:12
miscommunic...	136:18 232:6	222:20	163:20 165:7	268:15
175:3	234:20 297:17	narrow 268:4	182:10 193:8	negatives
misimpression	moot 201:2	299:15	229:21 233:10	235:13 254:5
66:13 97:9	morning 5:2	narrowed 71:20	255:18 262:1	neither 205:3
misinformation	16:12 43:21	193:7	281:10	net 235:19
59:9	62:16 142:10	narrower	necessity 102:9	networking
misleading	144:16 160:14	226:13	102:18,20	43:2
96:22 124:14	172:21 205:21	nation 6:8,14	103:1 107:19	neutral 274:16
misleads 15:17	209:17 218:18	55:8 234:7	108:1,3 142:4	274:17 275:20
misquoting	268:16 279:20	national 2:14,15	212:1	275:22
202:8	295:13 304:16	2:20 10:7,10	need 6:9,10 16:4	never 39:12
missed 265:16	motion 183:12	16:1 19:10,10	28:6 37:3	54:9 68:15
missing 235:13	304:4 305:2	25:9 42:8,12	53:12 56:17	91:17 93:13
mission 14:6	308:22	85:20 94:16	57:1 61:22	100:15 106:4,4
16:10 37:9	motivated	95:6 116:5	71:11 79:21	131:4 138:10

169:4 173:17 202:4 206:22 207:18 208:21 272:21 273:1 294:20 305:10 305:11	nondisclosure 119:11 nonfinal 256:19 nongovernme... 230:18 231:4 231:10 269:3 noninteresting 258:14 nonjudge 276:11 nonsensical 185:18 nonu 29:21 65:18 66:3 67:10 68:19,20 69:6,11 133:14 133:17 139:16 141:6,18 308:1 normal 89:18 normative 227:12 northern 3:7 143:9 notarial 310:16 notary 310:3,21 note 12:8 16:15 63:18 122:9 notice 150:11,11 164:1,7 185:4 215:22 noticed 12:21 87:16 notifications 131:17 notify 61:3 noting 68:6 notion 57:9 105:21 111:3 111:14 126:8 131:11 notwithstandi... 146:12 novel 135:3 148:15 151:21	156:16 159:13 159:16 160:18 174:6 230:6 240:12 258:2 259:4 266:3 268:19 285:15 298:8 300:1 novelty 192:9 november 1:12 5:6 9:18 122:6 nowpublic 35:9 nsa 10:13,17 11:14 12:9,22 13:4 14:17 17:6 18:20 19:7,16 21:2 26:21 27:21 29:22 30:3 36:3,8 37:2 38:4 51:3 56:15 57:19,22 63:22 68:6,10 68:22 70:1,2 79:10 89:8,17 96:13 97:2 109:17,20 121:5,13 122:16 131:22 139:14,19 213:11,18 214:6 262:17 279:21 281:16 nsas 14:2 76:17 131:13 nsl 20:16 23:16 43:1 nsls 19:1 41:12 41:14 42:16 43:8 number 13:10 16:20,21 17:5 17:18 18:6 19:12,13 27:6 29:4,20,21	31:22 32:14,15 34:10 38:20,21 38:21 42:21,22 46:8 47:1,12 48:10,21 49:2 49:2 55:18 62:1,22 67:1 73:19 74:14 75:5,13 87:3 87:14 88:3,3 88:15 95:17 100:2,8 106:1 128:15 144:20 145:4 158:6 162:15,19 169:8 185:9 206:6,7,20 207:16,17 210:3 225:15 232:10 244:7 281:21,22 282:2,15 290:22 301:11 302:8,13 numbers 17:3 19:5,13 27:17 32:12 34:11,12 39:1,10 40:18 40:19 41:3 43:4,5 45:15 45:16 47:2 61:13 73:20 74:17 75:7 83:2 110:14 158:7 249:10 nw 1:17 5:8	objections 161:21 objectives 40:16 obligation 211:10 obligations 289:4,17,22 obscure 255:7 observation 222:15 observe 233:7 obsolete 229:20 obtain 19:5,11 24:22 25:1 40:18,19 41:15 54:13,14 84:5 99:1 148:12 178:14 295:9 obtained 23:16 32:7,14 82:8 103:6 obtaining 99:3 145:11 307:11 obvious 81:8 285:5 286:2 obviously 13:22 14:13 47:6 48:10 55:1,3 58:10 65:4 70:2 77:1 85:10 105:17 110:12,15 112:22 114:4 117:2 119:17 126:21 177:2 178:17 200:10 213:19 238:17 248:13 249:16 265:20 281:5 307:13 occasion 149:9 151:4 208:18 217:13 occasions
--	--	---	--	---

148:17	ohio 3:7 44:1	242:8 243:9	operators 32:4	optimist 247:22
occupies 192:6	143:10	online 9:17	34:5,22	optimistic 273:3
occupy 208:4	oipr 205:18,20	oped 148:2	opine 89:1	option 18:18
occur 132:22	206:14 208:16	152:11	176:13	77:3 164:5
192:8 195:10	okay 10:3 74:8	open 17:17 18:6	opined 198:2	187:22 190:10
231:3	75:17 80:6	18:10 49:14,15	opinion 59:21	254:12
occurred 34:15	92:18 103:8	52:12 55:12	82:15 123:20	options 8:13
152:10 164:12	104:7 105:15	60:10 62:10	123:22 152:21	190:12
168:20 169:3	107:17 111:8	65:3 69:3,14	184:14,17,22	oral 271:19
218:18	135:22 137:19	72:5 123:8,15	185:3,16,18	order 5:18 7:15
occurring 219:5	174:3 179:22	131:12 255:1	186:3,18 188:8	11:14 14:20
occurs 131:9	180:6 196:12	271:18 277:22	188:14 189:6	22:13 27:9
194:6 212:7	197:1 205:4	opened 17:14,14	203:14 214:18	43:16 68:14
230:13	210:16 216:12	38:20	303:8 306:3	77:19,21 78:1
october 5:11	242:18 245:15	openended	opinions 97:17	78:2 83:12
odd 159:20	249:14 260:22	111:3	123:17,19	84:14 85:11
odni 28:1 62:11	264:17 269:18	opening 5:19	129:9,11	95:3 100:5
offense 204:16	296:8 300:20	202:8 236:12	131:21 138:13	102:12 103:10
offensive 252:21	old 40:6,6,7,7	openness 233:10	184:5 185:9,14	103:17 104:5
offer 46:12	111:5 118:2,3	operate 40:16	187:4 293:17	105:5 115:9
98:21 117:12	137:1 176:19	54:12 119:6	293:21 294:3,9	133:17 144:22
193:4 200:2	older 40:8	operated 1:7	opponents	149:5,8,20
222:14	omb 73:8	operates 123:1	199:2	151:16 157:9
office 2:19 3:4	once 24:12	126:16 300:15	opportunity	171:9,17
50:7,15 143:7	54:16 71:9	operating 61:18	33:5 91:14	184:19,19
154:5 162:10	132:18 149:4	62:7,8 64:8	144:4 156:20	200:10,15
162:11 192:7	150:21 152:16	230:11 234:4	163:9 176:22	212:10,10
194:18 195:7	153:2 154:16	operation 53:18	195:11 216:6	228:21 238:13
196:5,8,16	162:4 182:7	77:20 208:1	252:9 295:6	243:19 248:5
213:14,19	184:15 192:13	296:11	oppose 158:9	256:19 257:6
218:1 237:1	215:21 248:14	operational	190:22 191:13	270:21 273:22
250:18	257:11 285:11	13:20 32:20	196:11	orders 26:11
officer 5:13 7:2	286:1,1 287:5	38:17 53:2	opposed 40:2	27:3,20 29:20
7:3 28:17 51:8	oneill 253:3	63:1,6 64:18	51:15 109:1	30:5 35:9 55:2
121:13,20,20	onerous 211:1	75:11 119:17	111:5 180:14	64:15 74:15
122:13 237:8	211:10	141:21 142:4	184:8 192:2	75:5,13,14,15
274:17	ones 33:12 38:7	234:13 262:4	252:12	75:15 82:14
officers 33:12	69:22 73:6,11	operations 8:2	opposing 125:18	84:1,18 85:19
official 73:9	115:12 121:18	126:6 218:14	160:4 192:2	90:17 138:9,21
80:20	122:10 187:12	operative 29:4	289:18	156:4,21
officials 8:15	236:18 275:13	29:11 31:21	opposite 245:10	183:18 233:12
27:4,9 57:22	275:14	operatives 32:11	opposition	257:18 270:4
oh 230:10	ongoing 101:11	operator 31:13	195:21,22	294:16
265:15 293:1	101:20 117:14	33:19	optic 10:19	ordinarily

184:14	153:13 160:20	203:17 204:6	220:6,9 224:21	271:16 272:2
ordinary 84:10	161:1,6 162:11	241:17,19,21	228:8 230:2	274:19 275:18
84:18 104:11	164:15 166:7	242:7,9,12	244:9 308:11	279:2 283:9
127:21 149:15	167:20 170:4	243:22 244:7	panelist 9:20	285:7 290:17
152:6 162:16	175:20 177:5	244:11 245:10	panelists 6:19	293:16 305:4
179:1 184:16	190:18 215:17	245:14 246:2	9:11 10:5	305:14
185:13,13	228:10,19	246:19 247:2,2	142:9 190:17	parte 125:9
266:2	229:7,14	247:5,11,17	241:13,16	157:21 181:1
organization	244:21 261:1	252:7,12,16,18	277:22	181:16 211:20
27:8 32:1	276:13 280:21	252:19,20	panels 8:14 9:7	224:18 270:18
149:2	300:14	253:7 254:1	9:11 228:7	270:21
organizations	outsiders 138:13	258:16 263:8	246:20	partially 291:4
40:15	160:15	268:12 278:9,9	paper 29:13	participant
organized 116:3	outweigh	278:13 281:5	56:12 103:21	201:10
original 198:8	158:12	oversights	107:20 115:18	participate
201:7 203:20	overall 88:3	233:15	210:4 284:15	216:7 274:2
212:16 273:14	208:1	oversimplified	papers 86:12	284:14 287:2
298:5	overbroad	264:11	111:11 157:22	participated
originally	155:20	overwhelm	paragraph	162:5 172:14
225:18 296:10	overcome 181:3	210:10,13,18	12:21 13:2	participating
origins 28:12	overheard 70:12	overwhelming	paragraphs	6:20 42:20
orin 3:16 219:17	70:13	128:17	149:12	216:17
284:10	overlybroad		parameters	participation
orins 289:14	141:3	P	271:10	123:10 186:17
ostensibly 301:4	overreaching	p 309:1	pardon 212:12	186:20 241:3
outcome 49:19	157:2	page 208:11	parentheses	particular 11:20
116:11 238:13	overriding 88:9	pages 185:9,10	260:5	14:11 15:13,14
238:19 239:1	overruling	208:12	part 13:20 37:4	15:16 18:9,11
310:15	301:1	paid 267:1	38:15 42:3,14	19:5,5,11
outcomes	overseas 17:20	painful 215:9	43:10 59:7,8	22:11 29:8
292:15	32:2,8 69:11	panel 2:9 3:1,13	62:5 76:12	31:4 32:1
outdated 176:18	132:14	8:19,21 9:4,9	100:2,9 102:18	47:15 58:5,14
outer 147:4	overseeing 61:7	9:10 10:4,22	107:16 108:16	61:13 62:1,11
202:16	154:10 201:14	11:18 14:13	132:2 144:15	64:1 66:18,21
outlets 230:3	overseen 243:6	16:15 75:3	145:16 147:22	73:10 74:13
outset 146:6	oversight 1:3	126:5,5,14	161:15 174:12	87:11 88:1
outside 3:14	5:4 6:17 27:21	133:19 142:14	176:15 179:1	89:8 97:13
79:3 116:18	33:19 47:20,22	143:18 144:16	185:1,11 189:2	107:5 109:19
136:2,3,5,12	48:5 50:3,20	144:18 160:14	194:22 197:19	115:7,16,22
136:22 138:15	58:8 61:10	161:20 162:16	197:20 198:20	116:8 118:19
138:20 141:8	76:20 131:2,5	162:17 163:10	206:17 209:3,5	118:20 131:22
141:19 144:21	131:8 132:7	166:8 167:21	238:16 242:22	135:8 140:10
148:13 149:15	147:10 202:19	209:19 216:18	252:8 253:13	144:18 160:18
152:1,12	202:20 203:13	218:13 219:12	270:15,16	165:9 166:9

190:15 192:18 196:10 201:1 212:9 233:17 261:15 283:5 particularity 224:6 307:2 particularized 101:14 particularly 38:7 96:1 110:17 173:2 235:10 239:22 247:5 285:11 304:14 parties 156:19 248:13 308:15 310:14 partly 192:16 partners 86:4 96:13,14,15,18 partnership 97:5 parts 53:7 109:21 124:14 parttime 6:4 party 167:19 215:17 234:12 238:4,12 240:6 275:10 286:20 pass 169:18 passed 142:1 214:22 242:22 265:4,14,17 267:16 passionately 223:12 pat 18:22 22:12 23:16 28:17 36:21 42:17 49:8 84:10 87:7 90:2 262:10 patricia 2:5 5:17 patrick 2:17	10:7 patriot 1:8 2:10 7:8 144:8 243:18 266:9 267:16,16 pats 73:3 pattern 253:19 patterns 19:6 211:4 pay 149:12 282:19 paying 291:1 pclob 5:6 6:1,16 7:5 9:15 308:18 pell 3:21 219:19 227:21,22 231:19 246:3 249:16 268:2,4 279:18 290:3 293:8,10 pending 257:8 257:18 pendulum 293:3 people 20:7 24:7 39:7,16 44:9 53:9 61:6 68:22 79:12,12 84:2 88:11 96:4 106:4 115:10 125:20 131:16 132:14 135:4 146:22 160:20 161:17 168:22 169:8 169:18 172:1,2 172:5 179:18 190:3 196:8,16 198:10 199:1 201:8,19 203:8 209:6 211:13 213:22 217:7 221:20 228:20 230:8 232:6,11	233:11 248:10 250:15 252:22 253:12 255:14 261:9,12,13,17 261:21,22 264:22 265:13 266:7 267:9 269:15 291:16 292:17 296:4 296:13 peoples 161:4 261:12 307:12 perceive 113:12 perceived 105:18 279:13 percent 128:11 129:4,4 229:6 percentage 88:4 207:4 215:9 302:1 perception 96:8 96:10,16 131:3 perdue 4:5 220:3 perfect 22:1 perform 132:7 152:13 205:5 performing 212:6 period 23:15,22 24:2,8 29:19 33:14 40:22 72:14 91:16 99:15,15 118:6 118:7 119:11 119:21 120:5 156:7 299:8 periodic 89:20 211:18 periods 22:7 55:17 permissible 86:16 271:11 permit 9:12	110:5 256:19 permitted 17:15 157:22 perpetuating 272:10 perry 238:21 person 12:2,14 13:1,4 27:11 37:9 67:2 69:11,12,16,19 71:21,21 73:20 82:21 95:4 107:14 112:3,5 122:15 132:20 133:11,17,18 134:6 139:16 162:2,4,6 170:6,17 171:7 176:8 179:13 180:4 190:18 192:6,18 200:9 200:13 218:8 256:3 263:12 263:15 285:1 285:15 286:15 286:16,18,22 307:22 308:1 personal 54:2 69:6 205:19 221:1 255:11 288:19 personally 124:10 310:5 personnel 68:10 105:7 247:6 281:12 persons 46:22 65:18,22 66:3 67:10 68:3,4 68:19,20 69:7 69:9 70:11,22 71:8 95:19 121:17 132:13 133:14 136:7	141:6,12,18 165:14 199:19 200:14 239:4 263:4 301:4,10 302:3 307:19 307:20 perspective 15:9 76:17 82:19 88:2 131:13 188:9 193:5 persuade 178:17 245:7,9 persuaded 263:19 persuasive 303:8 304:5 pertain 82:6 146:1 pertains 80:15 philosophical 265:12 phone 18:21 19:5,11,12 32:12,14,15 45:14,16 49:2 61:13 62:1 106:14 110:14 113:4,7,8,8 118:20 176:19 176:19 210:3 249:10 physical 51:16 52:8 113:22 pick 10:3 198:14 picked 44:21 301:5 302:11 302:11 picture 188:8 285:19 297:20 pictures 280:12 piece 118:18,19 152:11 186:9 262:22 284:15 286:14 304:1
--	---	--	--	---

pin 161:2 173:3	277:21,22	198:9 221:17	245:9,17 273:1	potentially
pizza 255:15	278:5,6	228:5 233:6,7	286:7 289:3	54:19 101:10
place 12:12 66:9	plotting 34:14	police 33:11	positioned 13:1	200:15 254:16
67:1,6 72:15	278:21	44:7,10,13,16	positions 73:10	295:17
76:16 79:12	plus 169:15	46:14 47:7	86:13 121:22	power 80:15,16
89:17 92:16	png 177:15	48:2,8 51:8,20	192:13 218:10	80:17,19 165:3
95:7 115:14	point 12:15	79:7 256:7	229:13	225:17,20
121:7 134:11	13:22 14:2,10	policeman 46:19	positive 199:4	257:17 258:15
140:1 173:14	22:12 25:8	policies 6:13	positives 235:15	271:1 303:16
242:6 243:20	29:11 34:7	221:4,13	254:6 283:11	powerpoint
263:3 275:15	35:8 38:10	policy 3:5 66:9	possessed	97:3,14
294:2 298:14	46:5 50:22	115:14 143:7	305:10	powers 67:21
299:5 300:5	51:1,2,17	221:19 235:3	possession	303:17
301:20 310:6	57:16,18 59:4	239:7 243:5	25:13,14	practicable
places 112:5	63:10 66:22	282:7,18	possibility 48:9	187:4
156:13 255:16	74:10 86:19	283:14 285:4	172:9 239:16	practical 18:18
plans 292:4	93:22 97:7	political 232:17	239:21 240:7	61:20 62:2
platforms 87:11	106:7 114:8,22	233:3	possible 7:4,22	63:5 76:2
plausible 194:1	115:3 122:7	politically 217:3	8:10 55:13,17	123:12 124:21
play 118:14	133:2 139:5	politician	58:1 75:9	203:2 287:13
153:13 171:18	146:5,17 150:9	222:18	93:21 94:1	288:6
171:22 173:1	153:9 169:17	poll 291:16	95:3,10 101:13	practically 82:2
187:17 192:7	174:6,7 182:13	polls 56:13,13	111:19 115:15	practice 35:11
201:14 203:5	189:2 198:19	291:17	118:10 122:20	166:1,14
204:15 215:19	203:20 215:16	pool 181:8,14	124:9 172:2	210:11
218:7,9 297:22	218:11 219:8	poorly 227:10	176:5,11 177:9	practices 221:5
308:6	229:22 237:21	popular 252:6	232:16 235:6	221:14 222:12
playbook	240:22 242:14	population	255:4 262:2	235:2
291:14	245:1 250:6	215:10	268:17 275:5	precedent 239:9
playing 171:18	258:8 278:12	popup 145:4	281:3 301:19	259:5
182:14 272:3	279:16 288:10	portion 261:20	306:5,20	precedential
plays 58:22	292:18 293:5	261:21 291:12	308:13	125:4,6
154:9	297:12 299:9	portions 124:5	possibly 293:5	precedents
please 10:22	306:2	pose 8:5 9:8	post 65:12 91:19	195:3
143:16,20	pointed 107:20	156:1	posted 9:15	precepts 296:21
pleased 143:5	115:19 126:10	posed 238:21	308:18	precise 41:3
147:21 219:14	159:5,6 172:21	posit 22:22	postponed	281:3
pleasure 154:16	197:11	285:14	207:8	precisely 38:14
236:7	pointing 112:1	position 8:12	postquery 51:19	267:2
plethora 52:15	191:18	31:8,20 34:5	potential 14:21	precleared
pllc 3:9 143:12	points 11:7 14:3	80:21 90:21	112:2 141:20	150:13 164:9
plot 15:5,13	36:11 38:1	123:7 155:15	157:2 159:17	172:5
39:2,4	62:13 72:2,9	196:9 221:14	169:16 256:12	predicate 76:15
plots 35:19	89:12 194:2	223:21 234:2	269:7 291:10	predicated

126:8	president 3:18	pride 219:7	private 9:3 24:4	272:4 295:17
predict 188:21	7:6 117:7	prima 257:12	24:6,9 25:15	302:9
predictive 90:7	147:8 154:5,6	primarily 14:19	86:3 97:10	problematic
predominant	171:3 178:8,13	17:2 203:14	156:11 164:20	125:22 231:13
84:4	203:15 214:20	primary 6:6	165:6 232:15	problems 73:16
preferable	219:15 233:1	307:20	291:21	74:4 77:5,16
188:10	263:14 291:5	principal 3:21	privileged	206:16 233:14
preliminary	presidents 55:4	219:19 220:15	194:19	236:21 257:10
17:16,22 49:15	167:8	principle 297:6	privy 284:20	272:20 307:8
257:3	presiding 5:12	principles	proactive 29:22	procedural
premise 70:16	152:21	155:19 306:1	75:4,10	284:7 285:2,6
102:10 133:13	press 10:12	prior 228:8	probable 47:18	286:4,9 288:18
premised 75:14	11:13 146:13	248:6 259:1	75:14 134:22	289:1,9
223:19 224:2	230:3 255:1	priority 246:13	148:22 149:2	procedurally
307:1	pressure 157:8	246:14 253:18	184:18 212:1	271:22
prepared 98:8	presumably	287:19,22	224:5	procedure 95:15
143:16	19:1 75:3	288:2	probably 15:6	procedures
preparing	96:14 259:21	prism 164:3	15:17 22:11	12:10 72:14,17
268:21	260:7 289:16	172:18 174:8	41:20 90:10	94:8 106:21
prepatriot 84:7	308:2	181:21 212:10	96:21 97:6	120:22 133:21
prerogative	presume 76:4	privacy 1:3 5:3	98:7 118:15	136:11 138:5
260:17	presumption	6:10 12:2	119:12 122:22	170:12 173:14
prescribe 195:9	82:20	22:21 23:5	140:17 150:14	173:14,18
present 5:14	pretend 178:11	24:11,14 25:6	150:14 176:18	203:22 222:13
73:16 74:4	pretty 137:1,20	25:10 26:7	185:11 192:7	proceed 5:22
81:16 123:10	138:4 204:5	46:22 62:19	244:18 268:12	122:7
125:18 173:22	238:15 253:7	72:10,16 89:4	279:10 280:15	proceeding
205:22 207:19	263:6,19	111:16 112:14	291:16	122:3 181:18
217:14 229:11	prevent 16:2	112:15 113:12	problem 35:4	181:19 198:11
232:3 296:10	20:8 81:12	115:20 116:9	45:20 78:13,15	274:22
297:1 298:12	234:4 292:4	116:22 121:13	87:6 96:22	proceedings 5:1
presentation	preventative	121:20 122:13	129:5 161:11	23:8,9,9
295:7	177:21	123:11 138:18	173:4 174:12	158:17 162:5
presented	prevented 36:21	145:3,22 151:2	175:3,12,13	237:13 240:20
114:19 129:18	282:11	193:3 221:3	179:4,5,6	258:11,12,13
148:14 172:11	preventing	222:2 223:7	193:14 195:1	258:18 284:15
187:6 206:12	16:11 20:6	228:16 230:20	197:15 216:3	289:12
206:22 284:16	prevention	232:13 234:5	230:12 237:20	process 23:10
presenting	82:22	235:2,4,7	238:21 239:16	30:14 31:2,3,4
125:21 217:20	preventive	248:15 252:3	240:21 241:13	33:7 42:16
240:12	197:12	256:10 267:13	251:12,16	49:18 52:7
presently 152:3	previous 246:20	277:16 279:7,8	254:18 255:4	55:19 62:6,6
preserve 63:5	previously	291:20,22	257:15 259:20	66:9,9 85:8,21
85:20	82:11	292:16	261:10 269:12	89:20 92:15

95:10 117:13 118:22 121:16 122:3,8,19 123:9 124:11 124:18 125:11 126:9,16 127:17 130:7 135:21 137:12 137:14 151:7 151:10 155:18 155:22 156:5 156:18 158:7,8 159:18 160:5 161:15 167:3,3 167:5 179:1 182:4,19 183:10,22 198:19 213:6 216:17 218:5 228:5 230:13 231:14,15 235:17 248:5 256:22 267:2 269:12 270:6 270:17,18 272:15 274:19 282:21 283:3 284:7,13 processed 135:16 processing 148:6 produce 282:1 produced 38:21 39:18 productive 49:5 professionalism 130:9 professor 3:16 4:2,6 219:18 219:22 220:3 223:16 227:20 231:20 236:2,4 241:8 246:4	251:10 254:2 256:11 269:22 273:10 274:10 284:11 294:12 296:9 300:9 302:18 professors 228:19 283:16 program 7:8,9 7:10,11,13,17 9:14 11:1,3 13:9,12,13,17 13:20 14:1,4 14:12,14 15:18 15:20 16:11,17 18:7,15,17 19:4,7,16 20:20 21:2,4 22:13,13,19 26:4,10,14,19 27:1 29:12 34:9 35:10,13 36:4,12,13,17 36:22 37:4,13 37:20 38:2,6,8 38:12,14 39:22 44:7 46:15 48:13,13,14 52:13,14,22 53:1,6,11,13 53:16,18 54:8 54:9,19 55:14 56:1,5 57:3,5 57:13 58:5,12 58:22 59:4 60:2,6,11,12 60:15 61:10,12 61:18,19 62:7 62:15 63:6,13 64:7 65:15,16 65:21 66:5 69:10 77:7,21 81:11 82:12 88:17,18,21	90:6 92:17 93:13 97:16 98:19 100:22 101:17 102:7,7 102:11 104:15 105:15 107:21 110:16 111:13 114:7 115:8,16 117:19 126:17 132:12 134:19 134:20 164:3 172:18 261:14 261:18,20 262:5 266:4 277:19,20 278:7,8,9,11 280:2,8,14,15 290:14,17,18 290:19 291:3 292:19 293:2 294:15 296:17 297:13 298:3 298:17 299:2 300:11 302:22 303:11 programmatic 40:13 programs 1:7 7:7 8:1,17 11:2 11:10 26:5 33:8 36:9,10 37:19 38:7 54:11 61:8 89:3,8 90:8,19 94:4 108:20 112:16 116:17 116:20 117:1,4 119:6 121:17 122:16 129:14 144:12 166:12 227:10,13,19 233:19 244:6 261:4 278:3 283:5 290:9	progress 211:18 project 10:16 projection 229:21 promising 225:7 pronounced 197:16 proof 31:7 proper 70:18 142:2 properly 292:6 293:7 property 3:11 143:14 proposal 13:16 65:5 73:18,18 74:6,12 82:19 125:16 148:5 148:10 236:13 237:4 proposals 13:11 56:7 73:3,5,10 73:13 86:7,20 88:15 89:1 120:1 126:7 131:1 167:6 224:20 231:11 238:18 246:20 258:21 284:2 propose 194:7 proposed 101:2 279:16 292:13 296:14 proposes 191:1 proposing 81:12 163:9 201:19 proposition 238:12 prosecute 168:4 169:9 170:16 171:7 prosecuted 169:17 prosecutor 4:1	70:8 163:3 216:8 219:21 268:11 303:21 prosecutors 47:22 prospectively 184:8 protect 6:8,10 6:14 68:20 93:7 191:15,17 234:12 235:7 277:15 protected 25:13 110:13 113:3,9 116:10 291:20 308:3 protecting 69:6 154:13 166:3 281:15 protection 23:19 26:8 66:2 67:15 68:2 121:7 125:12 133:7,16 173:16 283:8 protections 62:19 67:1,5,6 67:10 68:4 69:9 72:10 132:21,22 134:3,11 protects 55:7 prove 168:14,15 provide 7:5 16:19 17:7,21 59:20 63:15 67:14 76:6,19 79:17 85:13,18 102:3 131:17 131:20 165:6 173:15 260:8,9 287:1 302:5 provided 22:14 30:15 39:1
---	---	---	---	--

88:5 250:9,9 264:7 273:21 provider 19:18 19:19,19 20:16 20:16,21 42:21 42:22 43:1 65:16 74:13,14 74:18,19 87:18 157:5,6,22 161:18 164:13 164:13,14 173:17 182:21 199:11 254:13 294:22 providers 7:19 18:20 21:14,16 22:5 42:19,20 43:6,9,14 96:1 96:7,14 99:9 99:14 119:7 138:14 155:9 155:15,16 156:1,3,12,16 156:19 157:10 158:5,20 159:17 199:9 199:16 294:13 294:15 provides 16:18 17:9,10 19:7 19:16 91:13 125:12 170:8 providing 55:21 87:9 96:3 123:17 190:2 280:7 283:3 provision 58:14 58:16 80:3,9 80:21 199:16 245:3 266:18 273:6 295:14 297:11,21 provisional 240:16	provisions 37:16 75:6 136:22 225:14 225:18 227:14 245:20 267:17 proxies 61:6 prudential 199:12,14,21 200:6 public 1:4,16 5:5 7:6 8:13 9:16 11:19 12:16 15:3 38:11 39:14 51:4 53:20 56:14,19 57:8 58:1,11,20,21 59:5,6,10 60:9 60:21 63:21 69:5 85:10 86:22 87:20 88:22 90:16,18 91:10,13 92:7 92:8,9,9,21 93:3,3 94:1 97:8 105:19 115:2 116:18 116:19 117:1,3 118:14 124:9 148:8 156:2 169:2,16 174:7 186:19,20 187:6 193:1 194:17 208:21 218:12 230:21 231:2,17 234:15,16 235:3,17 248:14 265:18 267:10,20 273:4 279:5 280:5,11 281:4 290:10 291:8,9 292:1,6,7	305:11 310:3 310:21 publication 186:21 189:2 publicized 296:12 publicly 14:3 39:1 53:19 64:13 68:9 90:6 122:6 128:10 280:1 291:15 publish 148:3 186:4 published 103:21 187:5,7 207:2 pull 255:14 punt 117:5 pure 173:6 187:20 191:20 purely 26:15 purged 77:18 purpose 7:21 8:8 26:14 45:5 66:16 71:7 82:5 100:18 114:15 133:4 134:15 281:18 290:18 purposes 7:14 24:17,21 26:15 26:16 58:19 66:21 71:3 99:6 107:15 115:8 138:18 149:6 276:5 292:5 pursuant 1:7 7:15 21:19 26:10 27:3,19 29:19 30:5 61:5 66:4,19 73:21 106:20	131:19 239:5 pursue 46:2 61:22 177:14 190:13 276:21 pursuing 295:10 296:1 push 201:17 205:17,20 207:20 268:15 269:17 pushed 243:16 268:16 put 37:9 39:12 41:2 51:2 57:11 105:16 113:19 119:21 121:21 130:15 131:11 132:21 175:9 186:8 209:8 211:20 213:22 222:8 235:2 262:17 302:20 303:7 304:3,7 putting 86:15 113:18 199:15 223:20 225:16 228:3 268:10 299:2	queries 27:4,5 30:10 55:18 68:18 82:7 106:1,12 121:5 query 27:16,18 28:19 29:7 76:15 106:5 107:7,8 118:20 120:11 134:5 134:14 querying 134:1 135:1 question 15:7 18:16 20:20 21:21 25:18 33:10 35:21,22 36:1,2,3,5,8 39:14 49:7,17 52:12 53:7,22 54:6,18 55:11 60:4 63:2 71:13 73:3 81:4 88:19 89:7 90:12 93:11 94:6 95:21 96:21 97:15 98:10,10 98:16 102:2 103:8 104:10 105:17 106:3 107:19 108:15 109:8,9 110:20 111:9 112:11 114:2 116:8,11 117:6,17 120:6 120:9 121:4 122:21 129:22 130:22 136:14 137:20 140:3 163:15 168:18 170:1 171:21 172:8,12 173:6 173:11 175:5 175:15 178:1
---	--	---	--	---

189:18 190:16	198:17,18	169:22 174:5	29:16,18 30:1	294:14
195:18 197:2,3	204:9 206:16	194:5 195:12	30:3,4,7,10,11	readily 187:7
197:6,22	208:15,22	197:6 228:4	30:19 31:3,4	268:8
198:16 199:11	209:10 227:11	230:12 236:21	32:6 33:18,21	reading 97:13
199:22 201:13	236:1,9 239:7	239:7 258:2	34:1,18 35:4	253:8
207:10 208:19	240:1,4,12	259:14 260:12	43:22 44:12	ready 296:7
213:2 215:16	247:9 250:19	307:13	49:9 55:20	real 34:3 154:16
231:14,14	252:21 260:2	raised 13:13	61:14 62:3,4	159:4 168:9
238:10 241:1	270:16 273:8	25:9 63:3,9	63:7,15 64:17	175:12 178:12
242:5,19	287:3,5 296:4	71:17 73:1	65:12 75:21	178:12,19
244:21 245:2	302:16 306:15	117:18 121:12	76:6 77:4,17	211:2 230:19
246:18 247:10	307:14 308:7	133:13 161:11	78:10,16,20	realistic 203:8
252:4,15	quick 49:6	161:17 169:13	79:4,13 97:19	realities 119:17
255:21 258:22	116:16 144:5	180:13 207:10	120:14 133:5	reality 76:2 96:8
259:15 260:12	146:5 171:21	230:2 237:17	134:16,19	realize 17:5,8
260:16 263:21	300:8	238:8 265:11	136:8 139:2	194:14 232:10
264:21 265:11	quickly 17:10	306:9 307:22	209:20 210:2	really 31:11
265:12,22	167:2 212:22	raises 69:22	rate 129:4,5	32:20 51:4
268:5 270:1,14	224:14 268:3	104:12 162:21	130:15 207:22	60:14 70:4
274:7 279:3,4	quintessentially	172:19 178:12	263:4 266:21	91:6 112:3
279:19 283:15	274:14	231:13 236:19	283:1	115:1 119:16
284:9 285:3,4	quite 85:12	237:12	rational 98:16	129:6,8,15
286:6 287:13	101:19 118:18	raj 16:18 33:22	rationale 90:16	138:16 144:6
289:8 290:3	140:16,22	35:6,17 41:22	98:15 99:16	144:14 149:15
295:16 296:1,8	148:10 149:15	48:4 49:7	139:15	152:13 162:22
296:16 298:2	151:7 174:13	50:22 65:11	raw 26:1,12	166:3 187:15
298:21 300:8	177:3 183:12	68:3 69:2,21	reach 153:4	187:18,18
304:8 305:4,21	199:17 215:22	69:21 84:21	164:8 177:4,5	188:18 189:18
305:22	216:1 228:2	94:7 120:20	244:5	190:21 197:1,5
questioning 9:9	251:22 275:7	126:14 127:12	reached 147:3	202:15 204:1
24:16 143:18	quorum 5:15	129:22 279:20	reaches 148:9	214:16,17
160:11 220:8	quote 52:15	rajesh 2:15 10:6	react 156:18	215:22 216:3
questions 8:4	105:7 108:2,21	rajs 59:18	reaction 34:9	224:22 226:1
9:8 20:13 28:5	128:19 151:14	ran 20:13	116:19 139:3	234:6 237:3
33:6 39:20	173:6 185:9	range 8:9 13:12	reactions 161:4	248:12 251:8
53:14 88:14	240:5 301:5	90:19 95:2	read 12:16,17	256:16 261:20
132:9 139:11	quotes 296:15	242:4	13:6 57:8 81:5	265:19 267:6
142:8 147:14		ranged 155:8	111:10 139:12	268:14 269:5
154:15 161:17	R	rapid 34:9 36:19	157:22 158:16	271:7,8 275:14
161:22 165:1	race 193:2	rare 15:13	205:16 207:16	276:16 286:22
176:7 179:2	rachel 2:4 5:15	148:16 182:8	208:10 230:9	287:18 291:19
184:2 190:21	21:22 39:21	rarely 88:2	250:15 253:5,5	293:1 305:9
196:21 197:17	radical 201:20	ras 27:17 28:4,8	254:7 265:7,8	reason 23:7
197:17 198:3,8	raise 38:15 89:3	28:18 29:1,15	266:2 268:9	25:21 29:8

31:19 38:14 42:12 43:10 44:3 45:1,9 46:7 48:21 51:9 67:13 105:17 149:19 175:22 198:12 201:8 247:9 272:21 301:22 reasonable 27:5 28:4 31:15 44:2 56:8 61:14 79:8 89:6 116:12,12 135:4 212:20 reasonableness 307:15 reasonablness 172:21 reasonably 132:13 133:15 139:17 147:4 160:15 202:16 203:9,12 reasons 22:6 48:3 65:11 82:10 93:15 149:6 167:13 167:14 246:8 reauthorization 30:14 240:13 265:5 299:7 reauthorizatio... 89:15 299:21 reauthorize 242:10 reauthorized 26:19 30:8 36:14 37:20 52:1 57:4 58:14 140:9 267:17 recall 122:4 147:20 176:21	187:17 290:20 recast 188:20 receive 155:16 156:5 received 158:7 308:4 receiving 5:21 241:21 287:20 recipient 273:22 274:1 295:4 recipients 295:22 recognize 83:21 111:18 197:4 recognized 284:2 recommendat... 240:16 recommendat... 1:6 7:22 8:9,12 184:2 record 20:18 22:7 23:1 51:5 98:7 100:1 113:6 118:20 126:11,19 128:19 208:20 211:20 219:10 220:18 271:17 310:11 recorded 9:14 207:2 310:10 records 7:11 20:22 21:12,18 22:17 23:3,4,7 23:14,18 26:1 29:14 37:8 40:8 57:8 82:8 83:11 84:5,11 84:12,15 85:12 99:1,2 103:20 145:7,8,12,15 recounting 90:22	recovering 222:18 recur 216:5 red 237:10 redacted 185:18 188:13 redaction 184:6 188:9 redactions 124:13 185:19 redebated 266:22 reduce 255:17 reduced 41:1 reducing 83:16 119:10 redundancy 295:17 reevaluate 37:18 reevaluated 89:9 114:6 reevaluating 38:6 reevaluations 89:20 reexamines 30:1 reference 46:5 96:12 245:1 referenced 156:16 referred 7:10 41:13 94:7 97:17 237:7 referring 50:3 96:13,17 112:20 202:12 202:13 303:2 reflect 129:5 reflection 185:8 reform 59:1 220:15 225:7 228:15 249:20 reforms 52:15	52:15,18 53:9 55:13 296:15 refused 158:13 regard 68:5 95:16 107:2 115:18 236:22 240:19 regarding 8:1 119:5 230:4 regardless 26:6 36:10 37:16 regards 256:9 regime 86:17,17 244:11 register 5:11 173:3 registered 207:2 regular 76:5 84:1,14 105:4 127:4,7,8 128:16 161:13 161:14 201:9 210:22 246:11 248:4 284:21 regularized 40:5 regularly 157:21 207:5 regulate 306:16 regulated 26:5 26:10 52:7 regulation 21:11 21:19 22:5 regulations 6:3 6:13 9:18 20:22 21:10 308:15 reinforcing 221:4 reingold 7:2 reiterate 69:2 reject 227:4 231:11 rejections 207:22	relate 228:5 related 6:14 20:13 66:16 108:6,11 109:3 132:10 160:9 171:22 relatedly 22:2 23:6 relates 21:11 70:10 279:4 relating 60:2 108:13 308:16 relationship 95:22 96:6,9 96:10,17,20 97:10 217:16 217:17 relative 74:17 115:19 282:16 relatively 25:2 162:15 164:11 245:12 295:19 release 188:1 released 55:2 68:8 123:21 124:6 129:10 152:22 relevance 37:7 81:18 84:8 101:2,8,12 102:8,21,22 108:3,16 230:6 relevancy 42:4 relevant 37:4 80:12 83:14,14 84:13 100:4,6 102:17 104:6 109:5 130:14 132:4 237:21 reliable 173:3 reliance 30:14 relied 173:13 relief 77:20 158:9
---	--	--	---	---

reluctant 73:9	252:22 257:19	requests 85:2	197:5 198:4	238:21
rely 92:8 111:13	reported 1:22	101:14 119:9	219:18 220:2	responsibilities
205:11	35:5,5 106:2	120:16 232:8	236:15	154:6 214:19
relying 158:20	reportedly 91:2	258:2,6	resembling	responsibility
remain 231:17	reporting 62:2	require 21:1	237:7	8:16 147:8
remains 112:19	63:10 78:8	23:20 48:17	reservation	153:21 154:12
113:13	89:21 242:3,4	73:14 106:8	101:9,10	203:15 214:8
remarkable	247:4,13,15	271:5 288:5	residents 53:17	288:15 289:19
218:22 219:2	249:16 250:12	302:4	resigned 68:22	responsive
remarks 143:16	252:9,10,17	required 22:4	resolve 45:4	132:1,2
202:8 236:12	reports 38:22	48:18 59:20	207:9 224:16	rest 10:4 127:9
remedial 56:18	39:17 153:1	60:2 61:3 70:7	resolved 44:15	131:11 270:13
77:22 79:18	211:18 241:21	74:12 138:6	44:19 46:3	restore 160:5
remedies 279:15	251:3 252:16	150:4 152:16	resolving 180:14	restricted 119:8
remember	252:20 304:15	175:17	resort 261:12	restrictions 56:4
48:12 78:20	represent 8:6	requirement	resource 38:4	100:12,19
185:8 205:2	150:21,22	20:18 23:1	159:17 228:13	106:11
244:18 291:17	200:14 239:4	69:15 75:21	resourced 203:3	restrictive 104:4
remotely 237:6	representation	80:1 94:11	resources 17:16	restricts 120:15
renaissance	148:19 155:10	137:21 150:1	18:3 65:10	restructured
1:16	165:11 239:10	210:1 246:21	156:17 248:19	225:1
render 240:10	representatio...	275:21 301:14	248:20 253:13	result 15:15
renewal 119:18	289:4	303:19 307:15	respect 6:18	20:5 56:15
182:11 225:17	representations	requirements	55:5,11 67:16	59:7,8 69:1
renewals 89:13	165:17,19	22:4 36:18	70:6 74:5 82:8	120:10 126:21
renewed 211:22	representative	63:11 78:1	85:17 99:8	134:4 148:2
rental 84:12	261:3 262:7	89:21 95:17	107:4 110:18	resulted 17:12
255:15	representatives	123:17 125:8	123:1 125:1	results 97:20
repeat 148:5	233:18 250:21	129:20 135:15	144:14 145:7	106:12 107:7,9
repeatedly	represented	139:15 242:3,4	145:15 147:2	255:6,7
41:19 42:17	158:1 159:15	247:4 249:6,17	231:15 241:20	resume 142:14
55:12 279:10	representing 9:3	302:5,6 305:18	283:19	218:16
repeating 83:4	195:17 239:2	307:2	respecting	resumes 122:4
repetition	represents 77:1	requires 47:14	191:17	retain 43:15
200:21	127:2 229:12	47:17 99:1	respond 9:6	70:21 164:8
report 7:6 8:18	repression	135:19 157:18	17:10 77:19	218:8
26:22 51:22	67:22	226:15 266:15	155:6 158:15	retained 21:19
63:11 64:16	request 100:15	274:16 277:13	168:17	23:7 40:21
75:5,12 77:17	100:17 119:11	282:10 303:16	response 13:16	43:13 305:15
122:1 131:3	122:4 156:15	requiring	36:20 39:20	retains 13:4
152:17 236:15	164:15 196:1	119:19 252:22	73:3 120:8	retention 12:13
236:19,20	258:5	requisite 17:21	170:1 243:11	20:18 22:4,7
237:12 238:8	requested	research 3:16	243:12	23:1 55:16
240:16 250:14	266:11,11	4:4 112:1	responses 9:12	67:4 72:14

94:9 95:12 118:6,7 retroactively 15:22 retrospective 257:14 retrospectively 184:9 return 75:20 79:22 182:5 246:21 290:2 returned 80:3 returning 197:3 revalidate 37:13 reveal 117:20 revealed 53:3 128:10 revelation 52:13 revelations 25:11 56:15 221:22 reverified 30:16 30:18 reverse 133:18 257:4 reversed 152:7 152:8 review 3:5 6:7 34:1 40:14 47:9,9 49:8,9 49:18 55:20 62:4,6 63:16 64:1,6 65:12 78:10 79:6 95:18 97:1,3,3 128:4,21 129:12 130:2 138:20 139:21 140:4 143:7 151:17 152:3,4 156:6 157:4 163:10,11,14 164:21 172:7 183:10 186:1,1	187:15 199:7 200:22 202:1 204:2,3 205:15 206:12,21 211:19 213:12 213:13,14,16 213:19,21 224:7 228:10 240:18 256:13 256:22 257:8 257:14 258:19 259:12,16 260:5,8,9 261:7 263:7 264:3,6 266:15 270:1,7 273:2 reviewed 50:11 63:20 66:4 140:20,21 144:11 151:16 243:5 256:16 reviewing 34:18 50:21 137:12 252:22 reviews 35:6 50:8 162:11 215:18 224:4 revisited 242:20 revolution 91:3 right 15:7 32:2 34:11 35:20 36:1 46:5 77:15 79:11 85:7 92:12 101:7 105:8 107:11 109:14 117:12 121:9 132:21 134:13 135:22 136:9 138:16 156:22 158:2,6 161:20 162:8 166:1 174:15 180:19 185:15,19	186:18 190:9 192:19,21 207:12 215:2 217:8 219:11 221:7,15 240:4 240:19 241:12 242:6,7,13,14 248:10,13,21 251:12 252:19 253:12,12 257:4 258:10 260:4,6,6 261:17 263:10 263:11,15,22 264:1,14 272:8 273:21 274:2 275:12,16 276:18,19,21 278:7 283:2,11 284:14 285:17 286:15,16 287:5,7,17 288:11,13,16 289:7 296:2 297:2,4,8 301:6 righting 233:15 rights 65:22 69:17 151:1 199:10,19 234:6 284:7 285:2,6 286:4 286:9,19,21 289:9 307:18 rigor 12:18 13:6 126:10 127:16 127:19 rigorous 52:7 89:9 128:20 131:12 rigorously 206:18 ripeness 271:2 risk 50:16 55:9	91:9 169:15,16 254:5 262:2 risks 91:9 124:12 265:20 robert 2:19 robertson 159:6 robust 223:7 243:3,22 267:13 307:4 rogers 125:10 role 6:17 57:21 62:10 121:17 121:22 132:5 152:14 153:10 153:13,15 154:9 180:13 180:17 181:1 181:14,15 183:3 190:17 192:7 201:14 203:5 204:15 204:20 205:4 208:4 215:18 215:18 216:16 218:5,5 244:2 244:7 271:16 272:3 279:6 285:7 297:22 roles 182:14 218:10 rookie 176:16 room 289:16 rotating 127:10 127:13 rotation 182:6 round 28:6 71:14 88:15 94:7 104:17 116:16 117:18 137:18 196:20 204:9 220:8 rounds 9:10,10 143:18 routine 149:16	156:15 258:1 routinely 41:21 50:8 239:13 rub 269:16 rubber 129:8 rug 252:13 rule 48:16 64:11 70:16 133:3 150:11 163:22 164:6 171:10 205:14,14 226:9,11,21 227:15 239:11 245:20 272:2,7 272:11 296:22 297:3 298:6,14 298:20 299:5,9 299:12 ruled 199:9 233:4 rules 12:12 27:20 68:20,21 69:5 70:20,22 104:12 105:13 105:14 106:22 136:13 150:3,4 157:13 rulings 157:19 188:2 run 22:13 41:4 46:15 82:14 97:18 161:21 running 46:22 174:10 257:14 307:3,6
S				
s 3:6 12:1,14 13:1,4 27:11 29:20,21 32:15 65:18,22 66:1 66:3 67:2,10 68:2,19,20 69:6,9,11,12				

69:16,18 70:22	202:1 227:1	132:19 136:7	297:10 298:17	210:12,17
71:8 73:19	250:14 296:17	searches 97:18	301:3 302:20	211:4,9 215:9
95:4,19 107:13	scale 301:9	292:14	303:3,12,20	225:19 230:10
111:20 132:19	302:14	searching 69:15	306:4	241:19 242:1
133:10,14,17	schedule 89:10	98:1 255:18	sections 186:6	251:14 258:8
133:18 134:5	scheme 64:9	281:13	266:12	284:15 294:9
136:6,6 139:16	scholar 231:21	seating 154:21	sector 9:3 24:9	seeing 75:8
141:6,12,18	275:4	second 8:21	25:15 86:3	93:19 173:21
165:14 199:18	scholars 12:3	19:14 21:16	291:22 292:1	274:11
235:3 239:4	scholarship 4:7	41:15,18 45:2	secure 57:2	seek 25:1 80:14
260:1 263:3	220:4	45:7 47:4 54:6	152:2 161:5	123:9 225:17
277:15 282:16	school 3:17	76:12 149:5	163:13 292:2	226:3 227:9
301:4,10 302:3	219:19 262:15	158:4 234:21	secured 161:20	228:10 276:22
307:19,20,22	264:12	237:11 275:4	security 2:14,15	seeking 83:2
308:1	science 4:2	300:6	4:4 10:7,11	117:9 126:16
safe 17:19	219:22	secondguessing	16:1 19:10,10	158:5 180:18
264:15	scoop 103:10	279:15	25:9 42:8,12	seeks 191:13
safeguard 234:5	scope 13:14	secondly 44:13	85:20 94:16	seen 22:7 96:12
safeguarding	71:18 280:21	66:15 151:13	95:6 127:2	112:20 113:14
256:8	307:2	191:2 229:22	128:3 132:6	116:18 119:18
safeguards	scrap 200:18	secrecy 53:13	162:20 168:13	126:8 173:20
174:2 263:7,17	scratched	54:7 59:8	169:19 176:9	229:9 234:19
264:14 283:7	303:12	120:3 155:20	191:20 198:13	241:18 255:1
292:12 293:6	scratcher 238:9	156:12 158:20	205:9 220:2	255:11,12
safety 234:12	scrubbed 232:8	198:13	221:3,3 223:14	280:6 282:14
salute 262:11	scrutinize	secret 52:13,22	262:3 265:20	segments 105:19
sanction 170:17	129:16	53:3 54:10	265:21 268:11	segregate
santa 157:17	scrutiny 25:7	81:9 93:7	269:14 279:8	104:10
satisfied 274:7	266:20	158:10 163:4	305:5,12	segregated
satisfy 166:2	seal 310:16	172:12 173:6	307:16	26:12
saw 268:16	seam 14:6	217:4 265:13	sedition 232:21	seize 103:14
saying 35:18	search 46:7 52:8	267:2 290:6	see 19:6 20:9	seized 70:14
83:14 92:4	69:18 71:12	secretly 10:13	32:15 34:12	seizure 116:13
99:19 137:9	108:17,20	secrets 221:8	38:8 43:1	selection 61:13
149:22 169:4	109:17 116:13	section 1:8,9	50:12 58:22	264:20
200:16 201:9	125:14 133:1,3	2:10,11 3:11	61:1 91:18	selective 96:22
201:21 229:8	149:7 181:9	7:7 71:5 75:15	96:19 101:19	selector 30:7
252:2 280:19	183:7 184:16	75:16 80:1	117:14 129:11	31:5 45:10
288:11 299:20	208:11 223:20	85:6,17 88:17	153:8 155:17	78:16 210:3,5
sayings 104:1	223:21 224:1,4	90:6 98:22	158:13 159:21	210:19
says 12:22 13:3	224:19 254:14	143:14 144:7,7	173:17 175:22	selectorbased
68:3 73:19	270:17 274:12	156:22 157:4	176:4,10,10	140:15
91:20 92:4	276:6,8,12	199:16 202:14	177:4 183:5,13	selectors 61:16
151:14 200:20	searched 98:1	202:15 254:9	188:7 199:17	75:21 76:6

78:21 97:19 210:2 sell 253:14,16 295:19,21 semiannual 131:3 seminar 195:4 senate 130:11 131:14 132:7 218:20 senator 68:7 send 260:13 sending 131:16 senior 3:6 27:4 57:22 143:8 sense 24:6 51:5 52:2 71:10 81:15 82:20 94:18 117:6 171:17 178:1 186:9 190:11 201:7 204:16 206:10 213:20 217:19 242:14 287:16 sensenbrenner 237:5 sensitive 55:8 61:7 117:14 sensitivity 157:8 sent 68:7 265:6 separate 59:2,10 102:19 124:4 242:8 separated 239:10 separately 58:18 121:21 september 5:11 sequential 41:14 41:14 182:9 sequitur 237:2 series 28:5 serious 36:3	52:19 153:7 201:12 seriously 124:7 215:11 serve 67:6 159:17 204:21 226:22 271:15 served 74:15 122:19 156:3 184:13 233:12 247:22 server 304:17 304:18 service 7:19 19:18,18,19 20:21 65:16 74:13,18,19 96:1,7,14 99:9 99:13 155:16 198:4 236:15 262:11 services 88:4 96:3,3 132:3 148:13 serving 224:2 session 142:11 143:2 set 29:19 61:3 64:10 101:16 104:9,10,11 121:3 124:1 125:11 203:6,7 206:6 235:1 237:1 259:5 261:6 305:13 310:6 setting 72:6 79:11,16,22 94:19 135:18 137:4,5,10 140:18 144:3 147:5 170:13 189:9 277:6 281:19 287:8	305:7,8,12 306:18 307:17 setup 58:7 seven 27:9 178:21 205:14 seventeen 248:1 shaken 59:7 shame 169:16 share 6:21 197:15 289:14 shared 113:4 239:15 sharon 6:22 sharp 273:14 sharply 251:22 shift 65:14 87:17 shining 54:4 shocked 221:21 short 99:14 192:20 236:12 253:15,16 shortcoming 294:18 shorter 40:21 55:16 72:14 shortterm 138:3 shot 199:5 shouldnt 176:11 202:17 218:9 229:4,8 234:18 241:1 263:22 show 104:3 179:12 207:21 showed 291:17 showing 37:7 84:14 100:2,6 149:3 257:12 shown 138:3,10 176:17 shows 128:19 shut 13:17 82:12 side 9:2 16:1 19:11 24:15	87:19 133:1 154:22 155:1 158:18 159:12 159:14 191:19 210:21 262:18 272:17,18 283:12 304:21 sides 159:8 171:11 sign 91:20 274:18 significance 17:5,8 significant 27:13 29:7 35:12 38:4 59:20 85:12 115:21 128:13 129:13 131:20 167:9 170:22 175:13 202:22 258:22 259:1 272:3 285:12 285:16 signing 130:12 silicon 10:21 silverman 237:16 similar 39:5 90:7 212:6 213:18 226:22 254:15 288:17 306:17 simple 191:16 208:2 216:1 simply 11:16 13:17 21:5 30:14 46:22 56:8 126:18 148:10,21 177:6 179:12 188:20 224:13 239:17 277:20 single 28:18	34:18 39:7 44:11 97:4 127:16 139:22 140:5 162:11 253:5,6 258:5 284:14,15 sit 208:10 site 14:18 308:18 sits 189:15 sitting 32:21 127:9 149:10 248:10 situated 126:15 situation 15:14 32:13 39:22 114:18 136:1 150:4,5 168:15 171:5 177:17 178:3 182:10 183:10 194:2 194:12 198:7 200:21 230:22 242:10 272:9 298:12 299:1 situations 112:14 six 68:8 147:19 size 263:10,11 263:16,17 sized 278:8 skeptical 271:14 skiff 251:19 skin 168:8 skp 3:21 219:20 sliced 174:13 slightly 277:13 slower 20:1 42:15 small 106:2 130:6 150:13 155:8 162:15 162:19 164:9 165:22 168:22
--	---	---	--	---

180:3 194:17 194:17 195:15 232:15 282:16 smart 248:10 253:8 smith 111:14,17 111:22 112:12 112:22 113:3,5 113:15 173:2 snap 123:20 snowden 25:22 222:20 socalled 97:21 130:15 138:8 266:17 solicitor 165:10 solutions 254:17 solve 198:15 241:5 257:10 259:21 solving 15:22 somebody 28:18 46:8 79:1 91:19 92:22 153:5 161:19 165:1 171:2 172:20 173:4 191:18 216:21 223:4 264:2 267:5 276:2,4 284:12 somebodys 70:14 somewhat 247:3 271:14 276:12 soon 91:4,6 121:15 292:22 sorry 11:5 16:13 21:22 42:9 59:16 109:7 135:11 189:19 197:2 sort 22:3,5,18 28:12,22 49:9	49:18,20,22 52:21 55:6,19 62:17 74:3 76:18 79:3 81:22 82:4,14 85:16,20 89:9 95:15 96:2 98:10 99:21 101:20 125:3 125:15 132:20 136:11 150:5 150:15 153:2 153:17 164:5 168:22 171:14 172:4 182:3 183:1,3 187:8 188:3 190:12 190:21 193:2,2 195:16 197:11 202:18 204:3 225:19 239:9 240:11,21 246:3 252:13 257:4,10 258:14 259:2,9 259:9,10,22 268:10 271:3 271:20 272:17 273:5 274:20 276:14 283:10 283:10 284:5 287:3,7 288:17 288:18 292:15 299:2,5,15,22 301:13 303:15 304:19 305:17 307:5 sorts 38:7 70:9 125:7 sought 23:8 293:18 sound 57:11 218:6 304:21 sounds 75:22	source 194:11 sources 60:19 60:22 spafford 4:2 219:22 231:20 231:21 236:3 250:11 254:2 254:19 281:8 speak 12:19 13:19 22:10,20 36:9 46:1 57:15 66:7 70:1 89:5 98:8 102:15 131:1 131:13 168:19 176:1 193:6 205:5 210:10 300:11,18 speaking 47:21 71:2 72:3 74:5 123:6 124:9 140:16 209:9 special 104:12 124:19,21 125:1 149:12 159:1 160:8 166:6 172:1 180:1 225:3 236:11,17,21 237:6,21 238:10,18 239:2 244:2,3 285:8,13 286:13 287:15 287:20 295:15 specific 27:7 33:6,13 44:2 44:22 45:8 57:3,4,11 72:12 74:5,11 100:2 114:14 119:22 140:16 140:17,22 242:3,4 254:20	254:20 268:5 277:14 278:2 289:4 294:16 298:11 300:2 specifically 101:18 161:10 168:18 271:15 290:20 302:13 specificity 74:22 specifics 40:11 156:6 spectrum 39:15 speculation 277:10 speed 167:1 spend 150:17 251:19 spending 282:8 282:8 spent 223:4 281:16 282:3 spike 87:15 spinning 115:11 sponsors 81:9 spouse 25:3 spreadsheet 210:19 square 256:17 squarely 64:22 staff 190:19 203:11 228:4 228:13 230:14 230:17 231:3 233:20 246:11 248:8 250:4,19 251:3,8 268:22 308:12 staffing 253:19 stage 95:10 135:20 stake 116:6 157:8 199:10 238:13,19,22 239:17 267:21	288:19 stakeholders 230:18 269:3 294:8 stamp 129:9 stand 61:6 136:20 137:2 288:20 standard 28:5 28:10,11,16 29:6 33:18,21 37:5,6 44:6 48:10,18 51:6 51:18 52:3,3,4 52:5 79:4,13 79:16,17 80:10 83:13 84:6,7,9 100:10 101:5 101:15 102:13 107:15 128:20 133:5 134:19 134:22 135:1,8 138:4 148:22 209:20 215:3,5 242:2 262:13 standards 31:7 48:11 109:14 120:12 127:5 standing 125:1 165:2 198:6 199:8,12,13,14 199:16,20 200:6 264:7 288:13 standpoint 72:4 271:8 276:13 286:10 start 11:4 14:12 43:7 66:6 87:6 90:22 98:13 133:12 139:7 142:5 143:2 160:11 191:10 218:1 220:11
--	---	--	--	--

262:20 293:4 started 9:21 10:1,2 16:16 35:18 70:8 204:22 starting 196:21 219:12 250:6 starts 87:9 stasi 67:20 state 24:20 73:9 310:4 statement 220:7 279:22 statements 118:14 states 32:17 34:12 45:17 46:9 48:22 49:5 67:14 69:13 91:21 105:2 132:15 136:3,4,5 137:1 141:9,19 143:9 144:21 181:10 203:16 215:10 222:3 223:4 237:8 304:2 status 50:12 296:10 297:1 statute 11:19 59:19 85:4 101:15,18 102:3,10 129:20 131:19 135:19 223:19 224:8,9 226:13 227:7 230:9,11 231:7 240:3 268:6,9 277:13 288:2 294:14 294:18 299:4 299:16 303:9 303:14 304:6	307:21 statutes 102:1 229:19 230:19 231:16 273:22 293:14 statutorily 144:10 178:15 statutory 64:10 64:11 86:17 100:9 101:5 138:2 156:20 191:5 192:15 193:9,13 196:13 197:17 198:18 stay 246:6,11,12 stenographica... 310:10 step 70:5 141:9 141:17 226:7 272:20 stephanie 3:21 219:19 247:20 249:15 262:8 stephen 4:6 220:3 steps 54:15 75:10 77:22 95:9,9 116:21 118:22 stevenson 3:16 219:17 stick 93:5 stood 165:11 stop 28:10,12,16 31:16 36:15 44:7,13 45:5,6 46:14,19 47:8 48:8 51:6,7,9 51:12,15,18 52:4 79:9,20 235:18 240:22 296:17 stopped 15:15	38:20 44:18 94:13 stopping 46:20 stops 44:12 48:2 79:7 storage 281:10 305:1 store 97:18,21 98:5 120:9 stored 235:11 304:11,16,22 304:22 305:1 stores 255:15 stories 117:21 story 91:1 144:15 145:16 171:11 straight 206:2 288:21 straightforward 149:16 216:1 strategic 191:8 strategies 3:21 219:20 strategize 192:16,16 strategy 261:15 streams 14:8,9 14:22 43:6 street 28:18 31:13,17 33:12 33:20 46:20 49:21 50:10 stress 232:17 strict 199:22 strictly 100:9 strictures 271:5 strike 138:16 strikes 178:2 274:14 305:6 305:21 stringent 105:14 106:9 107:6 strong 116:19	287:16 stronger 160:21 strongest 273:15 struck 306:6 structural 237:14 structure 202:3 203:20 264:5 270:11 304:20 structured 98:20 159:9 270:12 struggle 156:17 student 264:13 studied 231:22 studies 114:10 study 40:10 118:8 stuff 186:5,11 210:21 222:19 222:20 248:9 266:21 267:9 293:5 stunned 222:4 subissues 287:11 288:6 subject 8:18 11:2 13:9 20:14 56:2 61:10 65:19 67:6 70:11 84:20 97:21 105:3,12,13,22 106:5 108:13 109:5 120:21 125:13 184:1 264:3,13 266:19 300:22 305:18 subjects 19:6 67:3 submit 37:1 145:1 147:3 210:1,22	308:15 submits 157:21 submitted 9:17 66:20 128:12 206:21 subpoena 19:9 20:16 23:17 24:5 82:4 103:7 303:15 303:17,18,22 subpoenaed 24:4 subpoenas 41:11,14 42:16 43:8 subquestions 284:6 subscriber 14:17 115:9 subscribers 87:5 87:21 88:3,4 subsequent 47:8 118:22 181:22 257:13 274:22 substantial 74:2 151:8 214:1 substantially 206:7 subverted 233:8 subway 39:3 success 117:21 282:6 283:1 successes 281:22 successful 194:1 sudden 87:13,15 sue 7:1 suffer 170:17 suffered 288:12 sufficed 118:3 sufficient 79:8 173:15 174:2 250:12 257:6 261:2 288:13 sufficiently 29:9
--	---	---	---	--

260:11	sunsetting 246:9	85:13 86:15	256:14,18,20	table 154:22
suggest 11:11	super 146:19	90:11 92:11	256:21 268:8	171:19
15:12 59:6	202:18	104:13,14,21	270:5 283:5	tailored 101:18
135:3 201:18	supersede	129:16 131:10	299:14 306:10	255:19
201:19 225:10	106:21	150:7 163:16	surveilled 65:22	take 9:20,22
234:8 288:20	superimpose	166:20 171:10	susceptible 83:9	23:11 25:19
suggested 18:18	278:16	173:5 174:12	suspect 236:14	54:1,15,22
52:15,16,18	supervision	195:6 200:5	239:18	69:20 70:5
53:9 56:21	7:20	205:17 214:8	suspected 17:19	74:7 75:10
112:13 124:19	supervisors	215:2 216:3	31:17 80:16,18	77:21 88:6
138:19 199:1	50:12 51:12	218:19 221:14	suspend 77:20	91:15 95:8,9
226:9 275:21	support 30:20	222:9 233:8	77:21	97:7 98:6
299:19	79:9 119:10	235:18 257:1	suspicion 27:6	101:16 112:12
suggesting	123:5 124:17	279:4,11	28:4 31:16,22	114:11 119:12
56:14 96:20	supporting	287:19 288:4	45:3 61:15	119:16 124:7
112:9 160:21	269:8	300:10 305:9	79:9 212:21	142:13 169:10
194:16 302:22	supports 279:5	surmised 160:13	swallows 64:11	192:13 196:10
suggestion 31:1	suppose 185:2	surprise 229:4	swing 232:17	196:18 199:5
31:9 138:6	212:18 272:14	surprising	swiss 186:9	201:21 204:12
276:3	287:4	229:9	switch 183:21	207:13 214:21
suggests 152:22	supposed 244:3	surrounded	sworn 310:7	215:11 218:16
236:20 276:14	suppression	133:7	syllogism 93:11	219:7 232:9
sum 279:8	181:12 183:12	surrounding	system 21:14	246:3 248:19
summaries	216:9	133:9	34:9 39:3 42:5	270:9 279:16
188:7	supreme 23:19	surveillance 1:7	106:5 155:19	287:19 294:10
summarize	111:22 112:21	1:10 2:11 3:2	159:9 168:6	306:11,13
62:17	163:13 202:2,2	7:16,20 8:3,17	190:4 194:7	taken 59:1,5
summarized	237:7 238:11	8:22 11:16	210:9 215:7	75:11 116:21
294:4	240:2,4 259:13	14:5 26:21	233:8 235:12	222:20 277:14
summary 188:1	259:14,16,20	58:13 65:19	238:15,17	takes 6:8 140:1
188:7,10,13	260:3,13,14,15	85:4,5 88:12	239:9 240:19	149:14 276:12
189:13 190:5	264:4,6 270:9	96:15 117:4	261:6 263:5,9	talk 22:2 35:19
summer 122:2	271:15,17	134:2 140:13	272:10 276:14	48:20 79:21
152:22 238:11	272:13,16,20	142:15 143:4	systematic 36:4	103:22 126:15
sunset 131:5	273:1,8 274:4	144:11,19	40:4 47:22	126:15 131:7
225:13,17	274:13 275:19	146:7 150:3	48:5	146:3 147:11
226:5 227:14	282:22 288:9	153:3 154:2	systems 41:22	153:10,15
242:10 245:3	288:20	163:11 181:18	50:20 231:22	164:22 167:22
245:20 266:14	sure 21:8 23:13	182:16 191:21	231:22 232:4	172:1,2 175:16
273:6 296:21	25:16 35:1	193:7 205:7	232:14 233:2	183:2 194:9,14
297:21 299:8	36:9 57:17,20	218:15 219:3	234:22 254:21	194:18 204:14
sunseted 266:13	58:10 62:7	225:8 226:10		204:19 213:4,9
sunsets 37:15	66:12 77:10	226:21 227:19	T	223:1 231:8
297:10	81:5,14,20	230:9 239:6	t 190:8	233:13 262:22

280:10 290:9	tasked 252:7	14:11,14,15	270:10 271:10	147:15,16
290:15,16,17	tasking 138:8,21	17:3 18:19	302:21	152:8 154:17
290:18 294:6	294:16	29:4 37:8	terrorism 6:8,15	154:18,20,21
talked 55:16,17	teaching 262:14	46:22 47:2,12	40:15 82:22	160:10,13
55:19,21 64:4	tech 155:9	51:10 73:20	92:6 116:1,4	166:15 174:3
112:21 174:15	technical 27:13	99:4 105:1,20	277:16	183:19 209:2
256:12 285:22	27:16 94:20	111:14 145:7,7	terrorist 16:2,11	209:13,15
talking 33:10	95:1 129:17	175:10 291:3	17:19 27:7	218:13 219:9
74:11 78:21	174:18,18	telephony 98:16	32:1,8,10,11	223:15,17
83:9 84:10,22	187:12,19	100:18 101:17	34:14 45:11	227:19,20,22
94:21 105:9	223:10 228:10	102:7 280:8,13	46:9 149:2	231:18,19
116:2,3,4	234:22 251:1	304:1	201:10 235:18	236:1,2,5
130:11 141:5	262:18	tell 73:19 79:21	261:22 262:22	241:7,8,11
145:12,13	technicalities	91:4,6 121:14	280:12 282:15	246:14,15,17
153:19 166:19	99:19	127:15 180:11	terrorists 45:14	249:14 256:11
169:7 175:21	technique	189:7 215:4	49:2 125:12	260:20 283:14
177:7,17,19	149:13 151:21	227:4 246:22	234:1,3,4	290:1 294:11
184:8 186:13	technological	298:10	terry 28:10,12	308:8,8 309:1
195:16 197:7	108:4,17,19,22	telling 273:20	44:1,22 45:2	thanks 43:21
262:16 274:8	109:16 110:22	tells 127:12	46:4,14,19	69:21 95:21
275:20 281:7	174:16 175:16	269:15	47:7 48:2,8	104:18 174:3
talks 85:5	179:5 243:17	template 101:3	51:6 52:4 79:7	183:21 196:19
286:17	254:17 258:3	195:10	test 104:4	215:14 269:19
tangible 99:21	301:8	ten 9:9 145:8,10	107:10	296:2 308:10
tank 221:20	technologically	249:10 277:21	tested 157:14	thats 15:6 16:2
tap 212:1	176:20	296:3	202:5,5	20:19 22:1
target 69:10	technologies	tend 62:16	testified 237:16	23:21 24:3,3
71:15,16 85:3	175:2 225:9	271:14	testify 223:18	24:10 25:17
94:15 133:14	226:1	tent 54:3	228:1 268:21	28:16 32:8,13
133:17,18	technologists	term 97:5 183:4	testifying 222:4	32:18,19,20
139:16 140:11	175:4,11	terms 11:9	testimony 118:5	33:13 34:5,14
200:9	technology	15:17 22:3	223:10 281:6	35:20 37:17
targeted 84:5,15	109:10 111:4	27:18 37:10	285:22 310:11	38:13 39:3
targeting 71:20	113:11 174:10	40:13 48:9	testing 225:19	42:9 43:9 44:6
138:3,17 139:8	224:13,13	59:18 72:9	thank 6:19,22	47:1 48:3,18
139:15 140:1,5	227:17 228:22	76:12 85:1	20:11 21:20	48:22 56:22
140:8,9,15,19	229:1,12,17	98:1 103:22	33:1,3,4 43:19	60:7,19 64:10
141:2,6,18	244:9 249:3,22	115:7 118:16	52:9,11 54:4	65:2,6 68:1
142:6 173:13	250:13 251:8	121:5 123:2,16	72:19,21 77:13	70:4,17 71:21
173:18 301:6	264:2 278:18	129:6 135:15	84:21 107:17	74:6 78:11
301:14	279:1	195:13 200:4	121:9,11 126:1	80:7 81:17
targets 12:5,6	telecommunic...	204:5 207:22	132:8 137:17	82:9,22 85:9
75:7,13 85:5	74:14 228:21	233:14 241:18	142:9,16	85:14 86:11
85:19	telephone 7:13	242:7 268:22	143:21,22	87:15,16 89:22

90:10 91:5,16	299:9 300:5,20	269:13,16	218:17 234:9	42:14 43:9,13
93:14 94:11	300:21,22	270:6 271:11	252:14 261:16	44:5 46:13,16
97:6 101:15	302:20 303:4	271:12,21	264:14 265:4	47:19 48:6
104:6,7,17,22	305:1,2	274:22 275:9	277:18 281:19	49:4 50:2 51:3
106:1 109:5,22	themes 90:3,3	276:3 277:5	284:4	52:4,18 53:6
110:12,15	theoretical 22:9	279:14 283:21	things 7:12 12:4	53:10,11 54:7
111:12 114:15	theoretically	285:3 287:5	18:14 21:1	55:12 56:12,17
115:15 117:13	261:11	292:11,12	25:1 35:14	57:2,16 58:4
119:2 120:10	theory 31:5	296:12,13	56:7 61:4	58:20 59:2,4
121:6 128:14	69:16 167:6	297:6 306:6,9	62:16 65:4	59:12 60:8,14
129:3 133:22	255:1 276:2	307:11,15,18	72:22 73:14	60:17 62:10,14
134:20,20	thereof 11:6	theyll 180:11	74:2 93:7 97:4	63:4,9,22
137:1 138:3	theres 15:4	theyre 31:17	99:21 103:20	64:13 65:2,5
140:2 146:21	18:15 31:15,21	38:8 43:17	115:13 117:7	66:2,6 67:13
148:14 149:2	32:11,15 34:14	54:12,17 59:11	121:14 129:6	68:1,5 70:4
151:11 154:4	35:18 37:12	81:12 87:9	130:16 141:14	71:10 72:2
159:8,9 160:21	38:11 45:3	94:8 127:8,9	148:17 161:3	73:11,13 75:8
168:9,9 169:11	47:15,21 48:3	144:14 152:9	168:3 175:11	77:8 78:19
174:11 175:12	49:8 54:18	156:9,21 177:7	176:3 177:16	79:1 81:6,8,9
178:10,16	56:14,17 57:6	182:15,18,19	180:9 195:3	81:11 82:5,9
180:8 185:3,5	64:15 65:17	190:18 192:1	204:4 206:19	82:18 83:7,8
185:11,18	68:15 69:4	192:13 194:19	208:10 211:4	83:21 85:2
187:13 192:9	71:3 77:8 86:2	196:17 197:19	214:1 216:12	86:7,19 87:19
195:5,8 198:13	89:6,11 92:4	208:11,12	216:22 221:16	88:1 89:6,21
199:2 200:1,10	97:17 99:20	218:7 271:19	223:13 230:2	90:4,13,20
200:16 202:4	103:19 105:18	285:8 291:18	232:20 234:14	91:5 92:21
202:19 203:17	115:9 116:19	theyve 54:17	234:15 235:13	93:8,10,19,22
212:15 215:12	119:4 121:1	112:6 129:13	243:18 246:9	94:1,11,21
222:5,9 234:11	124:22 125:3	179:13 215:5	251:4 252:13	96:21 97:5,12
239:21 240:18	131:3 134:13	277:6	264:1,2 281:8	99:10 100:8,10
240:20 241:17	134:18 148:21	thing 16:3 24:15	282:11 291:18	101:22 102:4
244:7 246:1	149:13 151:21	38:3 46:2,16	think 11:6 12:21	102:10 103:1,3
254:10 260:15	152:14 167:4	47:4 48:12	13:5 14:2,10	104:2 107:19
261:8,14	169:4 174:9	49:6 73:22	15:3,6,16 18:5	109:8,15,20
264:10 269:11	175:5 181:6	74:3 75:3 94:3	18:10,15 20:5	110:20,22
270:12 275:15	183:13,14	94:5 97:17	20:22 22:16	111:8 112:19
276:10 277:7	184:18 185:5	104:21 122:9	23:20 25:6,12	113:13 114:1,9
279:11 280:18	200:18 204:16	125:15 129:10	25:17,18 26:3	114:17,17
280:21 281:6	205:17,19	153:17 168:1	26:6 31:5,11	116:11,13,15
281:11,19	213:19 214:3,4	180:12 190:6	31:12,19 32:2	117:11,13
282:17,18,18	214:6 218:4	192:9 196:7	32:5,19,20	119:19 120:2,7
283:9 287:2	237:3 239:18	198:22 201:16	33:5 34:4 35:9	120:18 121:6
288:6 290:21	251:11 253:11	201:17 211:7	36:7 39:12,14	121:15 122:4
294:10 295:22	260:22 266:1	212:7 217:5,11	41:2,4,9,17	122:11,14,18

123:7,14 124:7 124:20,22 125:3,9,15,16 125:16,19 126:7,13 128:10,16,18 129:2 130:8 131:1,2 134:10 134:21 135:2 136:10 137:4 138:1 140:12 141:16,19 142:1,4 144:15 145:2,17,19,21 146:15 147:2,3 148:3,6 150:22 151:6 152:4 153:12 158:19 160:19 161:6 161:10,12,22 162:10 163:1 163:19 164:2 164:10,21 166:2,9 167:1 167:10 168:11 169:11,14,17 170:21,22 171:22 172:17 172:20,22 173:2 174:20 178:10,12 179:9,17,19 180:2 182:9,12 183:3,14 185:11 186:2 187:8 188:21 189:3,17 191:12,14,22 192:6,20 193:11,15,21 194:6,10,10,13 194:16,21 195:3,5,7,9,15 195:19 196:15	196:19 197:9 197:15,18,22 198:1 199:3 200:16 201:12 202:5,9,14,15 202:18,22 203:1,19 204:4 204:15 205:2,5 206:19 207:2 207:15 209:21 210:7 211:2,11 211:16 215:3,7 215:11 216:5 216:15 219:4,6 220:17 221:11 221:14,20 222:10 223:6 225:6,17 226:7 228:5,12 231:8 231:13 236:16 237:1,3,10,20 238:7,9,17 239:8 240:20 241:1,18 242:1 242:6,19,19 243:22,22 244:2,5,8,22 245:13,18,19 246:1,13 248:1 248:2,3,7,18 248:22 251:11 251:12,13,21 252:1 253:14 253:19,20 257:1,9,19 259:7,8,19 260:17 263:6 265:12,15 267:3,4,5 268:14 269:11 269:17 270:20 271:1,12 272:4 272:19 273:12 273:13,15,20	274:5,10 275:18 276:18 277:18 278:4 278:14 279:7,9 279:13 280:18 281:2,6 283:4 283:9,22 285:1 285:17 287:12 287:17 288:6,9 288:10,22,22 289:2,6,8,13 289:14 291:15 291:15,17 292:5,16 293:13 294:19 294:21 295:6 295:11,15,18 295:21,22 296:9,20 297:11,21 298:15,18 299:9 300:15 301:18 302:7,9 302:13,19 303:6 304:5 305:3 306:17 thinking 44:1 89:22 94:3 163:18 175:1 175:18 185:12 188:17 209:6 211:7 215:20 268:20 271:7 284:3 285:10 287:8 299:11 thinks 37:16 194:4 third 9:4 19:15 38:3 41:15,18 47:19 62:21 66:22 154:9 thirteen 155:5 thorough 208:13,14	thought 33:15 77:22 91:3 162:14,22 163:6 178:4,20 179:19 193:17 193:22 194:6 195:12 197:9 197:10 201:3 209:7 236:11 236:17 252:15 252:16 256:4 260:11 280:4 280:18 281:3 293:10 299:18 thoughts 65:20 98:22 166:18 199:4 232:3 254:16 262:6 270:1,10 293:9 304:12,19 thousands 78:21 78:22 146:22 threads 115:11 threat 14:7,9,22 235:18 threats 154:14 three 8:14 26:19 40:6 81:22 92:16 118:2,6 118:15 119:3 163:10,12 180:10 209:2 236:18 241:16 243:4 255:10 255:13 threepart 36:5 threshold 259:3 302:9 throw 277:22 thwarted 35:20 40:14 277:21 277:21 282:15 thwarting 278:5 tied 158:21	tier 19:12,14,15 198:21 ties 14:21 tight 262:2 time 17:11 18:9 18:13 20:9,13 23:15 24:1,9 29:19 30:2,15 30:18,19,22 34:3,16 40:22 41:10 43:16 54:22 55:8 75:19 85:19 91:16 92:15 99:15,16 111:9 116:15,16 123:4 124:11 137:15 143:19 145:18 150:17 155:1 156:7 157:7 162:18 180:16 188:17 196:20 207:13 209:8 210:21 212:19 216:17 216:17 223:12 225:19 235:12 240:5 241:18 250:18 260:3 262:8 267:11 274:11 282:3 293:13,21 298:15 310:6 timeframe 269:2 times 90:14 152:7 214:9 215:21 278:17 291:4 tip 291:14 292:10 tipped 46:1 47:12 tips 14:22
---	--	---	---	--

tireless 7:4	110:3,5	75:18 87:20	264:13	26:14 40:6
title 70:12,13	top 107:8	119:5 123:2,16	try 16:8 19:20	44:4 53:7,10
87:14,15 94:13	221:19 249:4	147:12 184:1	43:7 81:8 82:7	55:2 59:10,11
127:22 128:16	278:20,21	185:12 190:3,7	93:20 94:17	87:3 100:8
149:8 174:11	295:14	190:14 211:12	161:18 162:9	121:14 122:22
183:8 184:19	topic 143:3	228:5 233:9	166:20 168:12	155:17 161:22
208:13,14	145:20 277:13	292:12	175:2 189:7	164:5 165:10
212:1 277:6	308:16	transparent	192:19 198:15	171:22 182:8
today 8:5,14	totally 282:13	85:14 93:21	227:9 235:12	182:14 188:15
26:5 33:4 53:5	292:20 305:13	214:11	236:9 256:8	190:21 207:1
63:17 67:11	touch 222:6	transportation	260:19 268:4	208:11 221:17
76:13 90:4	tracing 49:21	16:14	273:8	225:10 228:4
93:12,16 97:22	track 117:19,22	treasure 146:13	trying 49:1,3	232:3,22
98:8 121:19	tracking 50:1	treated 72:12	75:9 111:2	238:20 249:9
122:11 139:9	113:20	137:3	136:15 157:11	255:13 259:10
144:6 155:12	traditional	treatise 205:6	157:17 167:1	291:18 296:20
167:4 178:11	108:6,10 109:1	tree 97:19	172:17 185:15	297:13,18,22
184:13 193:10	198:6 242:2	tremendous	189:21,21	twopart 35:22
209:3 221:19	256:7 271:2,5	271:11	194:7 198:14	type 12:1 32:13
225:22 228:1	275:11 276:9	trends 112:13	203:6,18 207:9	40:18 41:15
232:6 236:10	276:14	trespass 113:17	224:7 229:19	60:6 83:8
241:12,14	traditionally	trial 193:19	235:17 245:15	90:19 95:15
254:13 268:21	94:8,13 125:8	tried 118:9	262:21 269:20	136:8 138:3
269:20 308:11	277:2	119:1 214:15	272:20 276:8	144:3 146:19
today's 6:20 7:21	tragedies 220:17	263:5 294:22	299:3 303:22	156:15 166:8
11:2 13:9	tragedy 248:3	trigger 150:8	tuesdays 251:21	178:14,15
308:12,16	trail 29:14	164:7 258:21	turn 13:8,21	190:5 196:4
toil 158:20	120:16 210:4	259:9	17:7 18:2	213:19 250:8
told 24:18	trained 203:4	triggered 185:4	28:13 54:3	268:7
176:17 206:8	training 33:14	tripartite	61:9 156:13	types 26:12
222:1 253:3	33:15,18 35:14	276:14	179:12 223:13	56:19 83:10
265:2	transcript 9:15	trivial 152:19	277:12 284:6	85:2 117:4
tolerable 139:5	308:17 310:11	troublesome	turndown 208:2	134:10 136:19
toll 21:11,18	transit 304:17	152:15,20	turned 179:14	145:11,15
23:2,3	translatable	true 12:17 33:11	turning 69:8	147:10 203:22
tool 14:19,20	186:16,22	91:5,12 93:14	87:4 258:22	221:20 250:1
15:5,16 16:5,6	translated	155:22 177:11	turns 36:5	278:1
16:6 29:9,10	175:11	284:13 307:4	150:17	typical 94:12
36:19 40:18	translates 94:16	310:11	twice 37:20	149:16 198:6
48:19 122:17	translation	truest 178:2	58:13,14	typically 33:14
tools 14:5 15:10	175:10	truly 144:1	164:20	typo 27:15
17:4,4 41:6	transparency	287:2	two 6:16 7:6 9:1	128:13
108:4,18,19,22	55:5,22 56:7	trust 149:20	9:7,11 12:22	
109:18,21	73:5 75:4,10	262:17,19	20:3 23:2	
				U

u 3:6 12:1,14 13:1,4 27:11 29:20 32:15 65:22 66:1 67:2 68:2 69:9 69:12,16,18 70:22 71:8 73:19 95:4,19 107:13 111:20 132:19 133:10 133:18 134:5 136:6,6 141:12 165:14 199:18 235:3 239:4 260:1 263:3 277:15 282:16 301:4,10 302:3 307:19,20,22	undermine 11:14 96:16 underscore 151:5 underside 113:20 understand 31:12 61:11 69:9 71:14 79:13 80:11 85:3 90:12 92:11 97:19 104:21 105:3,7 112:20 129:17 130:5,13 133:2 134:7 137:8 138:5 139:13 140:4 141:7 143:15 156:17 177:6 184:14 186:10 190:3 198:12 200:5 220:6 229:17 250:22 251:7 251:20 259:13 265:19 understanding 21:9 99:13 102:16 105:4 132:15 153:5 174:17 179:11 188:15 211:6 244:3 249:5,6 270:16 273:18 277:3 297:10 301:7 303:9 understood 107:16 153:12 185:20 303:15 undertake 288:14 undertaken 12:7 95:19 underway 85:21	undesirable 60:9 undifferentiat... 239:3 undoubtedly 164:18 unearth 14:20 unearthed 15:15 unexplored 270:19 unfamiliar 156:5 unfortunate 221:7 unhappiness 105:19 unintended 8:10 unique 154:8 155:15 194:2 197:8 205:4 208:4 218:14 uniquely 221:12 united 32:17 34:12 45:17 46:9 48:22 49:5 67:14 69:12 91:21 105:2 132:15 136:3,4,5 137:1 141:8,19 143:9 144:21 181:10 203:15 215:10 222:2 223:4 237:8 304:2 universities 228:20 university 3:17 4:5,8 219:18 220:3,5 unknown 29:11 unnecessarily 190:1 unquestionably	91:11 unquote 128:19 240:5 301:6 unrest 105:18 untangle 173:5 unusual 70:5 149:14 184:15 184:21 185:5 232:19 235:20 updating 137:12 upheld 235:7 uphill 157:12 upper 198:21 upwards 128:11 urge 145:16,19 urged 9:11 urgent 61:22 221:11 urging 203:7 usa 1:8 2:10 7:8 144:8 use 12:13 18:22 19:9 20:15 27:1 41:11 42:7,12 49:10 49:12 52:5 58:16 71:6 74:18,18 84:4 94:9 95:11 97:13 99:6,11 100:13,18 108:22 114:15 114:16 117:21 121:1 133:4 138:2 168:5 174:18 256:6 265:2 295:22 useful 13:5 40:9 48:19 54:19,21 63:14 72:6 85:14 141:2 153:4 210:8 211:11 212:8 249:17 250:5	250:10 255:2 271:16 usefulness 62:15 user 156:11 users 156:2 199:12 uses 11:14 72:7 255:10 usual 108:1 usually 108:10 151:11 276:17 utah 281:17 utility 55:15 56:5 <hr/> V <hr/> v 111:17,20,22 112:12,22 190:8 vague 274:17 vaguer 45:9 valeo 237:9 valid 29:18 57:18 89:6 validation 64:21 validity 79:7 valley 10:21 valuable 14:4 36:8 63:10 value 15:17 18:7 18:15 38:5 39:16 42:4 69:4 102:12 112:2,15,15 118:11,16 134:8 278:10 values 221:4 255:21 282:18 variety 55:13 62:16 97:7 115:5,13 167:13 168:16 177:15 various 53:9
---	---	--	---	--

75:6 87:1 224:20,22 293:17 varying 8:16 vast 13:1 148:20 258:1 vehicle 63:14,14 113:20,21 veracity 11:5 version 124:18 188:13 264:11 versions 291:10 versus 167:21 188:13 191:20 237:8 280:14 vet 206:18 vetted 232:7 viability 30:11 victims 39:11,12 39:12,17 victory 281:4 view 13:22 14:2 57:21 112:17 116:18 118:9 119:15 139:5 153:18 155:15 173:9 188:11 188:16 192:22 218:11 228:22 229:15 247:3 250:7 267:1 284:8,10 289:14 294:17 294:18 303:5 viewing 232:4 246:9 viewpoint 87:20 views 6:21 8:6,6 9:13 117:12 174:20 229:5,6 229:11 violation 68:16 252:3 287:9 virginia 16:14	visit 176:17 visits 115:12 vizaviz 230:5 289:4 vladeck 4:6 220:3 236:4,5 241:9 251:10 251:11 256:12 257:1 258:8 259:19 273:10 273:11 276:17 282:20 283:17 284:11 288:8 294:12,19 300:9,18,22 301:18 voice 160:4 195:22 198:12 volume 301:3 volumes 83:11 voluntarily 43:15 113:7 voters 288:13,15 vs 44:1 288:10 <hr/> W <hr/> waiting 9:19 waive 199:14,22 wald 2:5 5:17 52:10,11 56:10 57:17 59:15 60:4 104:19,20 105:11,15 106:14,17 107:1,11,16 109:12 110:21 111:2 137:18 137:19 139:10 140:6 141:1,7 141:11 160:12 160:13 162:13 170:1 180:9 196:22 197:1 201:6 230:1	260:21,22 262:11 264:16 265:17 268:2 296:5,6,8 297:5 298:5 299:6,18 300:6 300:8,20 301:16 wall 92:4 172:15 186:14 walltowall 162:19 walton 124:2 128:5 295:3 want 6:19,22 10:2,5 13:8 20:7 23:12 24:20 28:3 33:9 34:11 51:1,5 53:11 54:8 56:3,5,18 59:17 65:14 67:9 69:20 72:21 75:17,19 81:10 84:11 85:13 92:8,12 92:13 97:2,8 100:17,19 103:8,10 104:20 106:17 114:20,20,21 114:22 126:22 129:2,22 130:1 142:9 146:10 146:16 148:17 151:5 159:18 162:7 168:7 171:3,6,8,17 176:13 179:10 180:4 185:17 190:7,8 192:11 196:7 197:6 201:17 202:5 204:12 205:21	215:15 217:8 217:11 218:13 231:6 249:16 263:1 266:5 279:22 283:20 285:12 290:9 291:14,18,20 292:2,3,9 300:10 wanted 33:4 35:16 41:8 80:9 86:1 98:13 100:22 104:9 107:12 120:7 122:21 175:19 176:1 177:10 180:20 209:15 216:3 217:15,20 241:15 250:11 267:6 290:2 wants 23:11 32:16 53:22 161:8 164:14 182:22 196:9 196:10,11,13 226:15 262:9 283:17 war 232:22 warrant 47:18 48:15,16 69:14 71:12 125:8 127:21 128:1 149:7 181:10 184:16 208:11 223:20,22 224:1,4,11,19 225:1 270:17 273:16 274:9 274:12,15,18 274:19 275:7 276:9,12,22 warranted 42:3 warrantless	144:11 warrants 25:7 125:14 183:7 183:18 261:19 273:17 275:14 276:6 wartime 146:15 washington 1:18 3:17 4:8 5:8 32:21 150:14 219:18 220:5 221:9 wasnt 38:16 94:14 102:18 152:19 186:9 187:18 199:8 209:17 242:22 252:15 267:10 269:5,9 280:6 watch 292:8 way 17:9,10 19:22 22:14,18 36:4 40:5 44:10 45:11 46:6 49:21 50:21 72:11 76:4 79:6 84:5 85:9,15 123:1 132:22 151:18 157:12,19 159:8 171:8,20 180:8,8 185:21 186:8 188:20 195:4,5 198:15 201:17 203:4,8 208:6 211:5 212:6 215:2 216:9 222:19 226:1 229:12 240:20 253:12 257:20 259:8 259:21,22 269:5 270:11 271:3,13 272:3
---	--	---	---	--

272:10 278:11	weve 14:3 18:5	widespread	women 262:12	148:22 182:15
287:2 292:16	22:2 26:16	56:14 107:22	won 151:18	182:18 224:1
293:1,3 294:10	31:2 32:2	wiegmann 2:13	wonder 296:9	227:15 228:15
296:18 299:14	38:19 40:11	10:9 23:13	wondered 268:2	228:17 232:11
300:14 306:5	45:13 49:1,2	31:11 33:22	303:13	242:21 251:14
310:14	55:16,17,19,21	42:14 65:8	wonderful	workings
ways 19:4 89:2	62:15 82:11	77:3,11,14	222:5	205:10
117:15 145:8	86:20 90:13	78:8 80:4	wondering 45:7	works 83:7
145:10 146:11	100:14 103:21	81:19 83:20	46:4 78:7 80:8	240:19 267:7
222:12 224:22	112:1 113:1	103:2 107:13	137:9 204:18	281:5 288:7
232:1 259:2	122:3 126:8	109:9,14	262:6 296:20	291:13 292:8
294:21 301:19	136:11 137:14	110:22 112:19	wont 261:22	world 10:15
302:8,14 306:6	140:12 147:3	120:2 126:20	woodrow 3:19	96:2,4 115:15
weapon 92:5	166:18 174:20	wifes 301:1	219:16	219:6 232:22
web 308:18	175:2 197:6	willful 68:16	word 57:2 154:7	worried 51:4
wed 19:12 20:4	202:10 232:5	willfully 133:17	183:9 248:16	167:16 168:1
20:4,5,6 64:9	236:10 257:22	willing 118:5	260:4	168:16 178:7
92:22 100:6	262:7 263:19	256:6	wordiness 109:7	281:4 305:9
119:12,22	272:21 275:9	wilson 3:19	words 37:6 43:2	worry 167:20
173:19	277:9 282:14	219:16 263:14	58:9 67:4	294:6
week 10:13	whats 30:13	win 126:11,18	77:14 80:12	worse 238:6
118:4 122:5	85:18 87:20	128:19 129:4	81:2 97:14	worth 38:8
125:11 127:14	91:9 98:10	130:15	134:5 163:22	65:12 68:5
179:12 207:9	110:10 157:8	winds 183:11	202:11 206:11	261:15 295:10
212:17 221:18	167:15 190:3	wins 151:13	260:6	296:1
221:19,19	211:14 250:22	wire 130:20	work 15:11	worthwhile 11:7
222:4 236:16	265:19	wires 176:2	35:12 58:1	189:17 194:4
262:15	wheel 150:17	wiretap 70:12	76:4 89:18	worthy 53:10
weekend 81:5	white 103:21	70:13 127:22	102:3 122:12	wouldnt 19:6
weeks 56:16	107:20 115:18	211:19	127:6,8 131:13	40:20 64:17
65:17 68:8	242:21 266:10	wiretaps 80:2	137:16 139:9	76:18 78:5
137:7	266:11	wish 197:5	147:19 151:9	97:8 113:22
weigh 15:19	whos 10:6,7,9	297:16	153:11 155:14	128:22 150:16
159:15 283:17	25:2 31:13	withholding	159:22 170:20	160:2 169:9
weight 302:20	80:17 83:15	163:4 170:3	185:6 208:5	179:5 229:19
welcome 5:5	124:2,10 143:6	withinnamed	210:11 217:8	247:22 253:15
9:17	150:21 168:6	310:5	224:12 257:20	257:2 260:8,9
wellqualified	176:2 179:14	witness 310:16	259:3 269:21	272:6 300:18
223:11	180:22 200:9	witnesses 143:5	272:1 289:1,15	wounded 39:7
wellsupported	213:8 219:15	204:10 209:17	worked 123:13	write 184:5,17
130:19	219:17,19	269:20 295:13	146:7 215:8	185:3,19 189:6
wellversed	276:2	308:9,10,11	228:20 243:7	208:8 210:19
14:13	whove 179:18	310:5,12	working 103:3	210:20 229:19
went 153:6	wide 8:9	woman 262:15	123:18 137:15	290:8,14

<p>writes 51:8 264:10</p> <p>writing 184:14 185:14 189:4</p> <p>written 9:16 12:4 30:4 102:1 139:17 146:12 186:3,3 230:20 261:18 270:3 303:14 304:9</p> <p>wrong 77:9 152:8 153:6 216:22 245:16</p> <p>wrongdoer 177:18</p> <p>wrongs 233:15</p> <p>wrote 152:11 185:10 189:4</p> <p>www 9:15</p> <hr/> <p style="text-align: center;">X</p> <hr/> <p>x 206:6 215:5 262:5</p> <hr/> <p style="text-align: center;">Y</p> <hr/> <p>y 215:5 262:5</p> <p>yahoo 10:14 155:9,10</p> <p>yall 130:8 177:8</p> <p>yeah 45:15 57:17 103:16 106:17 109:12 109:12 110:21 110:21 111:9 126:20 136:10 141:4 171:12 186:15 193:15 212:14 259:19 265:10 287:4 296:5 297:9 298:13 299:18 300:3 303:4 305:3</p>	<p>year 71:10 78:20 118:2,3 118:6,7 127:9 182:8 281:10</p> <p>yearly 137:22</p> <p>years 17:13 18:5 21:2 23:2 37:21 39:6 40:2,6,6,7,7 63:1 118:15,21 119:3 146:8 147:19 155:5 165:10 220:20 223:4 225:15 225:20 232:1 243:14 248:1 249:9 253:4 296:11 297:13 297:18 298:1</p> <p>yield 204:9</p> <p>yo 253:10</p> <p>york 39:3 44:6 44:11,18 48:4 51:3 291:4</p> <p>you'd 42:18 81:6 84:13 112:8 171:12 176:5,6 220:10 295:16</p> <p>young 217:1 262:15</p> <p>you're 11:20,21 15:13 31:10 43:2 46:6 50:2 52:18 53:4 57:12 64:20 75:8 93:19 104:3 105:9,22 112:6,20 130:10 133:13 135:10,13 142:6 145:2,4 145:12,12 146:4 166:22 173:20 176:7</p>	<p>177:16,19 185:14 186:13 189:20,21 190:6 196:5 200:16 212:2,2 213:12,18 220:7 221:9 248:16 299:21 305:8</p> <p>you've 36:20,21 44:21 56:21 63:2,9 92:2 97:22 101:7 106:2 109:12 115:3 133:5,7 174:15 175:9 177:17 192:20 199:4 203:21 204:4 209:8 241:18 266:13 270:3 304:9</p> <hr/> <p style="text-align: center;">Z</p> <hr/> <p>z 215:6 262:5</p> <p>zero 133:6 279:8</p> <p>zhou 91:2</p> <p>zone 277:8</p> <p>zoomed 277:9</p> <p>zwillgen 3:9 143:12</p> <p>zwillinger 3:9 143:11 154:19 154:20 160:10 162:21 164:17 173:7,9 180:12 182:13 191:12 192:19 199:5 217:21 286:7</p> <p>zwillingers 170:3 285:21</p> <hr/> <p style="text-align: center;">0</p> <hr/> <p>02 186:2</p>	<p style="text-align: center;">1</p> <hr/> <p>1 142:14</p> <p>10 310:22</p> <p>100 208:12</p> <p>101 222:17</p> <p>105 80:1</p> <p>11 6:3 15:21 150:11 164:1,6 243:8,8 263:10</p> <p>1127 1:17 5:8</p> <p>11s 243:9</p> <p>12333 11:14 66:17 68:14 105:5 107:1,2 107:3,3,7,10 120:14 132:10 136:3 137:13 144:22 243:19</p> <p>1254 260:1,4</p> <p>12542 240:3</p> <p>13 127:11</p> <p>14 9:18</p> <p>15 142:14</p> <p>16 5:11</p> <p>17 223:4</p> <p>18 21:1 40:1,2 121:1 136:21</p> <p>180 29:20 30:6</p> <p>1978 237:17 242:22</p> <p>1981 260:16</p> <hr/> <p style="text-align: center;">2</p> <hr/> <p>2 218:16 239:11 260:1,4</p> <p>20 5:6 309:1</p> <p>2002 143:11 176:15 205:1</p> <p>20022008 3:8</p> <p>20036 1:18</p> <p>2004 220:16</p> <p>2005 291:5</p> <p>2008 143:11</p>	<p>150:2 173:10 199:6 290:21</p> <p>2009 18:7 269:1</p> <p>2011 38:14</p> <p>2012 310:17</p> <p>2013 1:12 5:6,12 220:19</p> <p>2014 310:22</p> <p>2015 37:22 297:10</p> <p>215 1:8 2:10 7:7 7:10 11:3,10 13:9,17 14:11 15:20 16:17 17:6 20:20 21:3 22:13,19 35:13 36:11 37:20 38:8 39:22 52:13 57:3,8 60:8 73:1 75:15 80:11,14 82:3 82:14,17 84:1 84:18 85:6,11 88:17 90:6 92:17 97:16 98:10,13 99:1 99:7,11,16,20 101:8,13 102:7 104:11,22 107:21 111:13 112:16 117:19 119:7 120:10 133:5 134:20 144:8 145:13 145:14 147:3 202:15 209:19 212:11,13,14 230:1 238:3 254:9 261:1,4 264:17,20 266:16 267:7 268:6 273:16 273:19,22</p>
--	--	---	---	---

274:6 296:10	69:10 71:5,14			
297:2,7,10	75:16 85:17			
298:17 300:17	132:10,11			
303:3,4,4,12	137:19,22			
303:20	138:6,7,22			
215s 108:16	139:8 144:7			
22 27:3 51:11	147:2 156:22			
23 239:11	157:4 199:16			
23rd 148:3	202:14 203:21			
25 5:11 128:11	238:3 273:16			
27 18:10	273:19 274:1,6			
28 260:1	294:13 295:4			
288 78:20	300:10,14			
	301:3,6 302:20			
	306:4			
3	73 149:13			
30 1:18 13:2				
26:22 51:22				
63:12,14 64:16	8			
76:5 119:11,20	8 238:12			
120:5	80 208:12			
365 29:21	80s 253:5			
4	9			
4 1:12 309:1	9 1:18 5:6 6:3			
40 208:12	15:21 243:8,8			
45 218:16	243:9 263:10			
4th 5:6	90 26:20 27:1			
	30:2 35:6			
	36:14 37:1,12			
	42:1 50:12			
	51:19,20 52:1			
	58:13 62:6			
	63:13 73:21			
	182:6			
5				
50 129:4,4				
208:12				
5s 244:14				
6				
60 139:20				
208:12				
60s 217:3				
62 149:12				
6s 244:12				
7				
702 1:9 2:11 7:8				
7:17 11:3,10				
65:14 66:5,18				