

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

A	72:15 74:7	81:21 94:17	10:7,17 36:10	117:3
abilities 17:6	88:7 112:13	142:14	58:2	americans 18:21
ability 19:21	119:16	addressing	agent 80:15,16	47:17 125:13
40:20 70:21	accountability	74:11	80:19	amicus 123:9
86:3,4 90:7	130:10	adjourned	agile 17:9 20:4	124:18
100:13 110:4	acknowledgm...	142:17	agility 63:2,6	amount 13:6
119:8 125:17	57:5	administration	ago 39:6 68:8	57:6 59:9
able 19:6,8,14	acquired 70:10	31:8 73:4,9	118:21 136:18	60:13 83:16
19:17 20:15	70:17 73:20	80:21 85:1	136:18	85:12 90:5
29:9 102:4,12	132:13	118:5 123:4,7	agree 65:11 96:5	103:9,13 104:5
103:13	act 1:8,10 2:10	administrative	agreed 7:5	104:6
abolish 13:12	2:11 6:4 7:8,9	7:2	agreeing 6:21	amounts 13:1
abroad 133:15	9:1 11:16 84:7	adoption 52:20	ahead 59:16	113:13
139:17	94:3	advance 62:4	al 29:4	analogies
absence 73:7	acting 2:17 10:8	advantage 91:15	alarm 34:8	103:22 104:2
121:12	action 25:4	adversarial	allegations	analogous 79:22
absent 88:22	actions 6:7,9	123:2 126:9	10:12	analogy 31:13
89:1	25:2	130:7	allow 22:18	analysis 22:19
absolutely 16:7	activities 12:19	adversaries	27:17 86:8,21	85:16 95:12
34:17 104:16	46:10 57:20	54:14 74:16,20	87:7 102:4	113:1 134:1,5
abstract 76:1	67:17 80:16	87:17 91:14	108:19 109:10	analysts 140:20
101:22 102:1	84:19 132:5	93:1,4	119:18	analytic 135:21
115:13	activity 31:18	advertently	allowed 82:1	analytical 41:5
academic	45:3 51:10	133:10	114:12,16	41:6 83:10
114:10	actual 46:17	advertised	allowing 123:9	analyze 6:7 17:6
academics 3:14	105:10,15	122:6	allows 10:16	40:22
9:5	108:12 112:8	advisable 86:9	18:2 22:15,19	analyzed 135:18
accept 73:4 75:1	add 21:7 22:11	86:18	42:5 99:6	analyzing 33:7
118:6	35:8 37:14	advisory 6:17	alluded 95:9	announced 5:10
acceptance	38:10,18 48:17	advocate 124:19	alluding 51:17	75:4 122:2
117:1	51:1 59:17	124:22 125:2	alternate 48:10	annual 75:5
access 26:1	75:2 76:2	affect 60:12	48:11 88:20	anonymous
27:14 120:15	80:12 81:2	82:13,16	alternative 19:2	51:15
accompanying	83:20 93:10	affidavit 18:8	88:16 125:20	answer 31:10
90:17	95:14	affirmatively	amendment	54:6 80:22
accomplish	adding 37:15	71:6 124:14	23:18 69:17	91:3 116:13
73:22	addition 22:12	afoot 45:3	101:5 110:14	117:2 120:7,19
accomplishes	22:16 24:12	afternoon 8:21	111:16 113:3,9	120:20
81:13 123:14	43:11 50:14	age 40:1 117:18	116:10	answered 21:21
125:19	additional 23:4	117:22	amendments	answers 53:5
accomplishing	81:17	agencies 8:16	7:9	110:19 129:21
16:10 88:17	additionally	38:4 62:12	american 4:7	anticipate
account 25:20	19:17	67:19 137:13	20:7 92:21	100:20
	address 11:5	agency 2:16 6:2	93:3 96:3	anybody 53:22

anybodys 47:16	63:7 66:1 73:8	35:10 37:7	attacks 16:2,11	54:14,15 88:11
anyway 80:22	95:18 99:11	72:5 85:9	20:7 38:20	91:14
apart 37:21 38:5	100:1,10	articulated 64:5	40:14	aware 40:10
apocryphal 91:1	139:19	67:11 86:20	attention 39:15	52:19 58:11
apparatus 55:7	approve 27:4	93:15 123:8	122:14,15	75:3 135:5
appeared 9:1	51:12 62:3	articulates 37:3	attorney 2:13	aye 5:19,20
appearing	142:6	articulating	3:10 10:10	
142:11	approved 12:10	86:13	12:11 121:2	B
applicable	27:17 58:12	articulation	128:2,2 137:22	b 42:22 43:1
134:19	72:17 100:16	17:21 97:4	audit 120:16	back 32:21
application	106:21 121:2	aside 86:15	auditable 121:6	34:19 35:17
82:17 124:1	127:21 128:1	asked 39:21	audited 27:1	40:11,21 42:1
128:8	128:17 134:1	90:2 91:2	auditing 121:4	43:5 64:16
applications	138:9	107:19 114:19	audits 30:3 50:8	71:11 73:1
104:11 127:20	approving 31:4	117:7 136:17	51:19,20	74:9 75:18
128:1,16 129:1	arbitrary	136:18 140:3	authorities	80:4,7 84:22
130:17	119:16	asking 36:2,3,16	68:11 70:19	98:7,13 117:17
applied 48:11	arduous 137:13	78:12 105:17	87:2,12 88:7	119:20
127:19	area 56:22	109:8 117:20	89:13 114:3	backend 128:6
applies 121:8	areas 95:17	aspect 44:14,15	authority 71:7	background
136:1	arent 47:3 73:15	58:21	71:18 82:4	120:22
apply 83:22	102:1 114:12	assess 8:9 40:5	84:3,4 87:8,8	bad 37:17 44:14
98:17 127:5,15	140:14	64:14 88:20	99:8 111:5	baker 3:4
135:20 136:13	argument 31:12	130:15	authorization	balance 34:21
applying 79:4	125:9	assessing 78:17	61:19 126:17	138:16 142:3
79:14 128:20	arguments	assessment	138:2	balanced 6:9
129:6	125:19,20	25:22 50:1	authorized	72:2,10,16
appointing	arises 106:3	79:3 89:21	24:22 27:10	balancing
121:16	armed 132:3	118:11	63:13 66:16	115:19
appreciate	arms 96:6,9,10	assessments	108:2,7	ballroom 5:7
142:11	96:17 97:9	89:19	authorizing	based 25:22
apprized 61:16	arrest 44:17	assistant 2:13	35:10	27:5 44:12
approach 127:6	47:8	10:10 128:2	automatically	46:17 47:18
130:9 135:3	arrests 32:8	associate 4:7	110:4	60:6 75:14
approaching	article 11:6,9	associated 27:7	availability	100:2,11
88:18	12:22 124:22	31:22 45:10,11	22:17	113:16,17,21
appropriate	127:4	45:18 46:11	available 22:18	118:7
78:1 79:19	articles 12:17,20	47:1,3	24:3,14 83:17	basic 112:11
124:8	56:11 139:12	assume 53:4	90:6 109:17	113:5
appropriately	articulable 27:6	assuming 61:20	110:17 118:21	basically 104:3
6:12 33:20	28:4 31:16	assumption	avenue 1:17 5:8	136:1
79:4,14	44:2 45:1,8	82:20	avenues 48:15	basics 14:13
approval 61:11	61:14 79:9	assurance 4:4	48:16	139:8
61:12 62:6	articulate 28:14	attack 39:5,8	avoid 45:20	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 bear 98:22 141:20 bears 83:4 behalf 127:1 believe 25:21 32:9 44:3 45:1 45:9 46:7 48:21 68:7,12 82:6 117:20 137:5 believed 132:14 believes 8:11 believing 40:8 belongs 113:6 beneficial 14:1 beneficiaries 67:2 benefit 26:6 benefits 8:10 best 8:12 30:21 34:5 85:8,18 115:12 118:10 119:1 better 16:10 18:3 31:12 41:6 77:12 93:9 102:15 109:13 beyond 67:11 70:2 72:7 128:13 137:9 biannually 138:1 bifurcate 101:13 big 53:14 108:21 bill 57:1,8 80:10 81:5,10 billing 21:12,17 23:3,3 113:6	bipartisan 6:1 bit 41:10 56:11 94:18 107:18 131:7 blinded 54:5 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 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 bomb 39:2 books 111:18 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 branch 6:2,7 58:16 75:9 93:20 127:18 131:20 branches 92:16 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 breadth 71:17 break 8:20 9:20 9:22 142:13 breakdown 87:8 brief 9:12 59:18 briefing 137:5,6 137:10 briefings 131:17 briefly 65:15 briefs 113:1 bring 92:20 122:15 141:12 142:7 bringing 129:3 brings 141:11 british 10:17 broad 40:13 140:10,11 broader 84:8 broadly 103:9 103:12 broken 10:13 88:10 brought 15:10 106:4 brushing 130:20 buckets 62:18 budget 89:16 building 58:19 builds 63:21 built 37:17 101:17 builtin 37:12 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 bumper 113:19 bunch 32:12 47:2 burden 76:19 119:21 burdens 56:6 65:9 74:3 bureau 2:18 10:8 business 7:11 26:1 50:21 82:8 83:11 99:1,6 100:1	capture 69:11 car 84:12 113:18 care 127:16,19 carr 3:6 carrier 74:13 carry 10:20 98:18 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 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 cast 53:12 categories 81:22 139:1 category 100:7 138:3,17 cause 47:18 75:14 134:22 causing 114:2 caution 97:13 cell 14:18 center 3:19 4:3 centers 10:15,20 ceo 3:18 certain 13:6 66:19 73:2,5 90:16 91:18,18 103:9,18 105:6 certainly 25:7 30:17 33:11 57:6 59:12 62:9 94:1 97:1
C				
			c 1:18 3:16 5:9 43:1 111:20 cables 10:19 call 5:18 16:21 16:22 17:1 56:18 77:5 86:3 113:9 126:11 called 10:16 19:15 121:1 calling 25:3 32:16 34:12 43:4 45:16 calls 14:16 18:21 21:16,18 42:21 105:1 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 capabilities 55:10 87:10 capacity 108:17 108:20 135:7	

105:18 111:17 114:1,10 116:18 134:18 138:18 certification 137:21 138:17 certifications 66:20 140:14 chairman 2:3 5:3,12 6:5 20:11 79:2 81:7 125:10 chance 64:19 change 1:6 80:10 84:6 113:16 128:17 changed 112:12 changes 52:16 56:19 83:22 109:10 111:1 111:19 113:10 113:11,11 123:1,4 changing 83:13 channels 93:6 characterized 36:20,21 charged 15:22 chief 7:2,3 122:12 124:2 128:5 chosen 61:17 chris 12:3 circuit 111:21 circumstance 64:8 119:2 circumstances 26:18 61:21 70:9 93:21 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 classic 32:18 classified 93:14 94:19 124:4 135:17 clear 8:4 21:13 42:7,13 99:7 100:14,15 106:16,18 113:16 130:8 clearance 73:8 clearly 44:19 52:6 93:14 client 9:3 close 49:8 96:20 closely 122:12 closer 84:7 closes 122:5 codification 59:3 codified 58:18 102:13 codify 104:9 cognizable 111:16 cognizant 112:15 collateral 84:17 colleagues 15:18 15:19 collect 13:1 14:17 70:21 71:15 91:12,21 100:17 102:11	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 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 collections 136:6 collects 7:12 13:4 college 4:8 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 come 34:22 60:6 74:8 75:17 101:18 116:16 118:14 126:21 comes 30:3	71:11 72:11 91:9 102:21 107:7 119:3 comfort 130:6 comfortable 65:7 77:6 coming 33:4 127:12 131:5 commencing 1:18 comment 59:18 115:18 comments 9:16 46:13 117:16 commercial 22:6 commission 6:4 committee 3:22 committees 59:22 61:2,4 131:14,22 132:1,3,4,6 commonly 19:15 communicate 32:9,10 communication 10:14,18 65:16 69:13 96:1 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 community 37:3 89:7 91:8 109:22 117:8 141:15 142:7 communities 15:8 companies 10:21 23:14,21	24:13 25:6 86:13 87:7 96:3 99:5 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 compelled 24:8 compelling 116:5 competition 22:3 competitive 22:6 complement 15:11 complex 118:19 129:12 compliance 30:1 35:3 36:17 50:3,15 64:15 77:5,19 78:9 78:13,15 complicated 43:7,10 composite 19:22 comprehensiv... 62:21 comprised 6:4 compromising 55:9 60:18 computer 3:10 4:2 29:17 45:14 70:14 103:14,17 computerized 103:6 conceivably
--	---	--	---	---

24:10	confusion 57:7	53:10 55:13	135:3,5 136:12	120:9
concept 65:6	congress 3:20	74:6 110:16	contexts 97:7	corporations
102:9,19	7:6 9:5 37:14	119:13	103:5 110:17	96:13,18
concepts 101:16	37:18 50:5	considerations	115:6 120:4	correct 35:2
conceptual	53:19 57:1	25:6	continue 16:1	42:10 64:19
95:15	58:15 59:19	considered 6:12	28:6 53:12	90:21 106:9
concern 22:9	60:1,10 61:2	60:20 110:1,8	54:8 59:14	133:14 134:20
24:11 25:10,10	79:19 123:18	considering	continued 53:6	140:7
42:15 63:4,22	131:4	65:3,13 67:9	continues 36:18	correctly 105:4
64:3 65:18	congressional	69:3 89:2	continuing	122:4
88:9 121:11	89:14 131:2,8	consist 8:15	30:11 137:15	costs 8:10
concerned 93:1	conjunction	consistent 61:18	continuously	couldnt 24:17
125:4 130:7	35:6 129:14	75:11	50:16,20	41:13 73:6
concerns 6:11	connect 10:14	constantly 38:6	contributes 14:5	counsel 2:15,17
13:13 22:21	16:8,9 19:20	constitute	control 138:8	2:19 3:22 10:6
23:5 24:7 26:7	21:6	111:15	141:1	10:8 57:19
64:18 71:17	connected 19:13	constitution	controlling	97:2
89:4 104:13	connecticut 1:17	116:12 129:19	114:2	count 73:14,16
116:22 117:2	5:8	constitutional	controls 27:14	74:1
123:11,13	connecting 41:7	129:13 133:6	27:16 98:18	counterterror...
124:21	83:5	constraints 38:5	100:19 101:1	6:18 7:7,14
conclusion 54:9	connection	consuming	115:14	17:11 26:15
concrete 45:12	11:10 29:3	124:11	controversial	36:19 37:9
concreteness	83:15	contact 48:22	44:8	40:12 107:14
45:20	connections	80:18	controversy	115:8
concurrences	14:7 83:6,12	contacting	51:3 84:20	counting 73:15
111:21	83:18	17:19	conversation	country 68:1
conduct 30:9	connectivity	contacts 34:13	90:8 126:4	141:17
45:4 50:21	83:10	contain 56:12	cook 2:7 5:16	countrys 6:18
66:10 129:1	conscious 142:2	content 14:15	33:2,3 35:16	couple 62:13
conducted 38:12	consent 5:22	16:19 110:15	36:15 39:19	65:17 72:1,9
66:19 131:6	consequence	110:18 112:4,8	41:8 42:6,11	72:22 88:14
confidence	47:11	132:11	84:21 86:1,15	98:21 132:9
58:18 59:5,7	consequences	contested 25:3	88:13 90:1,13	course 24:13
63:21	8:11 47:5,7	context 17:7	94:6 126:2,3	27:21 44:5
confident	141:21	39:13 52:6,8	130:5,22	53:14 59:11
130:19	consider 7:22	75:19 84:3	cooperation	88:20 141:13
confirmed	116:21	85:4,11 89:13	86:5 92:6,6	court 3:2,7,8
130:11	considerably	89:14,15,18	copies 59:20	7:16,20 8:3 9:2
conflate 115:3	46:15,18,21	94:13,16	copy 10:19	18:9 26:21
conflation 51:4	47:6 48:7	103:22 109:19	core 103:10,13	27:9 29:19
confront 49:20	60:22	113:12 114:1	104:6	35:5,9 41:20
49:20	consideration	123:14 128:15	corporate 97:18	42:1,2,7 51:22
confused 59:9	1:6 52:19	128:21 130:15	97:21 98:5	55:3 58:13

63:7 64:13,14 64:19,22 65:9 66:1,20 76:3,7 76:9 77:17,18 78:9,13,14 80:2 81:2,16 100:7,16 101:1 102:16 106:8 109:16 110:8 111:22 112:21 113:2 114:6,19 115:9 124:3 125:2,17 128:7 130:4,17 134:2 138:4,10 140:14 142:5 142:15	criteria 62:14 120:15 critical 16:7 110:12 critically 42:18 122:11 criticism 57:7 cross 92:13 current 25:22 26:4 30:21 37:21 58:7 77:15 82:3 84:19 86:16 90:9,20 111:13 114:2 118:10 119:1 currently 63:10 63:20 67:5,9 86:11 90:5 119:6 126:9 curve 118:16 custodians 55:6 cyber 132:5	100:7,13 102:12 103:6,9 103:10,13 104:5,6 105:2 106:3,9,13,19 109:17 110:5 117:18,21 118:1,2,3,8,20 119:7 120:13 120:15,21 121:6 132:18 133:5,22 134:12,17 135:2 137:2 database 26:2 29:17 120:17 datas 24:13 date 16:22 david 2:3 5:2 12:3 day 35:6 62:6 63:14 89:18 120:5 days 26:20,22 27:2 29:20,21 30:2,6 36:14 37:1,12 42:1 50:12 51:19,20 52:1,1 58:13 63:12,13 64:16 73:21 76:5 119:11,20 139:20 daytoday 48:1 131:8 de 2:15 10:6 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 deal 115:4 dean 4:7 debate 15:4,17 58:20 59:10 92:14,16 93:12 debated 53:15 53:19 140:8 decide 98:12 decision 121:21 140:1,5 142:2 142:6 decisions 59:21 89:16 105:7 140:15,19 declaration 37:2 declarations 18:6 declassified 55:2 129:11 136:11 declassifying 123:18 decrease 22:6 deemed 79:19 defense 27:22 121:2 132:2 defer 18:22 76:11,22 define 46:6 definite 112:10 definitely 131:10	definitions 41:3 definitive 46:10 degree 46:17 47:20 66:2 67:15 68:2 degrees 8:16 delineate 75:12 democratic 59:13 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 dempseys 120:8 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 depending 74:17 depends 60:15 65:4 depth 62:22 deputy 2:13 10:9
courts 23:19 26:11 27:3,19 30:5 64:20 99:11,22 100:10 103:11 103:16 113:12 114:6	courtyard 92:3 cover 11:22 14:6 coverage 11:13 11:20 12:5,11 13:6 covered 11:21 11:21 56:22 covers 101:8 crack 54:1 create 23:4 24:2 29:14 created 22:22 creating 124:12 crime 3:10 71:4 92:5 105:6 116:2,3 134:9 criminal 23:9 31:18 45:2,4 108:7,8 125:13 127:7	D		
	d 1:18 5:9 111:20 damage 91:10 data 10:15,19,20 16:20 17:7 18:20 19:21 22:14 23:21 24:5,5,7,19 25:5,12,19 26:8,11,15 27:1,4,14 36:11 38:10 40:1,2,6,21 43:5,12,15,18 51:15 60:6 62:21,22 69:15 72:11,13 83:8 83:12,16 97:20 98:4 99:14			

derives 52:3	developed 33:15	3:18 4:3 7:1	discussions 64:5	34:3 37:15
describe 131:15	98:19 116:17	18:8 122:1	88:16 118:10	42:3 54:15
deserve 52:19	117:1 122:16	139:21 140:20	dispositive	65:1 91:20
53:19	developing	disagree 135:4	110:2	95:6 127:6,13
deserves 39:14	117:3	disappear 30:7	disrupted 35:19	doj 3:4 15:19
53:6	development	discerned 115:5	39:4	23:12 31:3,5
designed 34:8	6:12 33:18	disciplined	disseminate	31:10 32:21
65:21	developments	68:22	27:10 70:21	33:17
desirable 60:8	114:5	disclose 74:14	107:6	domain 124:9
desire 47:16	develops 109:20	86:4 119:8	disseminated	domestic 14:8
despite 108:8	device 113:18	disclosed 54:17	106:11,20	14:21
destroyed 24:13	113:19	60:18 111:12	107:9 134:6	dont 10:1 11:4
detail 88:11	devoted 126:5	disclosing 85:1	135:19	13:19 23:11,18
135:17	dialed 16:22	disclosure 54:13	dissemination	25:21 31:14
detailed 71:1	diane 7:3	54:20 56:20	94:9 95:12	41:2,18 43:17
131:16	dichotomy	60:22 92:19	105:5 134:1,4	48:16 54:7
details 11:6 53:2	112:10	93:2,17	distinguish 52:5	55:14 56:3,5
53:18 60:11	didnt 34:7	disclosures 55:9	district 3:7,7	57:9 59:2 61:1
94:20	difference 47:19	86:9 88:22	distrust 56:14	66:13 71:9
determination	111:1	91:7 97:1	division 2:14	73:17 74:1
28:19 29:1,15	different 15:10	106:6 126:22	10:11 127:2	81:19 83:1,7
29:16,18 30:10	16:3 40:17	discontinued	divorce 23:8	92:13,20 93:15
30:12,18,19,20	42:12 43:5,6,8	18:17	25:2	97:2,3 99:18
30:22 31:14,15	47:6 79:22	discourse 94:2	dni 67:8 75:4	110:19 114:1
32:6 33:13	81:17,20	discover 14:20	85:7,21 137:22	114:13 116:4
34:2,18 35:4	101:19 104:12	29:10	dnis 122:12	119:16 120:18
42:2 45:22	109:11 114:18	discovery 14:20	docket 127:13	127:10 129:2
46:18 47:10	136:13 140:18	29:10 48:13	doctors 115:12	129:21 130:16
61:14 62:4	differently	72:4 103:7	document 67:9	130:17 134:16
63:8 78:18	72:13	discriminatory	124:12	136:10 138:14
120:14 136:8	difficult 16:15	44:10	documentation	139:13 140:6
determinations	18:11 20:1	discuss 11:11	76:7,8,13,14	dots 16:9,9
30:1,3,4 48:2,7	38:19 63:5	135:4	76:18 79:10	19:20 21:6
49:9 55:20	64:14 73:15,22	discussed 82:11	139:22	41:4 83:5,5
62:5 63:15,16	74:22 83:18	97:22 99:4	documented	doublebarreled
63:19 64:17	118:17 124:4	discussing 26:17	28:19 29:17	53:21
77:4,17 78:10	124:11	121:18 126:6	63:16 139:17	doubt 53:12
determine 20:21	direct 122:1	discussion 8:13	documents	58:3
54:22 66:10	directed 66:14	9:6 15:4 38:11	99:21	downsides
115:11 118:1	67:21 94:22	43:22 60:10,21	doesnt 21:15	139:6
determined	95:1	74:21 75:20	54:16 68:3	downwards
68:10 102:17	direction 55:4	86:2 90:4,19	96:16 128:8	22:3
determining	64:20	92:20,21,22	135:13	dozen 68:9
31:6	director 2:20	93:6,12 115:2	doing 25:15	draw 54:7

125:17 driving 111:4 dry 91:19 duty 57:19	electronic 7:18 65:15 85:3 element 17:12 eleven 127:11 eliminate 55:14 56:4 81:10 elisebeth 2:7 5:16 email 38:12 emergency 64:6 emphasize 130:1 141:5 empirical 40:7 employees 97:4 enable 54:14 88:11 ended 38:14 44:9 energies 18:3 enforce 78:1 enforced 68:21 enforcement 24:19,21 28:17 engaged 46:9 115:2 enjoy 23:18 enlai 91:2 ensure 6:11 33:19 43:12 57:22 82:7 101:4 129:19 ensured 59:5 ensuring 6:9 entire 126:5 entirely 54:17 81:14 entitled 69:17 entity 97:10,11 environment 21:17 40:12 escalate 17:22 especially 75:18 essence 82:22 essentially 6:16	61:6 64:11 65:21 82:11 84:6 establish 81:16 139:16 established 6:2 76:15 93:6 101:3 establishes 81:18 etcetera 23:17 52:16 57:10,14 112:6,6 138:17 eugene 4:2 evaluate 38:1 39:9 61:17 114:7 evaluation 25:18 38:16 118:13 119:2 event 7:4 15:14 everybody 11:8 13:5 57:12 67:20 101:11 everyday 82:17 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 ex 125:9 exactly 41:15 48:22 49:3 65:5 72:6 76:2 76:3 78:12 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 exante 63:7 64:6 exceeding 64:20 exception 61:21 62:3 64:6,10 exceptionally 131:12 exceptions 105:5 109:2 exchange 9:13 exclusively 108:5 executing 50:17 executive 4:3 6:2,7 7:1 11:14 58:16 68:14 75:9 93:20 105:5 127:18 131:20 exercise 70:18 exercising 87:12 exigent 61:21 64:8 exist 40:15 existence 38:13 99:2 existing 30:11 exists 24:19 expanded 108:18 expect 12:18 58:7 78:15 128:21,22 expectations 64:21	expected 62:8 64:22 expeditious 122:19 expeditiously 122:8 expenditure 38:9 expensive 38:7 experience 31:6 60:7 131:8 experts 3:14 expired 20:10 expiry 37:22 explain 10:22 28:7 explained 65:11 113:1 128:6 explicit 101:15 explicitly 85:4 102:10 explore 8:9 expose 94:4 exposed 113:8 expost 65:12 expressly 35:10 extended 91:16 extending 66:2 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 external 50:4,20 extract 114:11 extraordinary 70:5 127:16 141:9,16 extremely 14:1 16:7 18:14
---	--	--	---	--

F				
face 57:9	46:1 47:13	49:1,3 112:3	127:3,11 128:6	66:10,21 67:3
fact 18:12,12	49:10 50:14	finding 68:15	128:20 129:8	71:2 80:15,16
29:10 33:20	92:2,2,9,10	fine 51:2	131:20 138:10	80:17,19 105:8
35:1 40:9	fbis 49:22	fingers 123:20	five 5:14 9:10	125:12 129:1
43:11 53:1,4	fcc 20:22 21:10	first 5:5 8:15,19	21:2 37:21	134:2,7,15
53:11,13,17	21:10,11,19	9:6,10 19:12	40:2,7 116:16	140:13 142:15
54:8 55:9,20	22:5	21:15 30:15	118:2,7,20	forgetting 84:2
57:7 62:2,5	fear 67:18 92:20	41:13 44:22	136:15	form 79:8
63:11,12 64:2	feasible 52:8	46:13 54:2,6	fiveyear 24:2	formal 123:7
64:13 66:8	86:9,18 95:5	55:11 57:15,19	flawed 82:19	formalizing
67:6 68:19	federal 2:17 3:6	66:14 68:13	flexibility 84:9	69:4
72:13 79:3,12	4:1 5:11 7:7	76:16 80:11	flip 87:19	former 3:8,9,19
85:14 90:14,15	10:8 24:20	81:1 86:10	floodlight 54:4	3:22 8:22 9:5
101:4 102:18	26:5 38:4	88:14 89:5	flow 47:5,7,12	59:12
110:3 121:19	feedback 79:18	95:7 98:22	flows 10:19	formerly 3:4
128:7 136:18	136:20	121:14 122:5	focus 17:15 18:2	formula 108:1
139:1 140:16	feel 44:9 62:12	127:20 129:7	18:3 65:21	forth 71:4 75:16
140:22	125:20	fisa 3:8 7:9	69:16	104:15 105:16
facto 110:4	feelings 57:14	11:19,21,21,22	focused 20:5	131:18 134:9
factor 58:3	fell 108:1	12:11 55:3	89:20 122:14	forward 40:20
109:22 110:2	felt 79:15	61:5 68:15,16	folks 12:3 26:7	42:5 55:1,4
110:12	fewer 83:5,6	70:13 75:6,13	51:5 66:12	117:3 122:7,17
factors 12:2	89:3	75:15,16,18	94:13 97:13	found 77:4
52:4 109:15	fi 66:16	80:1,13 82:4	115:2 119:1	78:13
110:7	fia 142:1	99:10,22 100:7	126:10 130:6	foundation 57:2
facts 17:21	fiber 10:19	100:10,16,22	133:19 140:3	112:17
34:19 44:2	fight 108:9	102:16 114:6	follow 33:9	founder 3:9
45:1,8 124:1,4	115:22	114:19 127:13	50:17 67:12	four 6:4 9:5
factual 76:14	figure 78:14	130:4,17 136:2	92:1 120:7	40:6 62:17
factually 104:21	85:8 118:19	136:2,12 138:4	126:3	fourth 23:18
fade 120:5	filed 18:6,8	142:5	followed 129:20	38:10 63:1
fair 57:6 88:15	86:12	fisas 87:14,15	following 88:13	67:8 69:17
fairly 71:1	files 103:15	fisc 9:2 12:12	90:1 107:18	101:5 110:14
familiar 133:19	filing 128:22	18:8 26:22	126:14	111:15 113:3,9
133:20	final 94:6	36:14 55:21	followup 20:12	116:10
far 52:6,6	115:18 120:6	58:7 59:21	28:3 49:7,22	fraction 88:6
105:13 108:9	130:22 142:8	62:10 63:11,12	56:10 72:22	franklin 7:1
fashioned 111:6	finally 9:4 27:19	63:15 64:1	75:20 86:2	frankly 88:1
favor 5:19 46:15	132:5	72:18 75:19,21	foreign 1:9 2:11	89:17
54:2	finances 40:15	76:21 77:2	3:2 7:15,18,19	fred 3:16
fbi 13:22 15:1	financial 103:19	90:17 105:14	8:2,22 11:15	french 91:3
15:18 27:10	find 15:14,20	106:7,21 107:5	14:7 26:20	frequent 131:12
	34:13 35:3	123:1,9 126:6	27:7 32:1,7	131:16
	44:16 45:15	126:12,16,20	58:12 65:18	frequently 36:1

41:21 64:8 124:2,3 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 frontend 132:20 full 17:22 18:10 39:15 49:16 58:15 fulltime 6:5 function 15:9 77:15 functions 6:17 122:10 fundamental 112:22 fundamentally 16:3 further 15:1 47:13,14 49:13 67:10 108:18 future 90:9,20 111:19 112:12 113:11 114:4	70:16 72:2,3 82:4 94:18 97:2 99:20 106:22 121:2 122:21 128:2,2 137:22 generalized 137:20 generally 47:21 66:11 71:1 89:7 97:1 99:10,22 103:16 generated 49:11 george 3:17 getting 54:5 63:2 71:7 78:12 108:4 129:3 134:22 136:20 140:2 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 given 33:15 34:16 46:1 58:1,7 64:7 83:8 87:11 93:17 95:6 97:14 132:5 gives 67:20 84:9 130:3,6 giving 44:3 45:1 45:8 gleaned 118:12 globalized 96:2 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 goes 97:20 131:4 140:13 going 15:13 31:20 36:5 40:19 41:19,20 43:17 52:11 54:21 55:1 57:13 60:21 73:1 74:8 83:3 84:22 85:1 87:16,22 91:7 91:10 98:9 108:12 109:3 111:6 112:6 117:5,17 120:19 122:17 123:20 125:11 142:6,13 good 5:2 16:12 20:19 22:1 24:15 31:20 37:17 41:9 43:21 44:14 67:13 74:16 75:22 94:2,5 google 10:15 gov 9:15,18 govern 120:12 government 7:12 8:15 9:2 10:18 13:15 24:10 26:5 32:8,16 34:10 53:2 70:18 77:6 86:6,14 86:21 87:5,22 88:5,7 92:17 95:22 96:7 97:6,11 98:12 103:20 105:16	115:22 119:7,9 119:13 126:11 127:3 128:22 138:10,20 governments 25:12 90:15 96:18 111:10 116:7 governmentwi... 87:1 governs 107:3 gps 113:18,19 grand 19:9 20:15 23:17 41:11,14 42:16 43:8 103:7 108:9 109:2 granted 128:7 granularity 87:10 grassley 68:7 great 25:17 67:18 76:19 80:7 115:4 119:5 greater 46:21 55:21 67:14 68:2 72:16 94:1 108:19 greatest 9:12 115:21 116:8 118:11,16 group 45:11 guarantee 43:17 guess 18:16 61:9 76:5 78:7 90:11 98:15 102:14 112:11 119:15 guidance 117:10 guidelines 121:3 136:19 137:12 guys 33:4 101:9	<hr/> H <hr/> hackers 24:15 hacking 25:8,13 half 30:1 44:22 45:2,8 halt 142:7 hand 15:1 86:21 86:22 97:12 handle 76:21 133:22 handling 127:8 hands 69:22 happen 89:10 happened 15:6 51:13,21 60:7 93:17 happening 22:8 85:17 93:16 happens 30:8 35:11 88:2 89:12,18 hard 59:10 72:5 72:12 131:15 harder 16:3 19:22 harm 93:16 harman 3:18 harms 93:15,18 hasnt 128:8 haystack 108:4 108:21 headphones 94:15 headquarters 10:18 92:2 hear 76:8 heard 22:2 31:2 62:16 90:13 94:14 115:10 hearing 1:4,16 5:5,10,18,19 6:20 7:21 8:8 11:3 13:10
<hr/> G <hr/> gather 18:19 gathering 66:14 gchq 10:18 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				

90:15 125:10	132:6	52:11,17 54:5	124:14 133:16	49:13 64:13
heavily 34:17	houses 60:1	59:16 73:1,8	141:20	92:15
111:13	huge 109:3	74:5,8 76:1	importantly	indication 18:7
heightened	human 51:16	77:6,9 78:7,11	105:13	indicator 74:16
95:17	humiliation	78:12 81:5,13	impose 56:3,6	indicators 20:3
held 1:16 13:15	44:18	81:19 90:11	74:2	indicia 58:6
24:8	hunch 29:8	98:7 99:19	imposed 100:12	individual 47:1
help 14:6 139:10	hundreds 39:6	105:17 109:8	105:14 133:5	47:3 49:20
helpful 9:21		111:2 117:5,19	improper 68:18	82:14 84:5
15:21 16:8	I	120:19 135:5	improve 31:2	113:18 125:18
18:14 33:5	id 12:15,15 13:7	135:11	inaccurate	127:14 140:11
37:8 72:4	14:10 15:18	imagine 118:18	11:17	140:14,19
92:14 126:13	26:3 37:14	immediate 47:8	inadvertent	individualized
126:18 142:10	38:3,10 54:1	immediately	132:17	138:22
helpfulness 40:5	62:13 63:18	44:16,20 45:4	inappropriately	individually
hes 128:10	66:22 72:9	46:3	67:21 68:11	19:20 93:8
high 79:16	76:7 80:4,22	immigration	incident 77:19	individuals 82:9
130:10	117:13 126:3	23:9	incidental 95:4	130:11
higher 84:14	idea 37:17,17,18	impact 11:1	incidentally	ineffective 54:18
128:14 135:1	48:14 64:5	12:1 71:19	12:14 133:10	inevitably 15:5
highly 26:4,10	65:12 75:22	72:16 82:2	141:12	infinitely 43:7
44:8 129:17	79:2 113:5,17	84:18	include 8:22 9:4	informal 131:17
hinges 101:12	124:7	imperative 95:6	21:15 136:5	information 4:4
hiring 122:3,8	identified 68:9	implementation	included 108:3	7:18 10:20
historical 59:8	identifies 77:16	6:13	includes 35:14	12:14 13:2,4
historically	identify 48:15	implemented	39:16 42:4	13:14 14:17,18
11:22 58:5	identifying	33:16 44:10	66:17 105:1	16:4 17:18
67:18 68:1	14:16 82:9	77:7	including 39:2	18:19 19:11
118:17	ii 3:1	implementing	92:5 133:21	20:17,17 21:4
hit 62:20	iii 3:13 70:12	6:3	138:14	24:3 27:10,11
hitting 90:4	94:13 124:22	implication	incomprehens...	28:9 30:20
holding 99:16	127:5,22	11:12	124:13	41:16 45:22
113:15	128:16	implications	increased 62:10	49:4,10,13
holdings 23:19	ill 28:6,13 53:22	70:2	increasing	58:15 67:2
homeland 132:6	76:11,22 92:1	implore 12:16	141:21	68:18 69:6,18
hop 41:13,15	138:2	important 17:12	indefinitely	70:6,10,15,17
hops 19:15 43:9	illegal 94:3	18:13 39:13	101:11	70:22 71:7,9
55:18	illustrations	43:14 48:12	independent 6:1	71:12,15 76:10
hotel 1:17 5:7	39:2	58:3 78:19	47:14	77:18 79:8
84:11 101:9,9	im 5:2,3 11:5	83:21 87:21	independently	80:3,14 82:1
101:10,10	16:13 21:10	92:10 96:5	78:10	85:14 87:4,22
hour 99:17	31:9 36:9,16	110:8 114:9	indicated 16:18	88:5,10 90:5
house 3:22	40:10 42:9	115:1 121:7	18:9 24:16	91:12,19 95:5
17:20 131:14	45:7 46:4	122:11 123:10	38:22 41:10,22	95:11,13 96:2

103:18 107:14	15:16 26:13,20	50:4,19 64:4	investigative	judge 3:6,6,8
110:6,9,10,11	29:3 31:21	121:6 139:14	17:4 18:4 19:4	9:1 52:10
110:13,18	36:9,10 37:3	internally 50:9	49:14 50:11	57:16 79:5,10
113:2,6 114:12	37:19 38:22	89:2 130:9	119:21	79:15,17
115:10 120:10	39:17 50:8	135:16 138:9	involve 12:9	104:19 115:4
134:4,6,8	54:11 55:7	international	14:15,16	115:17 124:2,2
135:6 136:1	58:12 59:22	14:21	128:12	128:5,6 137:18
138:13	60:18 61:2,4,7	internet 98:14	involved 27:12	judgement
informative	66:11,13,21	98:17 99:9,13	33:17 34:17,17	32:22 42:4
112:2	67:7,16,19	interpretation	57:10 68:13	judges 79:6
informed 20:4	71:3 89:7 91:8	108:6,11	115:10 124:10	127:5,11,12
59:19	91:13 94:2	interpretations	involvement	judicial 47:9,18
initial 133:13	105:8 109:21	35:13	31:3 141:18,22	61:11,12
inquiries 120:17	117:8 118:22	interpreted	142:3	123:22 141:17
inside 136:3	120:4 129:2	96:19 106:8	involves 7:17	141:22 142:3
139:19	134:2,8,15	interrupting	14:14 46:19	judiciary 3:22
insight 85:18	139:21 140:13	140:7	85:12	59:22 61:4
inspector 27:20	140:21 141:14	intervening 47:9	ipso 110:4	131:21 132:4
27:22 28:2	142:7,15	intimations	irrefutably	jump 10:3
30:4 50:6 68:6	intended 11:22	111:19	91:11	jurisdictional
inspectors 48:1	14:6 72:15	introduce 10:5	isnt 97:9 102:13	11:20
instance 56:21	intent 29:6 81:6	introduced	140:10	jurisprudence
66:14 127:20	81:8,11 82:7	13:11	issue 11:13	28:13
129:7	intention 82:10	intrusion 46:16	22:11 42:16	jury 19:9 20:16
instances 68:9	intentional	46:17,21 48:8	43:1 44:15	23:17 41:11,14
institute 100:22	132:17	113:22	124:22 125:4	42:16 43:8
institution	intents 58:19	invasion 115:20	issued 75:6	103:7 108:9
59:13	interagency	116:9	issues 44:4	109:2
institutional	66:9 73:8	investigate	103:4 129:13	justice 2:14 3:10
58:6,8	intercept 47:16	48:19	129:18	10:11 26:22
institutionally	interest 17:2	investigation	ive 24:18 80:8	27:2 30:2 34:3
93:8	71:22 111:16	2:18 10:9 15:2	96:12 103:4	35:12 36:2
instruments	115:21 116:7	17:11,17,22	111:9 115:10	50:6,6,7 63:20
108:17	119:5 122:5	18:1,12 47:13	119:18	76:22 77:16
integrated 22:15	interested 52:17	47:14 48:15,16		78:4 127:1
integrity 50:15	76:8	49:5,15,16,22	J	129:2 130:3,18
intel 131:14,14	interests 26:7	67:4 80:13,17	james 2:6 3:4,6	130:21 139:20
131:21 132:1	116:6 123:3	84:13,16 100:4	5:16	140:21
intellectual 3:11	interfere 64:18	104:7 108:2,7	jane 3:18	justices 13:22
intelligence 1:9	intermediary	108:12,14	janosek 7:3	justification
2:11,20 3:2,5	78:5	109:6	jim 54:3 107:19	47:15 111:11
7:14,15,18,20	intermingled	investigations	jones 111:20	justified 78:17
8:2,22 10:17	59:11	18:10 70:11	112:21 113:15	129:7
11:16 15:8,9	internal 37:12	82:2 120:4	114:1	

K	knee 118:15	large 59:9 60:12 83:11 87:14 113:13 138:22	59:3 90:15 95:18 99:8 111:10 112:15 112:17,18 115:14 123:11 123:12 124:21	limitations 55:17 97:22 98:2 100:12 101:16 107:5 119:18 133:8,9
k 3:21	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	larger 104:5 110:10	legally 111:16 125:21 130:19	limited 83:2 114:14 134:20
keep 9:12 20:22 21:1 23:14,21 25:19 43:17 63:1 65:8 76:13,18 99:5 136:15	knowing 105:20	late 16:13	legislative 13:11 37:15 57:3,5 57:12 89:1	limiting 27:14 71:20
keeping 135:10 135:13 141:2	knowledge 30:21 47:21 60:10	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	legitimacy 58:2 58:6,21 59:3 112:18	limits 41:11 67:5 119:16
keeps 21:2	known 17:19 29:3 53:20 54:13 58:10 80:18 83:2,16	lawful 19:4 57:20 94:4 132:17	legitimate 115:3 133:4	line 12:21 13:3 79:11 92:12,13
kelley 2:17 15:20 16:17 19:3 20:19 24:12 38:18 40:10 41:17 42:9 49:12 50:2 74:10 82:18 92:1 115:17	knows 57:12	lawfully 70:6,10 70:17 132:16 133:3,6 134:11 135:2,6	length 16:22 43:15 48:5 96:6,9,10,17 97:9	lines 34:4 92:12
kelly 10:7	L	lawyer 21:10 32:21	lengthy 119:20	links 10:14
kept 22:14 23:22 25:5 26:11 29:17 59:19	lack 11:5 130:7	lawyers 9:1 24:4 31:14 34:17,22 125:17	less 46:16 48:7	list 76:6
kerr 3:16	lacks 126:10	lay 37:9	letter 19:10 50:17 68:6 128:11	listening 43:22 74:20 94:14
key 12:2 110:15 116:11	laid 111:11	layer 41:19	letters 42:8,13	literally 78:16 124:17
keyed 108:16	language 81:12 82:6 85:9	lead 48:2,21 49:4 60:22 87:17 108:12 109:4 111:6	level 50:10 72:4 88:10 127:22	litigation 23:8 24:22 48:4 86:11
kick 120:19	laptop 32:7,9,11	leading 85:8,22	levels 24:19 130:10 139:18	litt 2:19 16:13 21:7,9,22 46:12 54:1 59:17 60:14 64:3 65:2 67:12 69:21 70:4 73:7,13 78:19 81:4 82:5 86:10,19 90:11,22 95:14 98:21 99:18 101:22 102:14 105:9,12 106:12,15,19 107:2 114:8 117:5,11 119:15 120:8 120:18 123:6 124:20 125:7 130:1,14 137:4 137:11 141:4,8
killed 39:7		leads 14:21 110:6 111:8	letter 19:10 50:17 68:6 128:11	
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		learned 12:3	letters 42:8,13	
kinds 87:11 91:18 105:6 106:6 112:4		leave 13:7 32:3 97:8	level 50:10 72:4 88:10 127:22	
		left 122:22 124:15	levels 24:19 130:10 139:18	
		legal 7:3 23:10 28:11 35:12 36:18 43:12 47:14 52:2,3	liberties 1:3 5:4 6:11 116:22 121:20 122:13	
			liberty 6:11	
			lies 138:8 141:1	
			lifetenedured 127:4	
			light 25:11	
			likelihood 21:3	
			limit 70:20 80:14	
			limitation 81:22 99:20 134:16	

141:13	129:15 132:19	101:2 113:21	127:10 135:9	79:2 89:11
little 16:14	137:2	125:21	135:12,14	132:3
34:16 41:9	lose 112:16,17	marc 3:9	meant 108:8	mere 102:8
54:4 56:10	137:6	maryland	measure 58:19	met 29:9 31:7
64:9 76:1	loss 126:11,18	111:14,17,22	75:4	101:6 104:15
94:18 107:18	128:19	112:12,22	measures 59:1	metadata 7:13
131:7	lot 13:13 15:4	material 26:1	79:18	14:11,14 16:18
livingston 1:22	20:6 33:14	80:12,13 81:2	meat 138:7	38:12,13 51:10
llc 3:21	35:18 39:14	83:14 111:12	mechanics	60:6 98:14,17
local 21:15	44:9 53:16,17	materiality	139:8	98:17 99:5
24:20 116:2	65:18 86:2	81:17	mechanism	100:3,18
located 5:8	87:10 97:2	materials 35:14	37:12 64:16	101:17 102:7
133:15 139:17	112:1,2,4	60:1 90:17	76:20 78:3	104:22 105:1
location 12:5,5	114:10,11	matter 12:8	139:4	105:20 106:10
14:18	116:17 127:19	29:22 43:12	mechanisms	111:15 112:2,4
logical 90:21	128:3,22 133:8	60:9 66:7	95:2	112:14 113:13
93:11	lots 15:10 56:13	86:11 108:13	medine 2:3 5:2,3	114:11,15,20
long 20:21 33:14	116:5 141:14	109:5 127:17	5:21 10:2 13:8	115:5
41:4 43:12	low 79:17	matters 94:2	18:16 20:9	method 111:6
55:14 142:10	132:20	mayflower 1:17	33:1 43:19	methods 60:19
longer 21:15	lower 127:22	5:7	61:9 64:12	61:1
23:20,22 24:8	lump 123:3	mean 24:5 26:9	65:14 69:8	metrics 36:6
25:5 38:13	lunch 8:20	28:15 31:14	71:13 72:19	mic 103:3
39:11 53:1,3	142:13,17	45:19 51:8,11	95:20 104:19	microphone
82:3 91:20	lyne 1:22	51:14,20 54:16	116:15 117:9	77:9
99:15		68:3 70:8 76:4	117:16 119:4	microscope
look 19:21 32:14	M	81:19 82:15	120:6 121:9	126:21
34:19 39:10,11	m 1:18 5:6	84:2 85:6	126:1 132:8	mill 82:14
40:11,13,20	madrid 39:5	91:17 93:13	137:17 142:8	mind 23:4 25:9
41:5 49:18	mail 9:18	99:12 102:14	meet 28:9 36:18	54:18 65:9
79:6,10 94:12	main 10:14	103:2 104:9,13	56:6 84:13	98:22 141:20
101:1 102:22	maintain 18:20	107:3 113:15	107:10	minimal 115:20
103:3 104:14	62:15 99:5,14	124:17,18	meeting 38:16	116:9
110:7 117:8	maintaining	127:20 128:8	142:17	minimization
119:22 126:18	62:19,20,22	135:17 137:11	member 3:19	12:10 94:8,11
127:17 128:18	major 62:17	140:10	9:5	95:15 120:22
129:9 138:15	majority 68:12	meaningful	members 2:1	133:21 135:15
looked 92:3,17	68:17 128:17	85:10	5:14,15 6:5 8:5	135:20 136:11
109:16 129:14	making 7:4 11:7	means 21:11	9:8,16 58:11	136:22 138:5
131:4	31:14 32:22	28:7 51:6	mention 38:3	minimize 12:12
looking 31:9	33:12 56:19	85:18 88:16,20	mentioned	95:3,3
39:15 46:6	69:5 83:17	89:3 95:1	23:16 35:7,17	minimized
50:16 78:16	113:8 127:19	104:4,4 108:7	36:13 39:19	135:6,9,12
91:8 103:11	manner 55:22	109:16 110:3	47:20 63:19	minimum 37:11

140:3	mundane 25:2	71:11 79:21	notify 61:3	48:10,21 49:2
minuscule 88:6	muscular 10:16	83:11,18 85:21	noting 68:6	49:2 55:18
minute 9:9,10		89:1,16 92:9	notion 57:9	62:1,22 67:1
13:20 28:13	N	93:7 102:4	105:21 111:3	73:19 74:14
60:5 99:17	nail 104:20	120:3 123:13	111:14 126:8	75:5,13 87:3
116:16	name 15:4 47:2	125:16,19	131:11	87:14 88:3,3
minutes 9:20,22	47:3	135:7 140:18	novel 135:3	88:15 95:17
122:22 136:15	narrowed 71:20	needs 37:7	november 1:12	100:2,8 106:1
misimpression	nation 6:8,14	38:17 59:5	5:6 9:18 122:6	128:15
66:13 97:9	55:8	85:20 104:15	nowpublic 35:9	numbers 17:3
misinformation	national 2:14,15	142:5	nsa 10:13,17	19:5,13 27:17
59:9	2:20 10:7,10	networking	11:14 12:9,22	32:12 34:11,12
misleading	16:1 19:10,10	43:2	13:4 14:17	39:1,10 40:18
96:22 124:14	25:9 42:8,12	never 39:12	17:6 18:20	40:19 41:3
misleads 15:17	85:20 94:16	54:9 68:15	19:7,16 21:2	43:4,5 45:15
mission 14:6	95:6 116:5	91:17 93:13	26:21 27:21	45:16 47:2
16:10 37:9	127:2 128:3	100:15 106:4,4	29:22 30:3	61:13 73:20
38:5 50:17	139:21 140:20	131:4 138:10	36:3,8 37:2	74:17 75:7
missions 6:6	nationality 12:4	nevertheless	38:4 51:3	83:2 110:14
mix 124:17	nationals 67:3	133:7	56:15 57:19,22	nw 1:17 5:8
mode 55:5	67:16	new 30:10 39:3	63:22 68:6,10	
model 83:7	nations 67:14	44:6,11,17	68:22 70:1,2	O
modification	natural 38:1	48:4 51:2	79:10 89:8,17	objectives 40:16
128:13	89:12	77:11 108:18	96:13 97:2	obtain 19:5,11
modified 128:9	nature 58:1	108:19 109:20	109:17,20	24:22 25:1
modify 13:12	60:15,17 64:7	newspaper	121:5,13	40:18,19 41:15
moment 22:22	110:11 137:21	139:12	122:16 131:22	54:13,14 84:5
month 68:7	necessarily 8:5	nexus 14:8	139:14,19	99:1
months 21:1	36:17 78:5	nondisclosure	nsas 14:2 76:17	obtained 23:16
40:1,2 136:18	necessary 59:3	119:11	131:13	32:7,14 82:8
136:18	59:13 62:14	nonu 29:21	nsi 20:16 23:16	103:6
morning 5:2	102:11 103:12	65:18 66:3	43:1	obtaining 99:3
16:12 43:21	103:14 104:5	67:10 68:19,20	nsis 19:1 41:12	obvious 81:8
62:16 142:10	107:21,22	69:6,11 133:14	41:14 42:16	obviously 13:22
move 21:16	108:2 110:9	133:17 139:16	43:8	14:13 47:6
moved 21:14	118:2 134:7	141:6,18	number 13:10	48:10 55:1,3
moving 33:7	necessity 102:9	normal 89:18	16:20,21 17:5	58:10 65:4
mueller 18:8	102:18,20	northern 3:7	17:18 18:6	70:2 77:1
multiagency	103:1 107:19	note 12:8 16:15	19:12,13 27:6	85:10 105:17
140:4	108:1,3 142:4	63:18 122:9	29:4,20,21	110:12,15
multiple 42:19	need 6:9,10 16:4	noticed 12:21	31:22 32:14,15	112:22 114:4
43:3,8,9	28:6 37:3	87:16	34:10 38:20,21	117:2 119:17
139:18	53:12 56:17	notifications	38:21 42:21,22	126:21
multi-point 80:1	57:1 61:22	131:17	46:8 47:1,12	occur 132:22

occurred 34:15	72:5 123:8,15	opposing 125:18	overall 88:3	62:5 76:12
occurs 131:9	131:12	optic 10:19	overheard 70:12	100:2,9 102:18
october 5:11	opened 17:14,14	option 18:18	70:13	107:16 108:16
odni 28:1 62:11	38:20	77:3	overlybroad	132:2
offer 46:12	openended	options 8:13	141:3	parte 125:9
98:21 117:12	111:3	order 5:18 7:15	overriding 88:9	participating
office 2:19 3:4	opening 5:19	11:14 14:20	overseas 17:20	6:20 42:20
50:7,15	operate 40:16	22:13 27:9	32:2,8 69:11	participation
officer 5:13 7:2	54:12 119:6	43:16 68:14	132:14	123:10
7:3 28:17 51:8	operated 1:7	77:19,21 78:1	overseeing 61:7	particular 11:20
121:13,20,20	operates 123:1	78:2 83:12	oversight 1:3	14:11 15:13,14
122:13	126:16	84:14 85:11	5:4 6:17 27:21	15:16 18:9,11
officers 33:12	operating 61:18	95:3 100:5	33:19 47:20,22	19:5,5,11
official 73:9	62:7,8 64:8	102:12 103:10	48:5 50:3,20	22:11 29:8
80:20	operation 53:18	103:17 104:5	58:8 61:10	31:4 32:1
officials 8:15	77:20	105:5 115:9	76:20 131:2,5	47:15 58:5,14
27:4,9 57:22	operational	133:17	131:8 132:7	61:13 62:1,11
ohio 3:7 44:1	13:20 32:20	orders 26:11	overwhelming	64:1 66:18,21
okay 10:3 74:8	38:17 53:2	27:3,20 29:20	128:17	73:10 74:13
75:17 80:6	63:1,6 64:18	30:5 35:9 55:2		87:11 88:1
92:18 103:8	75:11 119:17	64:15 74:15	P	89:8 97:13
104:7 105:15	141:21 142:4	75:5,13,14,15	panel 2:9 3:1,13	107:5 109:19
107:17 111:8	operations 8:2	75:15 82:14	8:19,21 9:4,9	115:7,16,22
135:22 137:19	126:6	84:1,18 85:19	9:10 10:4,22	116:8 118:19
old 40:6,6,7,7	operative 29:4	90:17 138:9,21	11:18 14:13	118:20 131:22
111:5 118:2,3	29:11 31:21	ordinary 84:10	16:15 75:3	135:8 140:10
137:1	operatives 32:11	84:18 104:11	126:5,5,14	particularized
older 40:8	operator 31:13	127:21	133:19 142:14	101:14
omb 73:8	33:19	organization	panelist 9:20	particularly
once 24:12	operators 32:4	27:8 32:1	panelists 6:19	38:7 96:1
54:16 71:9	34:5,22	organizations	9:11 10:5	110:17
132:18	opine 89:1	40:15	142:9	partners 86:4
ones 33:12 38:7	opinion 59:21	organized 116:3	panels 8:14 9:7	96:13,14,15,18
69:22 73:6,11	82:15 123:20	origins 28:12	9:11	partnership
115:12 121:18	123:22	orin 3:16	paper 29:13	97:5
122:10	opinions 97:17	outcome 49:19	56:12 103:21	parts 53:7
ongoing 101:11	123:17,19	116:11	107:20 115:18	109:21 124:14
101:20 117:14	129:9,11	outside 3:14	papers 86:12	parttime 6:4
online 9:17	131:21 138:13	79:3 116:18	111:11	passed 142:1
open 17:17 18:6	opportunity	136:2,3,5,12	paragraph	pat 18:22 22:12
18:10 49:14,15	33:5 91:14	136:22 138:15	12:21 13:2	23:16 28:17
52:12 55:12	opposed 40:2	138:20 141:8	part 13:20 37:4	36:21 42:17
60:10 62:10	51:15 109:1	141:19	38:15 42:3,14	49:8 84:10
65:3 69:3,14	111:5	outsiders 138:13	43:10 59:7,8	87:7 90:2

patricia 2:5 5:17	permitted 17:15	place 12:12 66:9	policeman 46:19	precedential
patrick 2:17	person 12:2,14	67:1,6 72:15	policies 6:13	125:4,6
10:7	13:1,4 27:11	76:16 79:12	policy 3:5 66:9	precise 41:3
patriot 1:8 2:10	37:9 67:2	89:17 92:16	115:14	precisely 38:14
7:8	69:11,12,16,19	95:7 115:14	polls 56:13,13	predicate 76:15
pats 73:3	71:21,21 73:20	121:7 134:11	portions 124:5	predicated
patterns 19:6	82:21 95:4	140:1	pose 8:5 9:8	126:8
pclob 5:6 6:1,16	107:14 112:3,5	places 112:5	posit 22:22	predictive 90:7
7:5 9:15	122:15 132:20	platforms 87:11	position 8:12	predominant
pell 3:21	133:11,17,18	play 118:14	31:8,20 34:5	84:4
people 20:7 24:7	134:6 139:16	plays 58:22	80:21 90:21	preliminary
39:7,16 44:9	personal 54:2	please 10:22	123:7	17:16,22 49:15
53:9 61:6	69:6	plethora 52:15	positioned 13:1	premise 70:16
68:22 79:12,12	personally	pllc 3:9	positions 73:10	102:10 133:13
84:2 88:11	124:10	plot 15:5,13	86:13 121:22	premised 75:14
96:4 106:4	personnel 68:10	39:2,4	possession	prepared 98:8
115:10 125:20	105:7	plots 35:19	25:13,14	prepatriot 84:7
131:16 132:14	persons 46:22	plotting 34:14	possibility 48:9	present 5:14
135:4	65:18,22 66:3	point 12:15	possible 7:4,22	73:16 74:4
perceive 113:12	67:10 68:3,4	13:22 14:2,10	8:10 55:13,17	81:16 123:10
perceived	68:19,20 69:7	22:12 25:8	58:1 75:9	125:18
105:18	69:9 70:11,22	29:11 34:7	93:21 94:1	presented
percent 128:11	71:8 95:19	35:8 38:10	95:3,10 101:13	114:19 129:18
129:4,4	121:17 132:13	46:5 50:22	111:19 115:15	presenting
percentage 88:4	133:14 136:7	51:1,2,17	118:10 122:20	125:21
perception 96:8	141:6,12,18	57:16,18 59:4	124:9	preserve 63:5
96:10,16 131:3	perspective 15:9	63:10 66:22	post 65:12 91:19	85:20
perdue 4:5	76:17 82:19	74:10 86:19	posted 9:15	president 3:18
perfect 22:1	88:2 131:13	93:22 97:7	postquery 51:19	7:6 117:7
perform 132:7	pertain 82:6	106:7 114:8,22	potential 14:21	presidents 55:4
period 23:15,22	pertains 80:15	115:3 122:7	112:2 141:20	presiding 5:12
24:2,8 29:19	phone 18:21	133:2 139:5	potentially	press 10:12
33:14 40:22	19:5,11,12	pointed 107:20	54:19 101:10	11:13
72:14 91:16	32:12,14,15	115:19 126:10	power 80:15,16	presumably
99:15,15 118:6	45:14,16 49:2	pointing 112:1	80:17,19	19:1 75:3
118:7 119:11	61:13 62:1	points 11:7 14:3	powerpoint	96:14
119:21 120:5	106:14 110:14	36:11 38:1	97:3,14	presume 76:4
periodic 89:20	113:4,7,8,8	62:13 72:2,9	powers 67:21	presumption
periods 22:7	118:20	89:12	practical 18:18	82:20
55:17	physical 51:16	police 33:11	61:20 62:2	pretty 137:1,20
permissible	52:8 113:22	44:7,10,13,16	63:5 76:2	138:4
86:16	pick 10:3	46:14 47:7	123:12 124:21	prevent 16:2
permit 9:12	picked 44:21	48:2,8 51:8,20	practically 82:2	20:8 81:12
110:5	piece 118:18,19	79:7	practice 35:11	prevented 36:21

preventing 16:11 20:6	74:4 77:5,16	15:20 16:11,17	7:7 8:1,17 11:2	protections 62:19 67:1,5,6
prevention 82:22	procedure 95:15	18:7,15,17	11:10 26:5	67:10 68:4
previously 82:11	procedures 12:10 72:14,17	19:4,7,16	33:8 36:9,10	69:9 72:10
primarily 14:19	94:8 106:21	20:20 21:2,4	37:19 38:7	132:21,22
17:2	120:22 133:21	22:13,13,19	54:11 61:8	134:3,11
primary 6:6	136:11 138:5	26:4,10,14,19	89:3,8 90:8,19	protects 55:7
principal 3:21	proceed 5:22	27:1 29:12	94:4 108:20	provide 7:5
privacy 1:3 5:3	122:7	34:9 35:10,13	112:16 116:17	16:19 17:7,21
6:10 12:2	proceeding	36:4,12,13,17	116:20 117:1,4	59:20 63:15
22:21 23:5	122:3	36:22 37:4,13	119:6 121:17	67:14 76:6,19
24:11,14 25:6	proceedings 5:1	37:20 38:2,6,8	122:16 129:14	79:17 85:13,18
25:10 26:7	23:8,9,9	38:12,14 39:22	project 10:16	102:3 131:17
46:22 62:19	process 23:10	44:7 46:15	proof 31:7	131:20
72:10,16 89:4	30:14 31:2,3,4	48:13,13,14	proper 70:18	provided 22:14
111:16 112:14	33:7 42:16	52:13,14,22	142:2	30:15 39:1
112:15 113:12	49:18 52:7	53:1,6,11,13	property 3:11	88:5
115:20 116:9	55:19 62:6,6	53:16,18 54:8	proposal 13:16	provider 19:18
116:22 121:13	66:9,9 85:8,21	54:9,19 55:14	65:5 73:18,18	19:19,19 20:16
121:20 122:13	89:20 92:15	56:1,5 57:3,5	74:6,12 82:19	20:16,21 42:21
123:11 138:18	95:10 117:13	57:13 58:5,12	125:16	42:22 43:1
private 9:3 24:4	118:22 121:16	58:22 59:4	proposals 13:11	65:16 74:13,14
24:6,9 25:15	122:3,8,19	60:2,6,11,12	56:7 73:3,5,10	74:18,19 87:18
86:3 97:10	123:9 124:11	60:15 61:10,12	73:13 86:7,20	providers 7:19
proactive 29:22	124:18 125:11	61:18,19 62:7	88:15 89:1	18:20 21:14,16
75:4,10	126:9,16	62:15 63:6,13	120:1 126:7	22:5 42:19,20
probable 47:18	127:17 130:7	64:7 65:15,16	131:1	43:6,9,14 96:1
75:14 134:22	135:21 137:12	65:21 66:5	proposed 101:2	96:7,14 99:9
probably 15:6	137:14	69:10 77:7,21	proposing 81:12	99:14 119:7
15:17 22:11	processed	81:11 82:12	prosecutor 4:1	138:14
41:20 90:10	135:16	88:17,18,21	70:8	provides 16:18
96:21 97:6	produced 38:21	90:6 92:17	prosecutors	17:9,10 19:7
98:7 118:15	39:18	93:13 97:16	47:22	19:16 91:13
119:12 122:22	productive 49:5	98:19 100:22	protect 6:8,10	125:12
140:17	professionalism	101:17 102:7,7	6:14 68:20	providing 55:21
problem 35:4	130:9	102:11 104:15	93:7	87:9 96:3
45:20 78:13,15	professor 3:16	105:15 107:21	protected 25:13	123:17
87:6 96:22	4:2,6	110:16 111:13	110:13 113:3,9	provision 58:14
129:5	program 7:8,9	114:7 115:8,16	116:10	58:16 80:3,9
problematic	7:10,11,13,17	117:19 126:17	protecting 69:6	80:21
125:22	9:14 11:1,3	132:12 134:19	protection 23:19	provisions
problems 73:16	13:9,12,13,17	134:20	26:8 66:2	37:16 75:6
	13:20 14:1,4	programmatic	67:15 68:2	136:22
	14:12,14 15:18	40:13	121:7 125:12	proxies 61:6
		programs 1:7	133:7,16	

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	26:10 27:3,19 29:19 30:5 61:5 66:4,19 73:21 106:20 131:19 pursue 46:2 61:22 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 putting 86:15 113:18	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	25:9 63:3,9 71:17 73:1 117:18 121:12 133:13 raises 69:22 104:12 raj 16:18 33:22 35:6,17 41:22 48:4 49:7 50:22 65:11 68:3 69:2,21 69:21 84:21 94:7 120:20 126:14 127:12 129:22 rajesh 2:15 10:6 rajs 59:18 ran 20:13 range 8:9 13:12 90:19 95:2 rapid 34:9 36:19 rare 15:13 rarely 88:2 ras 27:17 28:4,8 28:18 29:1,15 29:16,18 30:1 30:3,4,7,10,11 30:19 31:3,4 32:6 33:18,21 34:1,18 35:4 43:22 44:12 49:9 55:20 61:14 62:3,4 63:7,15 64:17 65:12 75:21 76:6 77:4,17 78:10,16,20 79:4,13 97:19 120:14 133:5 134:16,19 136:8 139:2	rational 90:16 98:15 99:16 139:15 raw 26:1,12 reaction 34:9 116:19 139:3 read 12:16,17 13:6 57:8 81:5 111:10 139:12 reading 97:13 real 34:3 realities 119:17 reality 76:2 96:8 realize 17:5,8 really 31:11 32:20 51:4 60:14 70:4 91:6 112:3 115:1 119:16 129:6,8,15 138:16 reason 23:7 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 reasonable 27:5 28:4 31:15 44:2 56:8 61:14 79:8 89:6 116:12,12 135:4 reasonably 132:13 133:15 139:17 reasons 22:6 48:3 65:11 82:10 93:15 reauthorization 30:14 reauthorizatio...
publicly 14:3 39:1 53:19 64:13 68:9 90:6 122:6 128:10	quantification 98:3,4 quantity 110:10 queried 106:2,4 120:13 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	questioning 9:9 24:16 questions 8:4 9:8 20:13 28:5 33:6 39:20 53:14 88:14 132:9 139:11 142:8 quick 49:6 116:16 quickly 17:10 quite 85:12 101:19 118:18 140:16,22 quorum 5:15 quote 52:15 105:7 108:2,21 128:19	rapid 34:9 36:19 rare 15:13 rarely 88:2 ras 27:17 28:4,8 28:18 29:1,15 29:16,18 30:1 30:3,4,7,10,11 30:19 31:3,4 32:6 33:18,21 34:1,18 35:4 43:22 44:12 49:9 55:20 61:14 62:3,4 63:7,15 64:17 65:12 75:21 76:6 77:4,17 78:10,16,20 79:4,13 97:19 120:14 133:5 134:16,19 136:8 139:2 rate 129:4,5 130:15 rational 98:16	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
published 103:21	quantification 98:3,4	questioning 9:9 24:16	rapid 34:9 36:19	reason 23:7 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
punt 117:5	queries 27:4,5 30:10 55:18 68:18 82:7 106:1,12 121:5	questions 8:4 9:8 20:13 28:5 33:6 39:20 53:14 88:14 132:9 139:11 142:8	rare 15:13	reasonable 27:5 28:4 31:15 44:2 56:8 61:14 79:8 89:6 116:12,12 135:4
purely 26:15	query 27:16,18 28:19 29:7 76:15 106:5 107:7,8 118:20 120:11 134:5 134:14	quick 49:6 116:16	rarely 88:2	reasonably 132:13 133:15 139:17
purged 77:18	querying 134:1 135:1	quickly 17:10	ras 27:17 28:4,8 28:18 29:1,15 29:16,18 30:1 30:3,4,7,10,11 30:19 31:3,4 32:6 33:18,21 34:1,18 35:4 43:22 44:12 49:9 55:20 61:14 62:3,4 63:7,15 64:17 65:12 75:21 76:6 77:4,17 78:10,16,20 79:4,13 97:19 120:14 133:5 134:16,19 136:8 139:2	reasons 22:6 48:3 65:11 82:10 93:15
purpose 7:21 8:8 26:14 45:5 66:16 71:7 82:5 100:18 114:15 133:4 134:15	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	quite 85:12 101:19 118:18 140:16,22	rate 129:4,5 130:15	reauthorization 30:14
purposes 7:14 24:17,21 26:15 26:16 58:19 66:21 71:3 99:6 107:15 115:8 138:18	quorum 5:15	quote 52:15 105:7 108:2,21 128:19	rational 98:16	reauthorizatio...
pursuant 1:7 7:15 21:19	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quorum 5:15		
	querying 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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	quote 52:15 105:7 108:2,21 128:19		
	quoting 134:1 135:1	quote 52:15 105:7 108:2,21 128:19		
	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			

89:15	reference 46:5	relating 60:2	26:22 51:22	47:17 99:1
reauthorized	96:12	108:13	63:11 64:16	135:19
26:19 30:8	referred 7:10	relationship	75:5,12 77:17	requiring
36:14 37:20	41:13 94:7	95:22 96:6,9	122:1 131:3	119:19
52:1 57:4	97:17	96:10,17,20	reported 1:22	requisite 17:21
58:14 140:9	referring 50:3	97:10	35:5,5 106:2	research 3:16
recall 122:4	96:13,17	relative 74:17	reportedly 91:2	4:4 112:1
receiving 5:21	112:20	115:19	reporting 62:2	reservation
recognize 83:21	reflect 129:5	relatively 25:2	63:10 78:8	101:9,10
111:18	reform 59:1	released 55:2	89:21	residents 53:17
commendat...	reforms 52:15	68:8 123:21	reports 38:22	resigned 68:22
1:6 7:22 8:9,12	52:15,18 53:9	124:6 129:10	39:17	resolve 45:4
record 20:18	55:13	relevance 37:7	represent 8:6	resolved 44:15
22:7 23:1 51:5	regard 68:5	81:18 84:8	representing 9:3	44:19 46:3
98:7 100:1	95:16 107:2	101:2,8,12	represents 77:1	resource 38:4
113:6 118:20	115:18	102:8,21,22	127:2	resources 17:16
126:11,19	regarding 8:1	108:3,16	repression	18:3 65:10
128:19	119:5	relevancy 42:4	67:22	respect 6:18
recorded 9:14	regardless 26:6	relevant 37:4	request 100:15	55:5,11 67:16
records 7:11	36:10 37:16	80:12 83:14,14	100:17 119:11	70:6 74:5 82:8
20:22 21:12,18	regime 86:17,17	84:13 100:4,6	122:4	85:17 99:8
22:17 23:3,4,7	register 5:11	102:17 104:6	requests 85:2	107:4 110:18
23:14,18 26:1	regular 76:5	109:5 130:14	101:14 119:9	123:1 125:1
29:14 37:8	84:1,14 105:4	132:4	120:16	respond 9:6
40:8 57:8 82:8	127:4,7,8	reliance 30:14	require 21:1	17:10 77:19
83:11 84:5,11	128:16	relief 77:20	23:20 48:17	response 13:16
84:12,15 85:12	regularized 40:5	reluctant 73:9	73:14 106:8	36:20 39:20
99:1,2 103:20	regulated 26:5	rely 92:8 111:13	required 22:4	73:3 120:8
recounting	26:10 52:7	remains 112:19	48:18 59:20	responses 9:12
90:22	regulation 21:11	113:13	60:2 61:3 70:7	responsibility
redactions	21:19 22:5	remedial 56:18	74:12 138:6	8:16
124:13	regulations 6:3	77:22 79:18	requirement	responsive
reduced 41:1	6:13 9:18	remember	20:18 23:1	132:1,2
reducing 83:16	20:22 21:10	48:12 78:20	69:15 75:21	rest 10:4 127:9
119:10	reingold 7:2	renaissance	80:1 94:11	131:11
reevaluate	reiterate 69:2	1:16	137:21	restricted 119:8
37:18	related 6:14	renewal 119:18	requirements	restrictions 56:4
reevaluated	20:13 66:16	renewals 89:13	22:4 36:18	100:12,19
89:9 114:6	108:6,11 109:3	rental 84:12	63:11 78:1	106:11
reevaluating	132:10	repeatedly	89:21 95:17	restrictive 104:4
38:6	relatedly 22:2	41:19 42:17	123:17 125:8	restricts 120:15
reevaluations	23:6	55:12	129:20 135:15	result 15:15
89:20	relates 21:11	repeating 83:4	139:15	20:5 56:15
reexamines 30:1	70:10	report 7:6 8:18	requires 47:14	59:7,8 69:1

134:4	140:4	rounds 9:10,10	scholarship 4:7	4:4 10:7,11
resulted 17:12	reviewed 50:11	routinely 41:21	school 3:17	16:1 19:10,10
results 97:20	63:20 66:4	50:8	science 4:2	25:9 42:8,12
106:12 107:7,9	140:20,21	rubber 129:8	scoop 103:10	85:20 94:16
resume 142:14	reviewing 34:18	rule 48:16 64:11	scope 13:14	95:6 127:2
resumes 122:4	50:21 137:12	70:16 133:3	71:18	128:3 132:6
retain 43:15	reviews 35:6	rules 12:12	scrutinize	see 19:6 20:9
70:21	50:8	27:20 68:20,21	129:16	32:15 34:12
retained 21:19	revolution 91:3	69:5 70:20,22	scrutiny 25:7	38:8 43:1
23:7 40:21	right 15:7 32:2	104:12 105:13	seam 14:6	50:12 58:22
43:13	34:11 35:20	105:14 106:22	search 46:7 52:8	61:1 91:18
retains 13:4	36:1 46:5	136:13	69:18 71:12	96:19 101:19
retention 12:13	77:15 79:11	run 22:13 41:4	108:17,20	117:14 129:11
20:18 22:4,7	85:7 92:12	46:15 82:14	109:17 116:13	seeing 75:8
23:1 55:16	101:7 105:8	97:18	125:14 133:1,3	93:19
67:4 72:14	107:11 109:14	running 46:22	searched 98:1	seek 25:1 80:14
94:9 95:12	117:12 121:9		132:19 136:7	123:9
118:6,7	132:21 134:13	S	searches 97:18	seeking 83:2
retroactively	135:22 136:9	s 3:6 12:1,14	searching 69:15	117:9 126:16
15:22	138:16	13:1,4 27:11	98:1	seen 22:7 96:12
return 75:20	rights 65:22	29:20,21 32:15	second 8:21	112:20 113:14
79:22	69:17	65:18,22 66:1	19:14 21:16	116:18 119:18
returned 80:3	rigor 12:18 13:6	66:3 67:2,10	41:15,18 45:2	126:8
revalidate 37:13	126:10 127:16	68:2,19,20	45:7 47:4 54:6	segments 105:19
reveal 117:20	127:19	69:6,9,11,12	76:12	segregate
revealed 53:3	rigorous 52:7	69:16,18 70:22	secondly 44:13	104:10
128:10	89:9 128:20	71:8 73:19	66:15	segregated
revelation 52:13	131:12	95:4,19 107:13	secrecy 53:13	26:12
revelations	risk 50:16 55:9	111:20 132:19	54:7 59:8	seize 103:14
25:11 56:15	91:9	133:10,14,17	120:3	seized 70:14
reverified 30:16	risks 91:9	133:18 134:5	secret 52:13,22	seizure 116:13
30:18	124:12	136:6,6 139:16	53:3 54:10	selection 61:13
reverse 133:18	robert 2:19	141:6,12,18	81:9 93:7	selective 96:22
review 3:5 6:7	rogers 125:10	safe 17:19	secretly 10:13	selector 30:7
34:1 40:14	role 6:17 57:21	saying 35:18	section 1:8,9	31:5 45:10
47:9,9 49:8,9	62:10 121:17	83:14 92:4	2:10,11 3:11	78:16
49:18 55:20	121:22 132:5	99:19 137:9	7:7 71:5 75:15	selectorbased
62:4,6 63:16	rotating 127:10	sayings 104:1	75:16 80:1	140:15
64:1,6 65:12	127:13	says 12:22 13:3	85:6,17 88:17	selectors 61:16
78:10 79:6	round 28:6	68:3 73:19	90:6 98:22	75:21 76:6
95:18 97:1,3,3	71:14 88:15	91:20 92:4	sector 9:3 24:9	78:21 97:19
128:4,21	94:7 104:17	schedule 89:10	25:15 86:3	semiannual
129:12 130:2	116:16 117:18	scheme 64:9	secure 57:2	131:3
138:20 139:21	137:18	scholars 12:3	security 2:14,15	senate 130:11

131:14 132:7 senator 68:7 sending 131:16 senior 3:6 27:4 57:22 sense 24:6 51:5 52:2 71:10 81:15 82:20 94:18 117:6 sensitive 55:8 61:7 117:14 sent 68:7 separate 59:2,10 102:19 124:4 separately 58:18 121:21 september 5:11 sequential 41:14 41:14 series 28:5 serious 36:3 52:19 seriously 124:7 serve 67:6 served 74:15 122:19 service 7:19 19:18,18,19 20:21 65:16 74:13,18,19 96:1,7,14 99:9 99:13 services 88:4 96:3,3 132:3 session 142:11 set 29:19 61:3 64:10 101:16 104:9,10,11 121:3 124:1 125:11 setting 72:6 79:11,16,22 94:19 135:18 137:4,5,10	140:18 setup 58:7 seven 27:9 shaken 59:7 share 6:21 shared 113:4 sharon 6:22 shift 65:14 87:17 shining 54:4 short 99:14 shorter 40:21 55:16 72:14 shortterm 138:3 show 104:3 showing 37:7 84:14 100:2,6 shown 138:3,10 shows 128:19 shut 13:17 82:12 side 9:2 16:1 19:11 24:15 87:19 133:1 sign 91:20 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 signing 130:12 silicon 10:21 similar 39:5 90:7 simply 11:16 13:17 21:5 30:14 46:22 56:8 126:18 single 28:18 34:18 39:7 44:11 97:4 127:16 139:22	140:5 site 14:18 sitting 32:21 127:9 situated 126:15 situation 15:14 32:13 39:22 114:18 136:1 situations 112:14 six 68:8 skp 3:21 slower 20:1 42:15 small 106:2 130:6 smith 111:14,17 111:22 112:12 112:22 113:3,5 113:15 snap 123:20 snowden 25:22 socalled 97:21 130:15 138:8 solving 15:22 somebody 28:18 46:8 79:1 91:19 92:22 somebodys 70:14 soon 91:4,6 121:15 sorry 11:5 16:13 21:22 42:9 59:16 109:7 135:11 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 sorts 38:7 70:9 125:7 sought 23:8 sound 57:11 sounds 75:22 sources 60:19 60:22 spafford 4:2 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 speaking 47:21 71:2 72:3 74:5 123:6 124:9 140:16 special 104:12 124:19,21 125:1 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 specifically 101:18 specificity 74:22 specifics 40:11 spectrum 39:15 spike 87:15 spinning 115:11 sponsors 81:9 spouse 25:3	squarely 64:22 stage 95:10 135:20 stake 116:6 stamp 129:9 stand 61:6 136:20 137:2 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 standards 31:7 48:11 109:14 120:12 127:5 standing 125:1 standpoint 72:4 start 11:4 14:12 43:7 66:6 87:6 90:22 98:13 133:12 139:7 142:5 started 9:21 10:1,2 16:16 35:18 70:8 starts 87:9 stasi 67:20 state 24:20 73:9 statements 118:14 states 32:17 34:12 45:17 46:9 48:22 49:5 67:14
---	---	---	--	---

69:13 91:21	streams 14:8,9	subsequent 47:8	81:5,14,20	54:1,15,22
105:2 132:15	14:22 43:6	118:22	85:13 86:15	69:20 70:5
136:3,4,5	street 28:18	substantial 74:2	90:11 92:11	74:7 75:10
137:1 141:9,19	31:13,17 33:12	subway 39:3	104:13,14,21	77:21 88:6
status 50:12	33:20 46:20	success 117:21	129:16 131:10	91:15 95:8,9
statute 11:19	49:21 50:10	sudden 87:13,15	surrounded	97:7 98:6
59:19 85:4	strictly 100:9	sue 7:1	133:7	101:16 112:12
101:15,18	strike 138:16	sufficed 118:3	surrounding	114:11 119:12
102:3,10	stringent 105:14	sufficient 79:8	133:9	119:16 124:7
129:20 131:19	106:9 107:6	sufficiently 29:9	surveillance 1:7	142:13
135:19	strong 116:19	suggest 11:11	1:10 2:11 3:2	taken 59:1,5
statutes 102:1	structured	15:12 59:6	7:16,20 8:3,17	75:11 116:21
statutory 64:10	98:20	135:3	8:22 11:16	takes 6:8 140:1
64:11 86:17	studies 114:10	suggested 18:18	14:5 26:21	talk 22:2 35:19
100:9 101:5	study 40:10	52:15,16,18	58:13 65:19	48:20 79:21
138:2	118:8	53:9 56:21	85:4,5 88:12	103:22 126:15
step 70:5 141:9	subject 8:18	112:13 124:19	96:15 117:4	126:15 131:7
141:17	11:2 13:9	138:19	134:2 140:13	talked 55:16,17
stephanie 3:21	20:14 56:2	suggesting	142:15	55:19,21 64:4
stephen 4:6	61:10 65:19	56:14 96:20	surveilled 65:22	112:21
steps 54:15	67:6 70:11	112:9	susceptible 83:9	talking 33:10
75:10 77:22	84:20 97:21	suggestion 31:1	suspected 17:19	74:11 78:21
95:9,9 116:21	105:3,12,13,22	31:9 138:6	31:17 80:16,18	83:9 84:10,22
118:22	106:5 108:13	summarize	suspend 77:20	94:21 105:9
stevenson 3:16	109:5 120:21	62:17	77:21	116:2,3,4
stick 93:5	125:13	summer 122:2	suspicion 27:6	130:11 141:5
stop 28:10,12,16	subjects 19:6	sunset 131:5	28:4 31:16,22	talks 85:5
31:16 36:15	67:3	sunsets 37:15	45:3 61:15	tangible 99:21
44:7,13 45:5,6	submit 37:1	supercede	79:9	target 69:10
46:14,19 47:8	submitted 9:17	106:21	swallows 64:11	71:15,16 85:3
48:8 51:6,7,9	66:20 128:12	supervision	syllogism 93:11	94:15 133:14
51:12,15,18	subpoena 19:9	7:20	system 21:14	133:17,18
52:4 79:9,20	20:16 23:17	supervisors	34:9 39:3 42:5	139:16 140:11
stopped 15:15	24:5 82:4	50:12 51:12	106:5	targeted 84:5,15
38:20 44:18	103:7	support 30:20	systematic 36:4	targeting 71:20
94:13	subpoenaed	79:9 119:10	40:4 47:22	138:3,17 139:8
stopping 46:20	24:4	123:5 124:17	48:5	139:15 140:1,5
stops 44:12 48:2	subpoenas	supreme 23:19	systems 41:22	140:8,9,15,19
79:7	41:11,14 42:16	111:22 112:21	50:20	141:2,6,18
store 97:18,21	43:8	sure 21:8 23:13		142:6
98:5 120:9	subscriber	25:16 35:1	T	targets 12:5,6
stories 117:21	14:17 115:9	36:9 57:17,20	tailored 101:18	75:7,13 85:5
story 91:1	subscribers 87:5	58:10 62:7	take 9:20,22	85:19
strategies 3:21	87:21 88:3,4	66:12 77:10	23:11 25:19	tasking 138:8,21

technical 27:13 27:16 94:20 95:1 129:17	40:15 82:22 92:6 116:1,4	74:6 78:11 80:7 81:17 82:9,22 85:9 85:14 86:11 87:15,16 89:22 90:10 91:5,16 93:14 94:11 97:6 101:15 104:6,7,17,22 106:1 109:5,22 110:12,15 111:12 114:15 115:15 117:13 119:2 120:10 121:6 128:14 129:3 133:22 134:20,20 137:1 138:3 140:2	38:8 43:17 54:12,17 59:11 81:12 87:9 94:8 127:8,9	55:12 56:12,17 57:2,16 58:4 58:20 59:2,4 59:12 60:8,14 60:17 62:10,14 63:4,9,22 64:13 65:2,5 66:2,6 67:13 68:1,5 70:4 71:10 72:2 73:11,13 75:8 77:8 78:19 79:1 81:6,8,9 81:11 82:5,9 82:18 83:7,8 83:21 85:2 86:7,19 87:19 88:1 89:6,21 90:4,13,20 91:5 92:21 93:8,10,19,22 94:1,11,21 96:21 97:5,12 99:10 100:8,10 101:22 102:4 102:10 103:1,3 104:2 107:19 109:8,15,20 110:20,22 111:8 112:19 113:13 114:1,9 114:17,17 116:11,13,15 117:11,13 119:19 120:2,7 120:18 121:6 121:15 122:4 122:11,14,18 123:7,14 124:7 124:20,22 125:3,9,15,16 125:16,19 126:7,13 128:10,16,18
technicalities 99:19	terrorist 16:2,11 17:19 27:7 32:1,8,10,11 34:14 45:11 46:9	themes 90:3,3 theoretical 22:9 theory 31:5 69:16 thereof 11:6 theres 15:4 18:15 31:15,21 32:11,15 34:14 35:18 37:12 38:11 45:3 47:15,21 48:3 49:8 54:18 56:14,17 57:6 64:15 65:17 68:15 69:4 71:3 77:8 86:2 89:6,11 92:4 97:17 99:20 103:19 105:18 115:9 116:19 119:4 121:1 124:22 125:3 131:3 134:13 134:18 theyre 31:17	theyve 54:17 112:6 129:13 thing 16:3 24:15 38:3 46:2,16 47:4 48:12 49:6 73:22 74:3 75:3 94:3 94:5 97:17 104:21 122:9 125:15 129:10 things 7:12 12:4 18:14 21:1 25:1 35:14 56:7 61:4 62:16 65:4 72:22 73:14 74:2 93:7 97:4 99:21 103:20 115:13 117:7 121:14 129:6 130:16 141:14	
technological 108:4,17,19,22 109:16 110:22	terrorists 45:14 49:2 125:12			
technology 109:10 111:4 113:11	terry 28:10,12 44:1,22 45:2 46:4,14,19 47:7 48:2,8 51:6 52:4 79:7			
telecommunic... 74:14	test 104:4 107:10			
telephone 7:13 14:11,14,15 17:3 18:19 29:4 37:8 46:22 47:2,12 51:10 73:20 99:4 105:1,20 111:14	testimony 118:5 thank 6:19,22 20:11 21:20 33:1,3,4 43:19 52:9,11 54:4 72:19,21 77:13 84:21 107:17 121:9,11 126:1 132:8 137:17 142:9,16			
telephony 98:16 100:18 101:17 102:7	thanks 43:21 69:21 95:21 104:18			
tell 73:19 79:21 91:4,6 121:14 127:15	thats 15:6 16:2 20:19 22:1 23:21 24:3,3 24:10 25:17 28:16 32:8,13 32:18,19,20 33:13 34:5,14 35:20 37:17 38:13 39:3 42:9 43:9 44:6 47:1 48:3,18 48:22 56:22 60:7,19 64:10 65:2,6 68:1 70:4,17 71:21			
tells 127:12				
template 101:3				
ten 9:9				
tend 62:16				
tent 54:3				
term 97:5				
terms 11:9 15:17 22:3 27:18 37:10 40:13 48:9 59:18 72:9 76:12 85:1 98:1 103:22 115:7 118:16 121:5 123:2,16 129:6 135:15				
terrorism 6:8,15				

129:2 130:8	137:15	33:15,18 35:14	twopart 35:22	69:9 71:14
131:1,2 134:10	times 90:14	transcript 9:15	type 12:1 32:13	79:13 80:11
134:21 135:2	tipped 46:1	translates 94:16	40:18 41:15	85:3 90:12
136:10 137:4	47:12	transparency	60:6 83:8	92:11 97:19
138:1 140:12	tips 14:22	55:5,22 56:7	90:19 95:15	104:21 105:3,7
141:16,19	tireless 7:4	73:5 75:4,10	136:8 138:3	112:20 129:17
142:1,4	title 70:12,13	75:18 87:20	types 26:12	130:5,13 133:2
thinking 44:1	87:14,15 94:13	119:5 123:2,16	56:19 83:10	134:7 137:8
89:22 94:3	127:22 128:16	transparent	85:2 117:4	138:5 139:13
thinks 37:16	today 8:5,14	85:14 93:21	134:10 136:19	140:4 141:7
third 9:4 19:15	26:5 33:4 53:5	transportation	typical 94:12	understanding
38:3 41:15,18	63:17 67:11	16:14	typically 33:14	21:9 99:13
47:19 62:21	76:13 90:4	treated 72:12	typo 27:15	102:16 105:4
66:22	93:12,16 97:22	137:3	128:13	132:15
thought 33:15	98:8 121:19	tree 97:19		understood
77:22 91:3	122:11 139:9	trends 112:13	U	107:16
thoughts 65:20	today's 6:20 7:21	trespass 113:17	u 3:6 12:1,14	undertaken
98:22	11:2 13:9	tried 118:9	13:1,4 27:11	12:7 95:19
thousands 78:21	told 24:18	119:1	29:20 32:15	underway 85:21
78:22	tolerable 139:5	true 12:17 33:11	65:22 66:1	undesirable
threads 115:11	toll 21:11,18	91:5,12 93:14	67:2 68:2 69:9	60:9
threat 14:7,9,22	23:2,3	try 16:8 19:20	69:12,16,18	unearth 14:20
three 8:14 26:19	tool 14:19,20	43:7 81:8 82:7	70:22 71:8	unearthed 15:15
40:6 81:22	15:5,16 16:5,6	93:20 94:17	73:19 95:4,19	unhappiness
92:16 118:2,6	16:6 29:9,10	trying 49:1,3	107:13 111:20	105:19
118:15 119:3	36:19 40:18	75:9 111:2	132:19 133:10	unintended 8:10
threepart 36:5	48:19 122:17	136:15	133:18 134:5	united 32:17
thwarted 35:20	tools 14:5 15:10	turn 13:8,21	136:6,6 141:12	34:12 45:17
40:14	17:4,4 41:6	17:7 18:2	unanimous 5:21	46:9 48:22
tier 19:12,14,15	108:4,18,19,22	28:13 54:3	unauthorized	49:5 67:14
ties 14:21	109:18,21	61:9	92:19	69:12 91:21
time 17:11 18:9	110:3,5	turning 69:8	unclassified	105:2 132:15
18:13 20:9,13	top 107:8	87:4	124:5	136:3,4,5
23:15 24:1,9	tracing 49:21	turns 36:5	unclear 13:3	137:1 141:8,19
29:19 30:2,15	track 117:19,22	twice 37:20	76:1	university 3:17
30:18,19,22	tracking 50:1	58:13,14	uncomfortable	4:5,8
34:3,16 40:22	113:20	two 6:16 7:6 9:1	64:9	unknown 29:11
41:10 43:16	traditional	9:7,11 12:22	uncover 46:8	unquestionably
54:22 55:8	108:6,10 109:1	20:3 23:2	undermine	91:11
75:19 85:19	traditionally	26:14 40:6	11:14 96:16	unquote 128:19
91:16 92:15	94:8,13 125:8	44:4 53:7,10	underside	unrest 105:18
99:15,16 111:9	trail 29:14	55:2 59:10,11	113:20	unusual 70:5
116:15,16	120:16	87:3 100:8	understand	updating 137:12
123:4 124:11	training 33:14	121:14 122:22	31:12 61:11	upwards 128:11

urged 9:11	118:11,16	140:6 141:1,7	94:14 102:18	whats 30:13
urgent 61:22	134:8	141:11	way 17:9,10	85:18 87:20
usa 1:8 2:10 7:8	variety 55:13	wall 92:4	19:22 22:14,18	91:9 98:10
use 12:13 18:22	62:16 97:7	walton 124:2	36:4 40:5	110:10
19:9 20:15	115:5,13	128:5	44:10 45:11	white 103:21
27:1 41:11	various 53:9	want 6:19,22	46:6 49:21	107:20 115:18
42:7,12 49:10	75:6 87:1	10:2,5 13:8	50:21 72:11	whos 10:6,7,9
49:12 52:5	varying 8:16	20:7 23:12	76:4 79:6 84:5	25:2 31:13
58:16 71:6	vast 13:1	24:20 28:3	85:9,15 123:1	80:17 83:15
74:18,18 84:4	vehicle 63:14,14	33:9 34:11	132:22	124:2,10
94:9 95:11	113:20,21	51:1,5 53:11	ways 19:4 89:2	wide 8:9
97:13 99:6,11	veracity 11:5	54:8 56:3,5,18	117:15	widespread
100:13,18	version 124:18	59:17 65:14	weapon 92:5	56:14 107:22
108:22 114:15	viability 30:11	67:9 69:20	wed 19:12 20:4	wiegmann 2:13
114:16 117:21	victims 39:11,12	72:21 75:17,19	20:4,5,6 64:9	10:9 23:13
121:1 133:4	39:12,17	81:10 84:11	92:22 100:6	31:11 33:22
138:2	view 13:22 14:2	85:13 92:8,12	119:12,22	42:14 65:8
useful 13:5 40:9	57:21 112:17	92:13 97:2,8	week 10:13	77:3,11,14
48:19 54:19,21	116:18 118:9	100:17,19	118:4 122:5	78:8 80:4
63:14 72:6	119:15 139:5	103:8,10	125:11 127:14	81:19 83:20
85:14 141:2	viewpoint 87:20	104:20 106:17	weekend 81:5	103:2 107:13
usefulness 62:15	views 6:21 8:6,6	114:20,20,21	weeks 56:16	109:9,14
uses 11:14 72:7	9:13 117:12	114:22 126:22	65:17 68:8	110:22 112:19
usual 108:1	violation 68:16	129:2,22 130:1	137:7	120:2 126:20
usually 108:10	virginia 16:14	142:9	weigh 15:19	willful 68:16
utility 55:15	visits 115:12	wanted 33:4	welcome 5:5	willfully 133:17
56:5	vladeck 4:6	35:16 41:8	9:17	willing 118:5
<hr/>	volumes 83:11	80:9 86:1	wellsupported	wilson 3:19
V	voluntarily	98:13 100:22	130:19	win 126:11,18
v 111:17,20,22	43:15 113:7	104:9 107:12	wellversed	128:19 129:4
112:12,22	vs 44:1	120:7 122:21	14:13	130:15
vaguer 45:9	<hr/>	wants 23:11	weve 14:3 18:5	wire 130:20
valid 29:18	W	32:16 53:22	22:2 26:16	wiretap 70:12
57:18 89:6	waiting 9:19	warrant 47:18	31:2 32:2	70:13 127:22
validation 64:21	wald 2:5 5:17	48:15,16 69:14	38:19 40:11	wiretaps 80:2
validity 79:7	52:10,11 56:10	71:12 125:8	45:13 49:1,2	wondering 45:7
valley 10:21	57:17 59:15	127:21 128:1	55:16,17,19,21	46:4 78:7 80:8
valuable 14:4	60:4 104:19,20	warranted 42:3	62:15 82:11	137:9
36:8 63:10	105:11,15	warrants 25:7	86:20 90:13	woodrow 3:19
value 15:17 18:7	106:14,17	125:14	100:14 103:21	word 57:2
18:15 38:5	107:1,11,16	washington	112:1 113:1	wordiness 109:7
39:16 42:4	109:12 110:21	1:18 3:17 4:8	122:3 126:8	words 37:6 43:2
69:4 102:12	111:2 137:18	5:8 32:21	136:11 137:14	58:9 67:4
112:2,15,15	137:19 139:10	wasnt 38:16	140:12	77:14 80:12

81:2 97:14 134:5 work 15:11 35:12 58:1 76:4 89:18 102:3 122:12 127:6,8 131:13 137:16 139:9 worked 123:13 working 103:3 123:18 137:15 works 83:7 world 10:15 96:2,4 115:15 worried 51:4 worth 38:8 65:12 68:5 worthwhile 11:7 worthy 53:10 wouldnt 19:6 40:20 64:17 76:18 78:5 97:8 113:22 128:22 wounded 39:7 writes 51:8 written 9:16 12:4 30:4 102:1 139:17 wrong 77:9 www 9:15	year 71:10 78:20 118:2,3 118:6,7 127:9 yearly 137:22 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 york 39:3 44:6 44:11,18 48:4 51:3 youd 42:18 81:6 84:13 112:8 youre 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 youve 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	11 6:3 15:21 1127 1:17 5:8 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 13 127:11 14 9:18 15 142:14 16 5:11 18 21:1 40:1,2 121:1 136:21 180 29:20 30:6	107:21 111:13 112:16 117:19 119:7 120:10 133:5 134:20 215s 108:16 22 27:3 51:11 25 5:11 128:11 27 18:10 288 78:20	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
<hr/> X <hr/>	<hr/> Z <hr/>	<hr/> 2 <hr/>	<hr/> 3 <hr/>	
<hr/> Y <hr/>	zero 133:6 zhou 91:2 zwillgen 3:9 zwillinger 3:9	20 5:6 20022008 3:8 20036 1:18 2009 18:7 2011 38:14 2013 1:12 5:6,12 2015 37:22 215 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	30 1:18 13:2 26:22 51:22 63:12,14 64:16 76:5 119:11,20 120:5 365 29:21	
		<hr/> 0 <hr/>	<hr/> 4 <hr/>	
		<hr/> 1 <hr/>	4 1:12 4th 5:6	
yahoo 10:14 yall 130:8 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			<hr/> 5 <hr/>	
			50 129:4,4	
			<hr/> 6 <hr/>	
			60 139:20	
			<hr/> 7 <hr/>	
			702 1:9 2:11 7:8 7:17 11:3,10 65:14 66:5,18 69:10 71:5,14 75:16 85:17 132:10,11 137:19,22 138:6,7,22 139:8	
			<hr/> 8 <hr/>	
			<hr/> 9 <hr/>	
			9 1:18 5:6 6:3 15:21 90 26:20 27:1	