

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

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

July 9, 2013

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

Reported by: Lynne Livingston

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

BOARD MEMBERS

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

PANEL I

Legal/Constitutional Perspective

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

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

PANEL II

Role of Technology

Steven Bellovin, Columbia University Computer
Science Department
Marc Rotenberg, Electronic Privacy Information
Center
Ashkan Soltani, Independent Researcher and
Consultant
Daniel Weitzner, MIT Computer Science and
Artificial Intelligence Lab

PANEL III

Policy Perspective

James Baker, Formerly DOJ Office of Intelligence
and Policy Review
Michael Davidson, Formerly Senate Legal Counsel
Sharon Bradford Franklin, The Constitution Project
Elizabeth Goitein, Brennan Center for Justice
Greg Nojeim, Center for Democracy and Technology
Nathan Sales, George Mason School of Law

1 PROCEEDINGS

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

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

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

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

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

1 to our country's counterterrorism efforts.

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

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

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

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

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

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

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

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

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

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

22 At the end of the day there will be some

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 targeting of U.S. persons.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 So Steve, we'll start with you.

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

22 I'm going to focus my opening remarks on

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 committees of Congress.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 Since these programs were disclosed much

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

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

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

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

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

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

1 email he or she receives.

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

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

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

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

1 the Fourth Amendment.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 MS. BRAND: Thank you. Kate.

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

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

22 I think it is not debatable that secrecy

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

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

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

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

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

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

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

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

22 Secondly, the system is meant to prevent,

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

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

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

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

22 I think that the question that we need to

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

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

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

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

1 Judge Robertson.

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

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

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

22 So I know at firsthand, and I wish I

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

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

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

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

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

1 Judging is choosing between adversaries.

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

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

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

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

1 reviewable by another court.

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

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

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

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

22 That is why the Supreme Court had to

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

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

12 Thank you.

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

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

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

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

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

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

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

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

1 approved by the FISA Court.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 As this history demonstrates the FAA was

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

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

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

22 I appreciate the opportunity to address

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21 MR. BRADBURY: Thank you.

22 MS. WALD: You can pick up in the

1 individual questions, which will come about later.

2 Thank you. Jameel.

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

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

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

22 And you know, there's a certain

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

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

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

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

22 That too, that assertion I just made was

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

6 MS. WALD: Kate.

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

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

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

1 communications, especially communications with
2 people located overseas.

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

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

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

22 MS. WALD: Jim.

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

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

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

20 MS. WALD: Ken.

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

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

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

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

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

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

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

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

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

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

1 this information is used.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 I mean do you have a view on that,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 alternatives.

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

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

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

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

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

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

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

16 Steve.

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

19 MS. WALD: No, the FISA question.

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

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

1 that case everybody gets six minutes.

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

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

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

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

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

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

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

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

15 In terms of --

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

1 program is related.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 intrusive than what?

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

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

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

22 But I have to tell you that what keeps

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

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

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

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

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

1 original intent of the original legislation.

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

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

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

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

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

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

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

22 So if you look at section -- my question

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

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

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

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

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

1 business records subpoena.

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

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

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

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

1 statute requires or points to.

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

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

17 Can I just say one quick thing? Jameel
18 has used the word surveillance in describing this
19 215 order. This is not surveillance.
20 Surveillance is a defined term under FISA. That
21 includes getting the content of communications
22 usually when they're being transmitted across a

1 wire, for example.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 And the third question to all of you,

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

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

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

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

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

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

17 Okay, take it away.

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

20 MS. WALD: I sneaked it in.

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

1 read the other day that Eric Lichtblau story --

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

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

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

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

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

1 would be or exactly how it would work.

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

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

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

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

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

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

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

9 MR. ROBERTSON: Part way.

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

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

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

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

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

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

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

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

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

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

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

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

1 the United States.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 Instead the court was making these, and

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

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

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

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

22 I think that it was created, as Judge

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 As Steve said, this is exactly what we do
18 in the criminal side. When I go to judges like I
19 did with Judge Robertson to get a search warrant
20 as a prosecutor, or to get a Title III wiretap
21 warrant against somebody, that was done ex parte.
22 It was the prosecutor, maybe the agent and nobody

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

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

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

18 And I can tell you from experience that
19 judges on the FISA Court, they are Article III
20 judges they are, you know, contrary to what some
21 people have suggested not at all in the
22 government's pocket. They are very independent

1 and they put us through our paces to make sure
2 that what we give them measures up to their
3 standards and the standards in the law.

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

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

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

1 if the FISA Court can disclose some sanitized
2 version of these opinions, it's just good for
3 public education, but it's good because these
4 programs only work so long as we have the
5 confidence in the American public that they're
6 being conducted honestly and reasonably and
7 consistent with the Statute.

8 MS. WALD: Thank you.

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

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

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

21 My question is whether that raises a
22 Fourth Amendment issue by collecting and using

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

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

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

19 But then 9/11 hit, huge problem. We
20 suddenly needed to know about all suspicious
21 communications from thousands of potential
22 terrorist dots outside of the United States. When

1 are they communicating in or out of the U.S.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 So the I think you're asking the right
21 question. My view is the answer to your question
22 is the minimization procedures are insufficient,

1 insufficient to protect American's privacy.

2 MR. MEDINE: Steve you want a rebuttal?

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

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

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

21 And the argument that was made during
22 consideration of 702 is that the reason why you

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

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

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

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

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

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

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

19 So that you cannot, the NSA cannot target
20 somebody who's overseas for the purpose of
21 collecting a communication within the United
22 States. What 702 does permit, and this is I think

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

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

18 You know, and FISA was drafted
19 specifically to work around that collection to
20 make sure that didn't get hindered by the FISA
21 order requirement. And obviously the same thing
22 could to Title III. And so it would be a major

1 paradigm shift in our collections.

2 MR. MEDINE: A quick response from Kate.

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

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

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

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

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

20 MS. COLLINS COOK: I was actually at the
21 risk of assigning homework going to ask that you
22 all consider my question and if you are so moved

1 provide information afterwards to keep us on
2 track.

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

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

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

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

7 Jim.

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

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

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

1 forward here.

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

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

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

18 The way this was set up it was a little
19 bit we have two critics of the programs and two
20 defenders of the programs. I really think that
21 there's a role for former government officials to
22 play. It can't be that everything is perfect. It

1 can't be that no changes can be made, that no
2 additional improvements or checks and balances or
3 controls, etcetera, can be made.

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

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

17 Judge Robertson is a hundred percent
18 correct in terms of the misunderstanding at least,
19 or the use of that term in a way that it becomes a
20 mantra and no one really has dug in on that.

21 There is a document online, whether it's valid or
22 not, whether it's still right or not, I think

1 there's a document online that, assuming that
2 minimization procedures looked like what is in
3 that document, what's the reaction to them? How
4 do they play out here? Is it good, is it bad, is
5 it indifferent?

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

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

20 And then on the Zazi case I would like to
21 see some, whatever there is on the public record
22 in terms of Jameel had mentioned that. I'd like

1 to see somebody dig in a little bit and spell that
2 out for us.

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

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

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

14 (Off the record)

15 MR. MEDINE: Good afternoon. We're going
16 to begin the second session of our program today
17 and this is the section that will focus on
18 technology issues.

19 Jim Dempsey and I will be co-moderating
20 this. And I'll turn it to Jim to make
21 introductions and kick things off.

22 MR. DEMPSEY: So good afternoon again

1 everybody, and thanks to our afternoon panelists
2 as well for giving their time to us on this
3 important set of issues.

4 Our panelists for the afternoon are four
5 of the leading experts, and sort of one of the
6 questions or one of the challenges facing the
7 PCLOB, which is bridging the gap between
8 technology and policy.

9 So we have Steve Bellovin, currently a
10 professor in the computer science department at
11 Columbia University, many, many years at Bell
12 Labs, one of the country's leading experts on
13 computer security issues, as well as other issues
14 at the intersection of technology and policy.

15 Secondly, is Marc Rotenberg, long time
16 president and head of the Electronic Privacy
17 Information Center, and again a nationally and
18 internationally recognized expert on privacy
19 issues.

20 Ashkan Soltani is an independent
21 researcher on privacy and security issues, among
22 other things was a consultant to the Wall Street

1 Journal on its extensive series of articles on
2 Internet privacy issues.

3 And finally, Danny Weitzner, currently at
4 the computer science and artificial lab at MIT,
5 former White House science and technology policy
6 advisor, co-founder of the Center for Democracy
7 and Technology, and again, a long time participant
8 in these debates.

9 So again we will adhere to the rules we
10 established this morning, five minute opening
11 remarks from each of the panelists, followed by a
12 two minute response by the panelists to comments
13 made by their fellow panelists and then questions
14 by the Chairman David Medine and myself.

15 And as with this morning and as with
16 members of the public, the record of this
17 proceeding will remain open until August 1.

18 Several of the speakers on the second
19 panel have already submitted either final or draft
20 comments, which we're grateful for, but they will
21 have, like everybody else, until August 1 to, as
22 they say on Capitol Hill, revise and extend.

1 So Steve, please.

2 MR. BELLOVIN: Thanks, Jim. And let me
3 add a brief disclaimer, I wear many hats in this
4 town. Today the only one I'm wearing is as a
5 private citizen, nothing else.

6 And what I'm going to be saying is based
7 on my draft remarks. You have copies of them but
8 for anyone else, they're already on my web page.
9 You can find it easily with your favorite search
10 engines.

11 But these are draft remarks, draft
12 comments. I need to just make sure I've got the
13 facts right, let alone my analysis in writing. So
14 take it with a grain of salt, this is still a
15 draft.

16 So I'm a computer scientist, not a
17 lawyer, but it means when I look at a system, I
18 look at it from a technical perspective. And when
19 I see a system the first two questions I ask are,
20 why was it built that way and what else can I do
21 with it?

22 And you can say that that's my training

1 as a computer scientist, alternatively that's why
2 I became a computer scientist because that's in my
3 personality. Gee, shiny, pretty, what can I make
4 it do?

5 As a privacy scholar and technologist, I
6 also know that one of the things that's the
7 biggest problem in privacy is not the primary uses
8 of data collected for a legitimate reason but the
9 secondary uses that are often found later on for
10 some particular database. And that's another part
11 of the attitude I took towards this.

12 And so when I look at this large database
13 of phone records and presumably Internet metadata
14 as well, my first question is, why does somebody
15 need to build such a large database of phone
16 company records when the phone company has these
17 records?

18 I could come up with three possible
19 answers. One is retention. Perhaps the phone
20 companies do not retain the data for as long as is
21 necessary. The EU has a data retention law for
22 about two years covering a wide variety of

1 communications metadata. But that in itself is
2 controversial.

3 In the U.S. one reason why it will be
4 controversial is we don't have workshops and
5 hearings as much on what private companies are
6 allowed to do with their data, unlike in Europe.

7 Having a large telephone company maintain
8 data for longer might be worse for privacy. I
9 don't know. But it certainly is an issue. A data
10 retention law is not an automatic answer to a
11 privacy question.

12 A second possible answer that occurred to
13 me is the efficiency of search, and in particular
14 the indices. If you have a large amount of data
15 it's often organized to make it efficient to
16 answer the kinds of queries you need to answer for
17 your business purposes.

18 Arguably the phone companies do not have
19 the right indices for the kinds of queries that
20 the intelligence community wants to do and needs
21 to do. And that's perfectly reasonable for the
22 phone company not to. They don't have the same

1 questions.

2 It's a little harder to say what should
3 be done about that other than a copy. Asking a
4 phone company, could you build this index for me
5 is revealing of the kinds of questions an
6 intelligence agent, analyst might want to ask and
7 that could easily, very plausibly be seen as a
8 serious security issue.

9 The third answer, and the one to me that
10 I think poses the most difficult legal and policy
11 questions is machine learning, data mining, call
12 it what you will.

13 If you don't know what it is just think
14 of the phrase you've all seen in the press, heard
15 on the radio. I've heard several NPR stories in
16 the last year on big data. That's what this is,
17 big data.

18 What can you do with it? What can you
19 learn from it? It's a powerful technique but it's
20 also one very susceptible to abuse. Machine
21 learning finds things out by correlation, not
22 causality. It can find out very, very surprising

1 things.

2 The best example I can give you, go back
3 and read last year's New York Times Magazine
4 article on Target and the kinds of analyses they
5 were able to do with their customer base.

6 But the thing that makes it most
7 relevant, relevant, yes, that's an interesting
8 word here, isn't it? Machine learning often
9 requires a very large collection of data that
10 defines normal, precisely so you can say this is
11 abnormal because it's different than normal.

12 This means that by extension everything
13 is relevant, which makes for an interesting
14 reading of the law. It's not necessarily wrong
15 from a technical perspective.

16 I don't know what it means to do a Fourth
17 Amendment search which requires particularity when
18 it's data that's already there. We need to have a
19 legal understanding of what relevance and
20 particularity mean in the context of data mining.

21 We're going to have to go short because
22 I'm running very short on time. Metadata, you can

1 consult my written comments. Metadata, I look at
2 it from a technical perspective, a legal
3 perspective, third party doctrine, something I'm
4 giving to somebody else.

5 Can I look at this from a technical
6 perspective and say this piece of the technical
7 data is going to somebody else? It turns out that
8 it requires a very detailed technical analysis in
9 order to understand that. It cannot be done
10 easily.

11 There's a lot of invisible things that
12 can change the answer, and it's ridiculous to have
13 an expectation of privacy that depend on that.

14 How do we enforce the search limits that
15 the court has supposedly imposed? Can we do it by
16 technical mechanisms? Can we do it by auditing?
17 Do we do it on the server side or on the client
18 side? Both have problems.

19 Finally, there's the role of the system
20 administrator. In a recently declassified NSA
21 publication noted that system administrators,
22 because they have all privileges, are among the

1 very biggest security risks. This was once a
2 classified statement. I don't know why since any
3 system administrator knows it, and I've been doing
4 that for almost fifty years.

5 But looking at the technical,
6 organizational roles of the system administrator
7 is a very important thing that the board needs to
8 look at to understand the real security of the
9 system against the privacy against insider misuse.

10 MR. DEMPSEY: Steven, thank you. Marc.

11 MR. ROTENBERG: Thank you very much. I
12 want to begin by saying following Steve's comments
13 that I am not now a computer scientist. I was a
14 computer scientist and decided to go to law school
15 to help address the lawyer shortage in Washington,
16 D.C., and you know, I've contributed my time to
17 solving that problem.

18 In this statement that I've submitted I
19 outlined some of the steps that EPIC has taken to
20 date and made some recommendations to the
21 oversight board.

22 I do want to say that over the years at

1 EPIC I've had the opportunity to work with many
2 great computer scientists and technical experts.
3 And the one thing that they have taught me is a
4 healthy skepticism of technical solutions to what
5 are ultimately social or policy problems, which is
6 a point that I'll come back to.

7 In brief, let me first describe the steps
8 that we have taken. This may be of interest to
9 the oversight board. As many of you know, we
10 filed a mandamus petition with the Supreme Court
11 this week challenging the legal authority under
12 which the Verizon order was issued by the Foreign
13 Intelligence Surveillance Court.

14 This order was based on Section 215 of
15 the PATRIOT Act and it requires the
16 telecommunications firm to provide on an ongoing
17 basis all of the call detail records, that's the
18 phrase in the order, also described as telephone
19 metadata, for all Verizon customers on an ongoing
20 basis.

21 We looked very closely at that statute.
22 We read an enormous amount of commentary. We

1 simply concluded that the court did not have the
2 legal authority to issue that order.

3 We believe that the Supreme Court was the
4 only court that we could bring this claim to, and
5 that's a very important part of the analysis I
6 think.

7 Even as we talk about changes in the law,
8 we have to answer the question under current law,
9 is this surveillance activity lawful?

10 The second thing that EPIC has done is to
11 begin the formal petition process to the NSA
12 Director, General Alexander.

13 The National Security Agency, like all
14 federal agencies, is subject to the Administrative
15 Procedures Act and when it engages in a
16 substantial change in agency practice, it actually
17 has an obligation to notify the public of its
18 determination.

19 Now of course there are certain rules,
20 almost unique rules that apply to the NSA, and we
21 understand that. But that doesn't get the agency
22 out from under its fundamental responsibility to

1 be accountable to the public.

2 And as we did with the Department of
3 Homeland Security when they made the decision to
4 deploy the airport body scanners for primary
5 screening and that challenge was ultimately
6 successful in the D.C. Circuit, we think on a
7 similar basis the National Security Agency should
8 give the public the opportunity to comment on this
9 domestic surveillance program.

10 We have also asked the Federal
11 Communications Commission to determine whether
12 Verizon may have violated Section 222 of the
13 Communications Act when it turned over the
14 customer records to the National Security Agency.
15 The FCC plays a critical role in safeguarding the
16 privacy interests of American telephone consumers.

17 And finally, we've pursued a series of
18 Freedom of Information Act requests for some of
19 the key legal documents that have been thus far
20 kept secret.

21 If you have suggestions for more things
22 that we should be doing please send an email

1 marc@epic.org. We're very interested.

2 In brief, let me summarize the key points
3 of my written statement. The first point that I'd
4 like to make, as I did already, is that we think
5 the legal authority was exceeded in the Section
6 215 activity. It's set out in the petition in
7 considerable detail, summarized in our statement.

8 The second point as to metadata is that
9 this information is far more detailed and far more
10 revealing of person activity than typically the
11 underlying content in a communication.

12 And in this sense current law, U.S. law
13 in particular, is almost upside down with respect
14 to the privacy interest. As many of you know, our
15 laws have evolved following a paradigm which
16 basically distinguishes between the content of a
17 message, what's in the envelope, and the header
18 information contained on the exterior of the
19 envelope. And we've carried that forward with the
20 contents of a telephone communication, as opposed
21 to the CPNI, the call detail information.

22 But that analysis, you know, which might

1 have worked forty years ago when Smith versus
2 Maryland was decided, is almost unrelated to
3 current circumstance because in a digital word, as
4 opposed to an analog word, it's the digital data,
5 it's the transactional data that enables the
6 linking, the chaining, the profiling, the
7 matching, the assessing, the ranking, the rating.

8 All the analytic techniques that are
9 deployed to assess personal information are most
10 useful as against transactional data.

11 Underlying communications actually
12 requires interpretation and assessment, and it's a
13 slower process.

14 So the second point is that the metadata
15 which has been said as something of less privacy
16 interest than the content, in fact the opposite is
17 true. And I think that is the view widely held in
18 the scientific community.

19 The third point to make is that this type
20 of data, unlike underlying content, generates
21 additional uses.

22 I've said in the past that data chases

1 applications, which is to say that once you have
2 information collected and stored in a database,
3 you will not surprisingly find new uses for it.
4 In fact, it would be surprising if you didn't find
5 new uses.

6 Now you can through law attempt to
7 restrict and legislate the way in which the data
8 that you've collected may be used. But over time
9 almost certainly those boundary points will be
10 pushed further and further as more applications
11 for the data are found.

12 And I think the conclusion to draw from
13 this point is that a threshold is crossed once the
14 data is gathered because it is at that moment that
15 you've created the opportunity for future
16 applications.

17 Whether you choose at that moment in time
18 to permit those applications is a safeguard you
19 can put in place, but there is no guarantee that
20 that safeguard will remain over time.

21 The final point that I'll make, coming
22 back to my original comment is that it's very

1 tempting to imagine that there are technological
2 solutions to privacy problems. And I will say our
3 organization EPIC has been on the front line since
4 our founding to promote technologies to protect
5 privacy.

6 We were started over the freedom to use
7 encryption. We've supported de-identification,
8 anonymization, techniques of minimization. All of
9 these methods are very important, but there is no
10 question that at the end of the day the most
11 effective safeguards are the legal safeguards.

12 And I just wanted to close by sharing
13 with you a quote from President Jerome Wiesner,
14 former president of MIT, was the first science
15 advisor to President Kennedy.

16 He was asked to testify before the U.S.
17 Congress in the early days of the hearings on the
18 Privacy Act. And he was asked this question, are
19 there technological solutions to the problems of
20 privacy. And he said, there are those who hope
21 new technology can redress these invasions of
22 privacy that information technology now makes

1 possible, but I don't share this hope. To be
2 sure, it is possible and desirable to provide
3 technical safeguards against unauthorized access.
4 It is even conceivable that computers could be
5 programmed, this is forty years ago by the way, it
6 is even conceivable that computers could be
7 programmed to have their memories fade with time
8 and to eliminate specific identity. Such
9 safeguards are highly desirable, but the basic
10 safeguards cannot be provided by new inventions.
11 They must be provided by the legislative and legal
12 systems of this country.

13 We must face the need to provide adequate
14 guarantees for individual privacy. Thank you.

15 MR. DEMPSEY: Ashkan.

16 MR. SOLTANI: Thanks for having me. And
17 I want to just echo, before I start, just echo
18 Marc's points, that I agree wholeheartedly that
19 the metadata is actually more sensitive at times
20 than the content, and the retention of this
21 information exposes, even with policy safeguards,
22 just the existence of this information collected

1 at points it normally wouldn't be collected,
2 exposes us to great risk from breach, from misuse,
3 similar to the ways where hanging a piano over my
4 head might be legal but it exposes me to being
5 crushed by that piano at some point.

6 So I'm going to talk today about just
7 kind of four points, and I've written these in
8 comments, in draft comments on my blog, which you
9 guys can refer to and I'll submit them by the 1st.
10 I'm expecting that there's probably more
11 revelations that are going to be made and I'd like
12 to incorporate those before I submit.

13 So the points I want to make is, one,
14 that traditional ideas about geography and borders
15 don't really translate onto the Internet.

16 And that, two, that most of our modern
17 activities take place in part through some digital
18 medium. They create data trails about our
19 activities.

20 In fact, the NSA itself remarked that in
21 2002, they remarked that only 1 percent of the 290
22 gigabytes of traffic, of Internet traffic at that

1 time was outside of their reach at the time.

2 That's in any 2002, right.

3 And two other points, that computer
4 systems don't inherently understand law. They
5 don't understand borders. You know, they don't
6 have the same kind of limitations that we do or
7 understanding that we do.

8 And that they work under the guidance of
9 their operators. And these operators are
10 empowered under a legal authority which I feel
11 like might be confused or lack understanding of
12 the technical capabilities.

13 One is, for example, the point Marc made
14 that the metadata has more capabilities, or big
15 data has more capabilities than one would
16 naturally logically infer. But just other
17 understandings of how the technology operates.

18 And so I'd like to expand on that a bit.
19 And the one other point of clarification from this
20 morning's kind of discussion was that there's been
21 a couple of different kind of very clever
22 push backs and a couple of different revelations

1 we've made.

2 But the metadata collection wasn't just
3 business records. It wasn't just the NSA going to
4 AA&T and saying, show us your call records that
5 you collected historically.

6 There was at multiple times equipment
7 that the NSA had implanted at key Internet
8 exchanges and key junctions at service providers
9 in order to themselves create this metadata and
10 collect it.

11 And we want to be mindful of that in
12 particular because it's a very different issue
13 than just going to Verizon and saying, hey, give
14 us call records. This is generating call records,
15 generating IP metadata.

16 And the process by which that's generated
17 is problematic because, as I said, computers don't
18 understand law. They don't understand the
19 difference between, say -- they do understand the
20 difference, but it's a very small distinction
21 between an IP header and the email content itself,
22 right, and the same equipment is often very easily

1 able to capture that same data if it wanted to.

2 And we have some understanding that they were
3 actually collecting email content from the wire.

4 So I'm going to start just to expand on
5 the first point, which is on a quote that former
6 NSA Director Hayden himself made in an interview
7 recently where he said, let's keep in mind that
8 global telecom infrastructure, geography doesn't
9 mean what it used to mean. Things of a place may
10 not be in a place, and things in a place may not
11 be of a place. The Internet actually lacks
12 geography.

13 And so this is his statement. It's kind
14 of telling, the person who kind of spearheaded
15 these projects himself doesn't believe that
16 there's an inherent geography to the Internet.

17 And we kind of need to push on this a bit
18 because, in fact, we want to understand that the
19 NSA is collecting information about kind of any
20 geography and then using, or taking technical
21 measures to limit the amount of information they
22 use on Americans.

1 And to do this, it's kind of unreliable.
2 I describe a couple ways where this breaks down in
3 my comments around things like users using VPNs,
4 users switching email addresses, who uses, you
5 know.

6 For example, the NSA maintains a database
7 of identifiers on U.S. citizens which in itself is
8 information about Americans, not anonymous
9 information, but for example, phone numbers, MAC
10 addresses, Internet IP addresses, those kinds of
11 things to identify who's an American. And so
12 that's actually information about Americans.

13 And oftentimes these things can, to the
14 degree that they're right, they're problematic,
15 and to the degree they're wrong, oftentimes it's
16 problematic because they'll be inadvertently
17 collecting information.

18 The other thing that kind of complicates
19 things is that the systems that are in place, you
20 know, using these identifiers, using these
21 selectors, right, to discern content can often be
22 implemented improperly, right.

1 So in fact, we know that through contact
2 chaining targets of interest could be anyone that
3 has an affiliation or interactions with someone
4 else of interest, right. So I could be
5 potentially be a target of interest by my
6 communication with someone of interest.

7 But you'll find that most of the modern
8 Internet systems that we use today, things like
9 Skype, P-apps like Skype or Spotify, I don't know
10 if you guys use Spotify to listen to music. These
11 are P to P apps, right. They connect with anyone
12 on the Internet for the purpose of providing the
13 service.

14 So if I and a member of Al-Qaeda like the
15 same Britney Spears's song, right, does that
16 actually put me as a target, right? Does that put
17 me as a target under this contact chaining?

18 And so the system would probably say yes
19 because I have, you know, some sort of
20 communication with that target, some sort of data
21 sharing with that target. But we want to be
22 mindful that these systems are limited in the way

1 they understand geography.

2 And then finally I want to make the
3 point, I make this in my comments as well, that I
4 feel like most of the, you know, we might look to
5 Congress and look to policy makers at what, you
6 know, they've had repeated opportunities to shut
7 down and push back on these programs and they
8 haven't.

9 And we might infer that to mean that they
10 think these programs are justified or think that
11 they are effective or they're worth the tradeoff.

12 But one other explanation I want to kind of
13 propose is that, again, people don't understand
14 the technical implications and the raw elements
15 that go into these systems.

16 So that in fact, the policy makers don't
17 actually understand the technical capabilities of
18 these underlying infrastructures and what data
19 they ingest and what they're capable of.

20 And because of that lack of understanding
21 that it seems generally okay, right. The geeks
22 have the key to the castle where they'll give you

1 an explanation that of course the system won't
2 collect information. But in fact, if you looked
3 under the hood, you'd realize that there is
4 actually quite a bit of domestic surveillance
5 going on, quite a lot of inadvertent data
6 collected, quite a lot of misuse from both a
7 policy and a technical perspective. And I think
8 that lack of understanding might explain why there
9 hasn't been kind of tighter controls.

10 MR. DEMPSEY: Okay, thank you, Ashkan.
11 Danny.

12 MR. WEITZNER: Thanks very much. Thanks
13 to all of you for having me and congratulations to
14 us on having you here.

15 I think that we all know that as this
16 round of privacy discussions kicked off, the
17 President said we need a national conversation and
18 I think you guys are it, and that's great.
19 Hopefully there's more, too.

20 But you have my written remarks. I want
21 to just highlight three points from those
22 remarks. I want to touch on a little bit of a

1 what I see as the functional goals of a system
2 with sound oversight, some of the technical
3 challenges of getting to that kind of system, and
4 a new technical approach that we've been
5 developing at MIT as part of a larger family of
6 research that's going on around the computer
7 science world.

8 I see really two functional goals in
9 thinking about how a combination of law and
10 technology can shape the system that we're talking
11 about. And we've concentrated, you've asked us to
12 concentrate on the 215 and 702 programs.

13 I will say that I think it's important,
14 as Ashkan has suggested, to see these programs in
15 a larger context. They draw on data from a much
16 larger set of systems out there, and I think the
17 ability to draw boundaries in those systems is not
18 nearly as easily as changing section numbers in a
19 statute. So I think it's useful to look in a
20 broader context.

21 But I want to suggest that there are two
22 goals that we ought to pay special attention to.

1 First of all, I do think that we should be
2 thinking about how to enable, within the bounds of
3 law and under the rule of law, the process of what
4 Bob Litt has recently called finding a needle in a
5 haystack without undue privacy risk. That's goal
6 number one.

7 And goal number two, I think given that
8 kind of intensive information analytic
9 environment, to create an environment, as Ken
10 Wainstein said, where there's genuine public
11 confidence in the operation of these programs
12 based on oversight that's effective and a
13 meaningful sense of transparency.

14 I do think that if we look over the last
15 month it's been the lack of public transparency in
16 these programs and the continued revelations about
17 more data and more data and more information and
18 more information that's come out about these
19 programs that has caused people to feel more and
20 more uneasy.

21 I think it's caused American allies
22 around the world to feel more and more uneasy. I

1 think it causes citizens to feel uneasy. I think
2 it causes companies to feel uneasy.

3 And so I think that having a real sense
4 of transparency here is quite important. And I
5 would suggest to you that it's important to think
6 about transparency in two dimensions here.

7 The first panel spent a lot of time
8 talking about the reasonable transparency for
9 rules and the rule making processes associated
10 with these programs. But I think the second kind
11 of transparency that this panel can address
12 perhaps in a more focused way is transparency of
13 the actual data usage. How are we going to know
14 what's actually going on in these systems?

15 Let me talk for just a minute about what
16 I see is the technical challenge of having that
17 kind of transparency. Within certain bounds I
18 think it's safe to assume that the government is
19 going to have more and more and more data.

20 I think the constitutional process, the
21 legislative process will determine how much more,
22 but it's going to be more, and that's just because

1 of the trends in the world that we live in.

2 So I see the challenge, again picking up
3 on Bob Litt's, he's been very eloquent these days,
4 Bob Litt's statement, he's very up front recently
5 in a public statement said that we, the
6 intelligence community, collects all the data
7 because if you want to find a needle in a
8 haystack, you have to have the haystack.

9 Steve addressed some of this question
10 about whether you actually need all the haystack
11 all the time, but I think we can see the
12 development of government programs, the NCTC
13 programs as an example, are moving towards having
14 all the data in one place.

15 And then the challenge, the oversight
16 challenge for organizations such as the PCLOB, for
17 the internal oversight functions for the courts,
18 for the Congress and ultimately for the public is
19 how to have a sense of confidence that all that
20 data that's held where again the claim is only a
21 tiny bit of it is used, that in fact those rules
22 are being adhered to.

1 What I think it's very important to
2 recognize about these rules is that these are
3 rules that really are governing the usage of
4 information, not the access to or collection of
5 information.

6 Again, in the larger privacy policy
7 debate I think we can see more and more a
8 recognition that many of the privacy challenges we
9 have are going to have to be addressed by usage
10 limitations, not simply by collection limitations
11 because to a large extent all the data of interest
12 has been collected and is sitting somewhere.

13 Very briefly, I would say that if you
14 look at the computational techniques available to
15 address these kinds of challenges, in computer
16 science we're quite good at access control. We're
17 quite good at controlling who has what access to
18 what data at any given moment. We can encrypt it.
19 We can put it behind firewalls. We can do all
20 kinds of things. And Steve is one of the world's
21 experts on all of those sorts of techniques.

22 But what we're not actually as good at

1 until recently is the ability to examine a system
2 and determine how the information in a system is
3 actually used and whether its uses are in
4 accordance with whatever the appropriate rules
5 are.

6 Several years ago my research group at
7 MIT took on the challenge of trying to think about
8 whether there's a way to actually characterize
9 information usage rules in a formal computational
10 sense and whether you can then apply those rules
11 or you can ask whether those rules have been
12 adhered to in any given information system.

13 We've developed a number of research
14 prototypes that enable us to detect violations of
15 rules such as nondiscrimination rules, law
16 enforcement information sharing rules, and then
17 some non-privacy rules such as copyright law.

18 And you have in my written remarks a
19 description of this research. And by the way,
20 there's now a very active community of researchers
21 around the country and around the world who are
22 working on systems like this.

1 I guess if I could stress one thing about
2 these systems and the state of their development,
3 I think we know a fair amount about how to design
4 these systems.

5 We know much less about how to deploy
6 them at large scale. And I don't think we will
7 know anything about how to deploy them in large
8 scale until we actually start doing that. And
9 that won't happen until the entities that hold
10 information are actually told that they have to be
11 accountable to these usage rules.

12 What we have now I think, and I think we
13 can take --

14 MR. DEMPSEY: If you could, can we hold
15 it right there.

16 Mr. Weitzner: Yes.

17 MR. DEMPSEY: I was a little generous on
18 the five minutes on the first round and instead of
19 having a full two minute round where everybody
20 feels obliged to say anything, let me simply ask,
21 is there anybody who feels compelled to say
22 something at this moment before we get to

1 questions?

2 Marc.

3 MR. ROTENBERG: Thanks, Jim. Well, I
4 actually wanted to follow-up on some of the points
5 that Danny just made because I'm very troubled by
6 his description and his proposal.

7 He seems to be arguing that there's
8 really no need, purpose, or likelihood of success
9 for collection limitation rules.

10 So I mean let me stipulate that for a
11 moment, but ask you these questions, if that's
12 true, A, what is the legal authority under which
13 U.S. agencies are currently allowed to collect all
14 this data? In other words, what's the basis?

15 I used to think of that as a search
16 requiring some legal standard, even a low one. Do
17 you think there is such a legal standard that
18 operates as a limit on collection?

19 And secondly, if you don't, if you don't
20 think there are any legal standards that prevent
21 collection, is there any boundary point?

22 In other words, if the Verizon order, the

1 NSA were to go to FISC and say we want all credit
2 card information, all telephone information, all
3 web searches, everything you possibly have and
4 then we will sort out the usage conditions, do you
5 have any problem with that?

6 MR. WEITZNER: So let me make sure that
7 no one misunderstands, I am in no way suggesting
8 that we should eliminate all collection
9 limitations.

10 What I am suggesting is that our current
11 legal standards appear to allow the collection of
12 very large amounts of information. And I said
13 very directly that I think it is for the
14 legislative process and ultimately for
15 constitutional determinations to sort out how
16 broad that is.

17 But my belief is that agencies have
18 reasons to have large amounts of information. And
19 again, I don't know whether it's large or very
20 large.

21 I also think that it's quite challenging,
22 based on some of the comments Steve made, to

1 understand where those limits will be. We need
2 those limits, but what I would suggest is that
3 some of the protections that we have traditionally
4 sought from collection limitations, which I would
5 submit have mostly been practical limitations,
6 that it's hard. It used to be hard to store data,
7 it used to be hard to analyze a lot of data, those
8 practical limitations have fallen away.

9 And I believe we need to replace them in
10 many cases with very clear usage rules to prevent
11 against the misuse of data.

12 I don't think it's an either or question
13 in any way, Marc, but I think it's equally
14 mistaken to assume that you can solve this problem
15 with collection limits.

16 MR. SOLTANI: Just a quick comment on
17 that. I think I would agree with both sides here
18 in the sense that I'm a fan of usage or
19 audit-type, basically transparency, technical
20 transparency mechanisms, right.

21 For an agency that's, you know, whose
22 bread and butter is kind of data mining and data

1 analysis, they should be able to analyze what the
2 effectiveness and the usage of their information
3 is, right, that's a no brainer.

4 They could tell us what percentage of the
5 information throughout a trail was relevant to an
6 investigation.

7 However I want to push back on the use of
8 technology as a placebo or fix, or sorry, a
9 panacea of policy limitations, right, because all
10 that does, all the use of things like encryption,
11 or firewalls, or access control rules, all that
12 does is make it more expensive to get at the data,
13 but rarely does it make it impossible.

14 We've found that with enough resources
15 and enough effort almost every security
16 advancement, there's been some vulnerability
17 found, it just takes --

18 MR. DEMPSEY: Although I mean we can talk
19 about the abuse scenario. Honestly, I would
20 rather focus on the non-abusive uses.

21 MR. SOLTANI: Absolutely. But let me
22 give you, so let's say there's a database that's

1 encrypted or it has access limitations that has
2 the subject of a potentially suspected terrorist
3 and it's our only lead for it.

4 We know that data exists in a database
5 but it also contains, you know, millions of
6 records of individuals, innocent individuals,
7 Americans.

8 So not in an abuse scenario but in a
9 scenario where we know that data exists somewhere,
10 we have technical limitations, but do you think we
11 would not as a nation or as a country overcome
12 those technical limitations if the data exists?

13 MR. DEMPSEY: All right, that's a
14 different.

15 Steve, do you want to add anything
16 quickly here?

17 MR. BELLOVIN: I'll pass for now.

18 MR. DEMPSEY: Okay. For my first
19 question let me ask the following, which is
20 geography. A couple of you mentioned geography
21 and that the Internet lacks geography, quoting
22 General Alexander or whoever.

1 We have a law, 702, which is based upon
2 the geography of people, persons. And let's
3 assume for now that persons means an individual.
4 So an individual only exists in one place at a
5 time, and we have a system that's based upon
6 assessing where that individual is, and if they
7 are outside of the United States and not believed
8 to be a U.S. person, then they can be subject to
9 collection under 702.

10 Now my question is, what are the best and
11 what are the worst indicators of whether a person
12 is outside the United States? Steve.

13 MR. BELLOVIN: So there are several
14 technologies that are commonly used. The most
15 common one is something called IP geolocation.
16 There are databases saying where different IP
17 addresses are, Internet protocol addresses.

18 If you look at this, this is used by
19 gambling sites, by major league baseball to see if
20 you're in the blackout area and so on.

21 MR. DEMPSEY: And by the way, don't
22 forget the possibility of nontechnological means

1 in terms of your --

2 MR. BELLOVIN: Yes, absolutely. It's an
3 imperfect technology, is probably about 85 percent
4 accurate, certainly more accurate when we talk
5 about the country level rather than the city
6 level.

7 MR. DEMPSEY: Which one are you talking
8 about now?

9 MR. BELLOVIN: This IP geolocation. The
10 NSA actually has a patent on a somewhat more
11 advanced technique which uses round trip time from
12 geographically known points. Speed of light is a
13 limit. I don't know if they're actually using it,
14 but there is a U.S. patent that they were granted
15 on this.

16 The problem is that data doesn't respect
17 national boundaries and as we see more and more
18 data moving to the, quote, cloud, unquote, if
19 you're operating one of these large data
20 warehouses in the Internet someplace, you want to
21 disburse geographically for reliability,
22 redundancy, another northeast blackout or another

1 California blackout won't take it out, one of the
2 migration's going to happen quite transparently
3 and nobody is controlling where a lot of this
4 stuff goes. So the geography of the data makes
5 for a very, very poor analogue --

6 MR. DEMPSEY: Again, we have a law here.
7 We have a law here that ignores the geography of
8 the data and focuses on the geography of the
9 person, and I'm trying to ask -- Ashkan.

10 Finish up, Steve, and then go to Ashkan.

11 MR. BELLOVIN: There are approaches,
12 they're not perfect, especially a lot of the
13 technical mechanisms that business travelers
14 especially use when they're traveling virtual
15 private networks makes them appear in the U.S. who
16 are not in the U.S. depending on what their
17 country of origin is.

18 It's not a particularly useful paradigm
19 today. And there's a lot of stuff that's out
20 there which is not easily attributable to a
21 particular person because of twitter handles and
22 the solution of massive databases has its own

1 privacy risks.

2 MR. DEMPSEY: Ashkan, and then I'll go
3 back to Marc.

4 MR. SOLTANI: I want to echo Steve's
5 comment. There's actually the third largest ISP
6 in New Zealand, they have a feature where their IP
7 addresses become borderless. They can appear to
8 come from the UK or come to the U.S. so they can
9 have access to things like Hulu or BBC, right.

10 So these are like commonly used. VPN
11 tools are commonly used and they basically render
12 IP-based geolocations somewhat ineffective. IP
13 geolocation will tell you the source of the
14 network equipment but it won't tell you the
15 location of the individual.

16 But one thing I want to point out is
17 email addresses don't have the same property. So
18 an email address doesn't inherently have a
19 nationality that you can infer from the email
20 address, right, so perhaps you can look at the
21 country code or maybe the nationality of the name.
22 But there's nothing actually inherent to the email

1 address.

2 And in fact, we've learned that most
3 email, so most email between cloud providers,
4 right, so when you go to Gmail and you send an
5 email, even though you see a lock icon in your
6 browser, when Gmail delivers that email to someone
7 else, it's transmitted through Gmail servers in
8 the cloud, as Steve described in Cleartext, right,
9 and so anyone with equipment at large Internet
10 exchanges can monitor that and scoop that
11 information up, metadata or content.

12 And the question is at what point then or
13 how do they determine whether it's a U.S. citizen
14 or not? And we understand there's some indication
15 to show that they have database of U.S. citizens.
16 There's other indication to show that there is
17 other data appended to it, right.

18 And at that point you're actually looking
19 at the data. You're actually, so if 702 is a
20 collection limit, you've collected and looked and
21 processed the data, at which point then you
22 decide, well, it might be American.

1 And the problem with that is it kind of,
2 it's kind of after the fact, right, you've already
3 looked and processed that data.

4 And then we know under section, what is
5 it, Section 5 that if you actually encounter any
6 illegal activity in that process you're then able
7 to hand it over to other law enforcement agencies
8 for processing, right, under Section 5. So it
9 renders this problem of email identity somewhat
10 borderless and somewhat ineffective to try to
11 differentiate.

12 MR. DEMPSEY: Marc next, Danny and then
13 I'll come to you. Marc was next.

14 MR. ROTENBERG: Let me see if I can give
15 you a somewhat more precise answer shaking the
16 cobwebs of my computer science background.

17 Now for locating the device the typical
18 cell phone can be located based on three
19 techniques. One is the cell service
20 triangulation. The second is the GPS, which the
21 devices typically include. And the third is the
22 Wifi access to the local router.

1 But you're talking about the identity of
2 the individual, you're actually talking about the
3 individual using the device at a moment in time.
4 And that's actually a problem in isomorphic
5 mapping.

6 In other words, you need a big table of
7 all U.S. citizens and then you need a unique link
8 to the user of the device at that moment in time.
9 Because, by the way, the person who's holding John
10 Smith's device may not necessarily be John Smith.
11 So you actually have to authenticate the user to
12 the device and then determine if that person has
13 the status that allows them to be a U.S. citizen
14 for 702 purposes.

15 Now I actually suspect that the NSA has
16 given considerable thought to that problem because
17 they need to address that challenge in satisfying
18 their 702 requirements.

19 I also know something about this because
20 I participated several years ago in a workshop on
21 something that was called eDNA. And the theory of
22 eDNA, and this was not long after 9/11 was that it

1 would be possible to uniquely link every activity
2 on the Internet, every key stroke to an
3 identifiable user. It actually solves the
4 isomorphic mapping problem because you know
5 exactly who did what when, right? It's perfect if
6 you're trying to design something like total
7 information awareness.

8 But here's the problem with this
9 calculus, and I think it's why we've gone too far
10 down this road of distinguishing between U.S.
11 citizens and non-U.S. citizens. Our Fourth
12 Amendment actually doesn't draw that distinction.

13 Our Fourth Amendment, and almost all
14 privacy laws but for the FISA, regulate the
15 conduct of the police in undertaking law
16 enforcement activity. We certainly recognize the
17 need for the conduct, but it's the police conduct
18 that we're regulating.

19 What FISA introduced was the notion that
20 in the collection of foreign intelligence we
21 needed to safeguard the privacy interests of U.S.
22 citizens, and in that introduction attempted to

1 build a barrier against the overreach on the U.S.
2 side, which was very sensible.

3 MR. DEMPSEY: Marc, if we could, back to
4 the question of geography. Again, the law focuses
5 on persons reasonably believed to be outside the
6 United States. That's the first filter, let's
7 call it.

8 And what I'm asking is in terms of how
9 that assessment is made, is this person or device,
10 let's assume, because you don't care so much about
11 the identity of the person, you care about the
12 location of the person, reasonably believed to be
13 outside the United States.

14 My question is, can somebody give me,
15 give us a list of what are the most reliable
16 factors, answering just that question, and then
17 what are the least reliable factors in answering
18 that question.

19 I'm going to go Danny and then I'll yield
20 to David because we've got to move on.

21 But to me, personally, it would be
22 helpful to have some kind of way to go back to NSA

1 and say, how are you making this determination,
2 what are you looking at, what is technologically
3 more reliable and technologically less reliable?
4 So you don't get then to the second question,
5 which is, oops, we got it, turns out it's a person
6 inside the United States, or oops, we got it, it
7 turns out to be a citizen. How do you first make
8 this judgement of geography? Danny.

9 MR. WEITZNER: I want to suggest that
10 perhaps the more reliable, less reliable list may
11 not be the best way to do it.

12 What I would say about more and less
13 reliable is the more contact you have with some
14 target, the more reliable your determination
15 should become.

16 And I think that in these uncertain
17 cases, let's take Steve's 85 percent accuracy as a
18 given, and I think we can get, there's known,
19 there are known reliability levers for different
20 IP address blocks. We can get you that sort of
21 information. The NSA obviously knows it.

22 But I think the real question is, does

1 any intelligence agency as they develop more
2 information about a target, do they act on it? Do
3 they realize, oh, actually it's now more likely
4 that this is a U.S. person so we better start
5 treating them that way?

6 Or, so the question is, do we have a way
7 of establishing that dynamic threshold? That is
8 the way that any web service, any Internet service
9 functions is it learns over time about who it's
10 dealing with. And I think it's reasonable to
11 expect that intelligence agencies should deploy
12 that kind of technique also and be accountable to
13 it.

14 So I'm a little nervous about these
15 bright line rules because I think the hard cases
16 are going to be the ones that change over time,
17 and the question is when does that change get
18 recognized?

19 MR. SOLTANI: And just real quick,
20 because of the point that I made in my -- the
21 other assumption is that there isn't a reliable
22 method, right, that as Steve said and others have

1 said, the Internet is without geography and that
2 you need additional information to prove one way
3 or the other. Sometimes that requires looking at
4 the content.

5 And there's a perverse incentive here, as
6 we found in the minimization guidelines and the
7 targeting guidelines whereby the standard is, the
8 information is basically guilty until proven
9 innocent, right. So unless you can reliably prove
10 that it's a U.S. citizen, you are able to hold it
11 and analyze it and for later analysis. This is
12 encrypted data. This is data that we don't have
13 clear understanding of.

14 And so these two things together that the
15 Internet is inherently without geography and
16 there's not a reliable way and the standard is
17 hold the data until you can reliably prove that
18 it's not U.S., I think causes a --

19 MR. DEMPSEY: Let's move on. We could go
20 on this forever.

21 MR. MEDINE: Yeah, I want to pull back to
22 about 5000 feet. One of the board's

1 responsibilities is to oversee programs and see if
2 they strike the right balance between privacy and
3 civil liberties.

4 We've heard from panelists about there
5 are privacy and civil liberties issues with regard
6 to collection, use, access and disclosure of
7 information.

8 I guess my question for each of you is,
9 if you could guide us in how we should approach
10 these problems, where can technology address those
11 concerns? Where does law, where do we have to
12 rely on law to address those concerns, or how does
13 technology and law interact together so that we
14 could address those concerns as a framework for
15 thinking about these issues going forward?

16 MR. BELLOVIN: Technology at best can
17 implement a policy. If I'm designing a system I
18 have to know what, you know, what are the specs,
19 what are the things I'm trying to do?

20 And I get, depending on the problem, I
21 can come closer or not so close from a technical
22 perspective.

1 The flip side to that is audit. How do
2 you verify that people are staying within the
3 rules?

4 I'll take a somewhat different
5 non-national security system, electronic medical
6 records in hospitals. Anybody who's looked at
7 these realizes that you can't require really
8 strong authenticate need to know because someone's
9 going to walk into the emergency room. So all of
10 these systems have so-called break the glass
11 access. In case of emergency, break the glass,
12 look at the data.

13 But there's going to be an audit process
14 after the fact to say was this a reasonable thing
15 for this doctor, this nurse, whatever, to have
16 done at that a time? And that's a deterrent.
17 It's also a way to catch and punish people who are
18 ignoring the rules.

19 But what comes first is the policy.
20 After that I can design a technology and it will,
21 it has to include an audit function.

22 MR. ROTENBERG: Well, I didn't mean to

1 suggest by my earlier comments that technical
2 solutions aren't appropriate. Obviously they're
3 necessary, and audit logs are key.

4 My point is simply that I don't think
5 that's an ultimate solution, and I think you do
6 need legal safeguards. And to that issue, you
7 know, I listened to the panel this morning, which
8 I thought was absolutely fascinating. All of the
9 speakers I thought had very interesting things to
10 say.

11 But I was particularly struck by
12 Mr. Wainstein's comments regarding how the FISA
13 process is similar to the traditional Title III
14 wiretap process. He said, you know, we have ex
15 parte access. We don't tell our targets when
16 we're trying to get information about them in the
17 course of an investigation. And of course in that
18 respect he was absolutely right.

19 But what struck me also, you know having
20 studied the oversight mechanisms for both of these
21 frameworks for electronic surveillance in the
22 United States, is how many other things are in

1 place for traditional Title III wiretaps, law
2 enforcement investigations.

3 So it's true, you don't notify the target
4 and you wouldn't, but what do you do? Well, you
5 know, the courts are have to report on an annual
6 basis the number of wiretaps that were authorized,
7 how long they took place, what the outcome was,
8 what the cost was, what percentage of
9 non-incriminating information was gathered.

10 And all of that data, by the way, is made
11 available to the public, not any investigation-
12 specific information, but an enormous amount of
13 information is made available to the public about
14 the scope, use, purpose, and effectiveness of
15 those traditional wiretaps.

16 With respect to FISA, we have almost none
17 of that information. We have a letter that says
18 roughly in 2012 there were 1,784 applications
19 submitted, one was withdrawn and 1,783 were
20 modified or approved, or actually approved or
21 approved subject to modification, because they're
22 ultimately virtually all approved.

1 So the key point I'm trying to make with
2 regard to the legal safeguards is I think there
3 are necessary and appropriate ways to pursue the
4 collection of data and to safeguard the nation.
5 No one is disputing that. But I think there are
6 many more ways of establishing meaningful
7 oversight within the FISA that really we haven't
8 scratched the surface of.

9 MR. MEDINE: Ashkan, law versus
10 technology.

11 MR. SOLTANI: Yes, so I think there are
12 some technical ways to do this but you would need
13 essentially kind of an intelligence agency to
14 monitor the intelligence agency.

15 So you would need a set of technically
16 capable kind of actors, you know, they could be
17 under PCLOB, they could be under some other
18 agency, that are building tools, building audit
19 mechanisms, building security mechanisms to
20 measure exactly what the agency is doing and the
21 effectiveness.

22 This could be simply things like, you

1 know, the number of email addresses, IP addresses,
2 U.S. persons, gigabytes, whatever is collected,
3 how that information relates to investigations,
4 how effective it's been. And provide kind of a
5 good, in-depth kind of, you know, red teaming the
6 NSA essentially, right, having someone from the
7 outside that's independent of the NSA audit them
8 and provide intel to you guys to tell you whether
9 they're doing their job, rather than you relying
10 on them. And this could be technical.

11 But this isn't things like what Danny and
12 Steven have described as the NSA implementing
13 their own audit logs, right, because I think
14 that's -- they will perhaps not classify an email
15 address as an individual, whereas you guys might
16 feel that is an individual. So you would probably
17 want an independent team doing this, I think.

18 MR. MEDINE: Taking that a step further,
19 is there also an argument that some of these
20 programs should be subject to testing and analysis
21 before they're rolled out on a larger scale?

22 I mean typically in technology you test

1 something and then see if it works and then you
2 build it out, as opposed to waiting after the fact
3 and seeing if it ended up working. Is there a
4 lesson there?

5 MR. SOLTANI: Absolutely. And fed back
6 to the judges and the policy makers approving
7 these programs, right.

8 So as you give a FISA order for something
9 like this, do you know the actual number of
10 individuals affected, the number of records, the
11 amount of records collected from this, how much
12 was over-collected, how effective this was?

13 That is, there's no feedback mechanism to
14 the FISC or to Congress as to how well. You just
15 kind of trust the NSA to say, yeah, this
16 recommendation, this is working great, these
17 algorithms are on it. And I don't think you guys
18 have a way to say, actually, you know to call BS
19 on that.

20 MR. MEDINE: Danny, any thoughts on law
21 and technology?

22 MR. WEITZNER: So I think that along the

1 lines that Ashkan is suggesting, I think we have
2 21st century intelligence analytic capabilities
3 and 20th century accountability and enforcement
4 methods, and we have to get the privacy
5 enforcement methods up to date.

6 I don't think it requires creating a
7 whole other intelligence agency and you probably
8 were just being flip in saying that.

9 I do think it requires a much more
10 intensive approach to auditing and it requires a
11 way of looking at the results of those audits in a
12 fashion that can have a certain amount of public
13 transparency, certainly access for independent
14 entities.

15 Maybe there's a role for the PCLOB in
16 doing but there'd probably have to be more than
17 just five of you to do it.

18 So I think we should raise our
19 expectations of the ability to detect anomalies
20 and detect misuses in the way these agencies
21 operate.

22 I'm a little leery of blending together

1 the question of intelligence effectiveness and
2 privacy rules. I find it to be -- so, yes, I
3 think certainly if agencies are going to spend
4 lots of money on new data analytic systems they
5 should make sure they're effective and they
6 shouldn't waste their money.

7 But just because a system is effective
8 doesn't mean it passes our privacy test. I think
9 we should make sure to keep those two questions on
10 separate tracks.

11 But there is really a lot that can be
12 done in having better accountability, but it comes
13 back also to Steve's original point, the rules
14 really have to be clear and not dependent on
15 technical accidents such as whether a particular
16 IP address might be geolocatable or not.

17 MR. DEMPSEY: Steve, did you comment on
18 this question or did you have anything?

19 MR. BELLOVIN: Well, I started by saying
20 that policy has to come first, and that's the law.

21 MR. DEMPSEY: Okay. One quick follow-up
22 for Marc and then one general question.

1 Marc, you mentioned, you said we've
2 barely scratched, I think you said we've barely
3 scratched the surface on approving the FISA
4 project, there's a lot more to be done there.

5 Either off the top of your head could you
6 tick off a couple of items or submit them for the
7 record please, but anything off the top of your
8 head that you want to tick off.

9 MR. ROTENBERG: I think we could improve
10 public reporting through the availability of more
11 statistical information that doesn't compromise
12 any particular program or activity of the agency
13 but would give the public a better picture of how
14 these programs are used over time.

15 I mean we found, for example, with
16 respect to the wiretap data, it's very useful to
17 see trends. It's very useful to understand, for
18 example, why narcotics investigations today are
19 the primary reason we have wiretapping, and
20 bookmaking was in the 60s and 70s, or regions of
21 the country.

22 And I think it leads to a more informed

1 public debate because people who think these are
2 necessary tools have the data to support their
3 points. We're not arguing in the dark.

4 MR. DEMPSEY: Thanks. And anything
5 further you could submit along those lines would
6 be very helpful to us, or other witnesses, or
7 other members of the public.

8 Content versus non-content. I have to
9 say personally I'm not yet convinced the
10 statement, Marc, that you made that the
11 non-content is as revealing as or more revealing
12 than the content.

13 Two reasons. Often of course when the
14 government collects the content they collect the
15 associated non-content as well.

16 But even on sort of the big data basis, I
17 mean I get it that, you know, I call the cancer
18 testing clinic, and then ten minutes later I call
19 the oncology department, and ten minutes later I
20 call the insurance company, and then I call the
21 drug store, and then I call the oncology clinic,
22 you know, every week for three months. So you

1 infer that I have cancer.

2 Well, I may have called and said my
3 mother is 90 years old, she has cancer, what can
4 we do about it? Or my child is six years old, she
5 has cancer, I'm going to be bringing her in every
6 day.

7 Now it would be far better, far more
8 revealing it seems to me to have that content than
9 the unreliable inference.

10 And I think there's a privacy flaw in
11 the, there is no distinction, because I actually
12 think you fall into the argument that the content
13 is so powerful you actually end up making the
14 government's argument as to why they need it.

15 I think there's a different argument to
16 be made, which is actually the metadata can be
17 highly misleading and you conclude that I have
18 cancer when in fact it's a relative that has
19 cancer.

20 MR. WEITZNER: Could I speak in favor of
21 Marc's proposition, which is that I would just
22 amend it slightly to say that metadata at scale is

1 at least as revealing as content. A single piece
2 of metadata or even a single set of metadata about
3 you can very well be misinterpreted.

4 A few years ago two students of mine did
5 as a final class project a paper that they called,
6 Gaydar. They looked at the MIT social network on
7 Facebook and were able to infer relatively
8 accurately who in that 25,000 person social
9 network was gay and who was straight, based on the
10 strength of the friendship relationships, based on
11 a link analysis.

12 So that was information that was actually
13 not available for the vast majority of the members
14 of the social network either publicly or
15 privately. You couldn't get it with a warrant but
16 you could infer it by looking at the metadata.

17 MR. DEMPSEY: Good point. Marc.

18 MR. ROTENBERG: I mean I agree with Danny
19 who is agreeing with you that at the micro level
20 inferences can be wrong, but at the macro level
21 the amount of useful information you can glean
22 from the metadata is far more valuable than the

1 underlying content.

2 And the simple way to understand this is
3 the dramatic paradigm shift from an analog world
4 to a digital world. Analog information doesn't
5 lend itself to analysis.

6 To analyze analog information you need to
7 transform it into a digital representation, which
8 by the way, is what's happening with a lot of
9 telecommunications, because a lot of voice traffic
10 is now being digitized and transformed so that it
11 can be analyzed as a digital representation.

12 But once in digital format you have
13 unbounded opportunity to examine, compare, rank,
14 analyze.

15 And I have to say coming from a bit of a
16 computer science background, I mean it's
17 fascinating. It's absolutely fascinating what you
18 can learn that you didn't even think you would
19 look for at the outset.

20 I would be surprised if people at the
21 National Security Agency aren't uncovering things
22 they didn't anticipate that they would find.

1 But you also made a critical point, Jim,
2 and I agree with this. I think it's the hard
3 policy problem. It is the value of the digital
4 data to the NSA that's driving these programs.

5 It is also the risk to privacy that I
6 think has raised the need to update our privacy
7 laws to reflect the underlying interest, the
8 actual interest in digital data.

9 If I can make one final point. I know
10 I've talked on a bit but I really don't want to
11 lose this one. We're thinking a lot about the
12 communications realm and the linking of identities
13 through investigations, which is an appropriate
14 investigative technique, but you should also be
15 aware that these large data sets are used to
16 profile individuals, including American travelers
17 entering the United States, to assign a threat
18 index to the likelihood that they may commit some
19 act that poses a risk to the country.

20 So by taking all of that data, looking at
21 prior acts, you can assign a score across a large
22 data set and allocate your resources. That is

1 another way in which large data is being used.

2 MR. DEMPSEY: But if the data is so
3 powerful, isn't that a good thing?

4 MR. MEDINE: And let me just follow-up on
5 that. That's really the converse of what your
6 argument is, is if the goal here of these programs
7 is to find terrorists that the data is very good
8 at that and shouldn't we be using it, and doesn't
9 that support the government's argument that we
10 need to amass all of this data to be as effective
11 as possible in identifying --

12 MR. WEITZNER: But we're missing, we
13 missed some steps, because we have answers I think
14 in consumer privacy law, as you know, David, laws
15 like the Fair Credit Reporting Act that are good
16 at managing very large scale analysis of data in a
17 way that attempts to be fair to individuals, so
18 that when determinations that could be harmful to
19 them, like you're not allowed into the country, or
20 you don't get a loan, are made, that there's a
21 feedback process, that people have a right to
22 respond and correct the data.

1 I think that there are obviously, you
2 know, there have been calls for that. It seems
3 like there's been some progress in DHS in doing
4 that, but I don't think that we've gone far
5 enough.

6 When there are real adverse consequences
7 for individuals, people should have the right to
8 be able to respond and correct the record, not to
9 be able to hide from what's true, but to make sure
10 that in fact the inferences are accurate.

11 MR. BELLOVIN: And let me just clarify a
12 little bit what Marc just said, it's not digital
13 data that's helpful, it's structured data.

14 Anyone who's done one of these voice menu
15 systems on the phone knows just how bad computers
16 can be in processing unstructured, just voice,
17 especially unstructured conversations.

18 Structured data, this is the calling
19 number, this is the called number, is extremely
20 valuable. You can process it very efficiently at
21 scale, gather vast amounts of data. It's much
22 harder to hide. You can do it retrospectively

1 rather than prospectively.

2 I want to wiretap, I have to go in
3 advance because the phone company is not recording
4 all of my target's phone calls, but they are
5 keeping call detail records. You can go do this
6 retrospectively.

7 The intelligence community has known for
8 more than seventy years that just the metadata is
9 an exceedingly valuable technique, and it's gotten
10 more so with modern data processing and data
11 handling.

12 Content is great but it's much harder to
13 get, especially harder to deal with --

14 MR. WEITZNER: Can I just express one
15 note of caution? I don't think that we should
16 necessarily make assumptions in an unclassified
17 environment about what the capabilities are to
18 analyze very large volumes of digital voice data.
19 I don't know, but I don't think we should
20 necessarily assume what the limitations are.

21 Because there's certainly been a lot of
22 advances in voice recognition and in processing

1 very large streams of digital data of this sort.

2 MR. SOLTANI: I agree with Danny. And
3 I'd rather propose a different perspective, which
4 is rather than saying content is gold and metadata
5 is maybe less, or trying to come up with a formula
6 where a thousand pieces of metadata equal one
7 piece of content, we should kind of view this as
8 information.

9 And information has kind of confidence
10 levels, right. So you have certain amounts, like
11 certain ability that information is accurate.
12 Oftentimes you'll find content itself, right,
13 content itself will be unreliable. There will be
14 lies, or code words, or misleading statements in
15 the content itself, right.

16 So, and if there's not a gold standard of
17 the truth, there's the information reveals certain
18 characteristics about you, about the individual
19 and that information has some level of
20 confidence.

21 And so oftentimes you'll find that a
22 statement like, you know, I like puppies is a very

1 high confidence interval that I've made, right, or
2 you could try to infer that based on my, you know,
3 previous pet activity or previous browsing
4 activity of puppies.

5 And you have some levels of confidence,
6 as Jim said, sometimes they're wrong, but as you
7 tune systems you often find that in a large data
8 environment you start kind of improving these
9 algorithms and with enough information you can
10 make these inferences.

11 And the question of whether this is
12 effective or not is definitely one question,
13 right. We've found in some cases this stuff is
14 effective or can be effective, right.

15 There've been examples of calling
16 patterns. Getting a nation's calling patterns
17 will reveal, you know, who might be in a drug ring
18 based on just the fact that people make inbound
19 calls, right.

20 So there is effectiveness to that stuff,
21 but it doesn't alleviate the policy question,
22 which is that, or I'm sorry, the privacy question

1 or the privacy interest, which is that, does this
2 information reveal sensitive, does metadata reveal
3 sensitive information? And to some degrees it
4 does.

5 MR. DEMPSEY: Just one quick observation
6 and I want to go to other members of the panel if
7 they have anything.

8 You know we talk about machine learning
9 and the feedback process and sort of system
10 learning, and again, thinking about the role of
11 judges, traditionally the judge issues the search
12 warrant, he gets a return. But if the search
13 turned up nothing, it's not like it was a bad
14 search or a bad warrant.

15 So in a way we're talking about, as Judge
16 Robertson said, changing the role of judges in a
17 way with these programmatic approvals.

18 Also with this question of what's coming
19 back. There might be something to be done there
20 to say, well, it's not that it was a bad search,
21 but we're just not going to do it again.

22 MR. SOLTANI: Right. If in your example

1 if historically you do a thousand of those and you
2 do intrusive searches and you kind of expend a ton
3 of resources and they don't come back as hits, at
4 some point the judge might kind of say, hey, this
5 is kind of a waste of time, let's not expend
6 resources on this. We don't have that
7 accountability in this program, right.

8 MR. DEMPSEY: Do the other members of the
9 panel, I am willing to yield if you do, if
10 something has occurred to you since.

11 MS. WALD: I've got one.

12 MR. DEMPSEY: Okay, good. So let's go on
13 down, Judge.

14 MS. WALD: You talked a lot about,
15 several of you about the accountability and
16 enforcement mechanisms being 20th century, whereas
17 our technology is leaping ahead in the 21st
18 century.

19 This morning's panel we talked a little
20 bit about possibilities on a legal end. I mean
21 people talked about maybe having not an ex parte
22 thing before the FISA, but something that the

1 other side is represented by.

2 Now my not being a technological person
3 at all, but my impression is that right now the
4 accountability mechanisms are all, well pretty
5 much all internal within the agencies. I mean
6 they self-report when something goes wrong. They
7 do have to report already to some degree,
8 depending, back to the FISA Court in certain
9 situations.

10 But, you know, even then they kind of
11 decide, and I'm not saying no question of good
12 faith, but they have the initial option of
13 deciding, you know, when they will report, what
14 they will report.

15 Now do you think there are any, we talked
16 about like in the FISA Court on the legal end
17 having somebody presenting the other legal side.

18 Are there any outside of the agency
19 itself kind of accountability mechanisms, other
20 than the one you mentioned about having the FISA
21 Court say, come back to me and tell me how that
22 program is working out, hoping the FISA Court is

1 more knowledgeable than I would have been in that
2 situation, that would help to enhance your notion
3 of accountability?

4 MR. WEITZNER: Could I suggest, Judge
5 Wald, that one, I don't actually have an answer
6 about what outside institutions might be put in
7 place, but I think that having structured, well
8 understood audit returns could help a court, could
9 help an authorizing judge evaluate the authority
10 that that judge has given to a given agency in a
11 given situation.

12 You know, I think that the problem we
13 have is it seems like on the one hand sometimes
14 there's a very large volume of data, there's
15 millions of elements of telephone metadata and
16 then we hear only 300 of them were used.

17 And I think that seems to present, or
18 Jim's example looking at geolocation, maybe if we
19 follow Steve's numbers, one in five, or one out of
20 six times you misidentify the location of a
21 person.

22 Well, do we have to just accept that as a

1 given for all programs and should judges act
2 accordingly, or could a judge say, well this time
3 you were accurate five out of six times, I want to
4 see it better. Come back, you know, fix your
5 program, come back with 90 percent accuracy.

6 You know, these are in many cases
7 challenges that could be met and we can identify
8 the underlying policy goals, the underlying harms
9 we're trying to prevent.

10 So I guess I think that, again, from a
11 technical perspective we should expect better
12 analysis of the data that's returned so the judges
13 can make judicial and policy determinations.

14 MS. WALD: But just to follow-up on that,
15 as you know the judges, the FISA judges are picked
16 from the pool of U.S. District Court judges. My
17 impression, I knew many of them, is that they
18 didn't come with a great deal of technical
19 knowledge or with computer science knowledge. I
20 mean they do their very best. I think they
21 probably do a good job, but they are not technical
22 people.

1 And when you get a massive operation and
2 they say, X with the selector or something went
3 wrong and as a result we got X number of things
4 that we shouldn't have gotten, blah, blah, blah,
5 blah. I guess what I'm saying is, do they need or
6 is it possible that FISA judges need maybe a
7 technical law clerk, I don't know, somebody who's
8 outside of the system who can relate to them?

9 MR. WEITZNER: Certainly. I think
10 absolutely having technical expertise to evaluate
11 --

12 MS. WALD: Or not outside the agency to
13 evaluate the data that comes back on returns.

14 MR. WEITZNER: But I think it's
15 ultimately up to policy makers.

16 MS. WALD: Yes, I agree.

17 MR. WEITZNER: To set that expectation,
18 to say that we actually care about this U.S.
19 persons question and we want to see accuracy
20 increase. It seems to me a judge, a court with
21 technical resources could implement that
22 determination.

1 MR. DEMPSEY: Steve and then Beth. Steve
2 just to follow-up on this answer.

3 MR. BELLOVIN: Yes. I'm not going to
4 answer who should do the auditing because you
5 don't want me designing your organizational
6 structure. Trust me on that.

7 But I can give you a few questions that
8 need to be asked. The first question, is it
9 actually effective? Are you actually finding
10 targets? If it's not finding targets, what's the
11 point in the system?

12 Second, how accurate were the
13 preconditions? The analog through probable cause
14 saying this is a program that we think will be
15 good enough or this is why we think this
16 individual is or is not American. How accurate
17 was that judgment on later investigation? How
18 well is it actually working? Are you really
19 finding the people you want to find? What are the
20 risks to privacy, both from intrinsic risks, from
21 later reanalysis, from misbehavior?

22 These are the questions to ask in the

1 audit. How often are people actually following
2 the rules? Rules that are too strict tend to get
3 evaded, and those are no good either. There's
4 just pro forma adherence to it. So this is the
5 kind of question.

6 But yeah, you want to feed that process
7 both internal and external. I hope they've done
8 internal.

9 There's one NSA whistle blower, I forget
10 his name, who blew the whistle on some project.
11 He said it was not working, it was privacy
12 violating, but most of all it wasn't working and
13 we're spending a billion dollars on it. What's
14 the point of doing that? Assuming his claims are
15 correct, and I do not know.

16 MR. DEMPSEY: Marc had a follow-up on
17 that one.

18 MR. ROTENBERG: Just very briefly, Judge,
19 I recommended earlier enhanced public reporting.

20 I think the question also should be
21 considered whether the statutory scope of the
22 court should be limited. It has enlarged over

1 time to a significant degree. It was actually in
2 2003 that the number of FISC orders exceeded the
3 number of Title III warrants approved in the
4 United States. And that trend has continued.

5 And the final point which I thought Judge
6 Robertson made very eloquently on the earlier
7 panel today is that the judicial process works
8 best of course from an adversarial proceeding.

9 And so even to have a technical expert,
10 you know, maybe that's helpful, but I think you
11 really do need to hear both sides of the claim to
12 make a meaningful determination. Otherwise you
13 transform the judge into someone who's basically
14 an agency manager, and that doesn't seem to be the
15 appropriate role for the court.

16 MR. DEMPSEY: Ashkan, if you could --

17 MR. SOLTANI: Actually just a quick --

18 MR. DEMPSEY: Okay.

19 MR. SOLTANI: There are external actors
20 or external entities, right. These are the
21 companies. A lot of these programs couldn't
22 actually be possible without the assistance of the

1 companies, right.

2 And the companies are currently under gag
3 to report the number of people that are affected.
4 We've seen some expansion of that recently. But
5 you could actually try to get more information
6 from the companies to actually describe, you know,
7 what information is revealed, not specific to
8 targets of course, but kind of trend reports, in
9 the same way we have transparency reports by a few
10 companies. You could actually have the agencies
11 that are working with these companies.

12 And these, but these companies are
13 actually dying to tell us, right. They're dying,
14 their brand and reputation are going down the
15 drain. So they're dying to reveal that in fact
16 it's not as bad as it is, or that the NSA is over-
17 collecting, right. And that's a nice little
18 external hook you could latch onto.

19 MS. COLLINS-COOK: So thank you guys.
20 This has been extremely helpful from my
21 perspective.

22 Danny, I wanted to follow up on one thing

1 that you had mentioned which was the gap between
2 the development of the capacity to do more
3 substantive and more effective auditing and the
4 inability to deploy it on larger scales.

5 And I just wanted to confirm what I got
6 out of that is that there are potential
7 operational risks.

8 For example, if you were to attempt to
9 deploy some of these more substantive audits on
10 existing systems or in existing databases, or is
11 it possible to simultaneously task some of the
12 programs y'all are developing without risking the
13 operational efficiency of ongoing programs?

14 MR. WEITZNER: So I think that it is
15 possible to. These systems all generate logs.
16 They have logs coming out, you know, logs and
17 logs. So it's possible to parallelize the
18 analysis of the logs from the ongoing operation of
19 the system. I don't think that one needs to
20 burden the other.

21 Very often we've seen situations in which
22 analysts, it's actually helpful for analysts to

1 have real time assessment of the policy impact of
2 a query they're proposing or a conclusion they're
3 reaching. Can I use that conclusion for a certain
4 purpose or not?

5 You know, that's where it's important
6 that we have adequate computational efficiency to
7 get that answer in the time that the analyst needs
8 to make a decision. But I don't think that
9 there's a reason to worry that one burdens the
10 other.

11 I do think it is the case that, and my
12 guess is the agencies would say, well, they're
13 going to have to spend money on it, and that's
14 true.

15 MS. BRAND: Beth started the practice of
16 giving homework in the last panel, so I know we're
17 just about out of time here so I don't want to
18 make all of you go down the line and answer, but I
19 actually was focused on the same comment, Danny,
20 that Beth just mentioned.

21 You said something like, we're not very
22 good at figuring out how information is used and

1 whether it's consistent with the rules and we've
2 started to learn how to design the systems but
3 haven't figured out how to deploy them on a large
4 scale.

5 So you know, you presumably are not privy
6 to whatever the NSA is doing to audit its own
7 systems and so there's sort of the front end
8 restrictions, such as who can access it and what
9 the supervisory levels of authority are there, and
10 then after the fact whatever the audit trail is
11 and, you know, that's not public necessarily.

12 But it occurred to me that in the current
13 context with Snowden, his leaks are viewed to be a
14 national security risk because the things that
15 he's leaking are more structural in nature. But
16 you could also imagine a situation where somebody
17 in a position like his wanted to leak things that
18 would violate peoples' privacy, so the underlying
19 data instead of the structural documents.

20 And so perhaps in your written statements
21 you can address this. Is there a way to design a
22 system that would kind of issue a red alert if

1 somebody is accessing data in a way that seems to
2 indicate that they are going to use it for that
3 kind of purpose, as opposed to violating an
4 internal rule that might not immediately violate
5 someone's privacy?

6 That's not a very well-formed question
7 but --

8 MR. SOLTANI: Hospitals have the same
9 complaints. So hospitals, you know, it's a
10 commonly known thing that people will leak when a
11 superstar comes in and they'll leak it to the
12 press. So there are existing systems in place
13 that will do anomaly detection for access.

14 So why are you, if your region is here,
15 why are you accessing data on people? So it would
16 be much harder in a global, kind of in a global
17 operation, but.

18 MR. ROTENBERG: I just wanted to end with
19 a cautionary note here. You know when we talk
20 about audit logs in the 21st century this is not
21 simply the problem of a person accessing a data
22 set from a computer terminal. What we realize

1 increasingly is the amount of information that a
2 person can pull down from a system off of a server
3 and walk out with in something that's, you know,
4 smaller than a credit card is really remarkable,
5 right?

6 And I think this belief that through
7 carefully tailored audit logs we can ensure legal
8 compliance and prevent misuse has already been
9 demonstrated many times not to be a reliable
10 operating principle. So we --

11 MR. WEITZNER: Could I just very quickly
12 though differentiate between operational security
13 risks, which are real, and obviously Snowden and
14 Bradley Manning have demonstrated that there are
15 very real operational risks, and they can entail
16 privacy intrusions, as we saw with the WikiLeaks
17 situation to great harm.

18 But I would distinguish that from policy
19 compliance problems where in fact the assumption
20 is that an institution, or at least large parts of
21 an institution is prepared to be accountable to a
22 set of rules, but because we don't have fine

1 grained enough, precise enough audit mechanisms,
2 we allow a lot of fuzziness. We allow fuzziness
3 about who is a U.S. person or not because we can't
4 determine it. We allow fuzziness about what's a
5 terrorism investigation use and what isn't.

6 We can get much more precise and close
7 these gaps. I agree with Marc that there are, the
8 rogue insider problem is not one that can be
9 solved with the kind of information accountability
10 that we're proposing.

11 I would suggest that it can be solved by
12 detecting, as Ashkan suggested, anomalous activity
13 by someone who's supposed to be infrastructure
14 analyst but is instead doing something else.

15 But I think, Marc, you're right to
16 distinguish the two, but I don't think that the
17 difficulty of doing one means that the other is
18 not useful.

19 MR. BELLOVIN: Here's a quote from
20 Bradley Manning, attributed to Bradley Manning in
21 the WikiLeaks case, weak servers, weak logging,
22 weak physical security, weak counterintelligence,

1 inattentive signal analysis, a perfect storm.

2 He was able to get away with downloading
3 all those documents because no one was paying
4 attention. The stuff wasn't being logged or no
5 one was paying attention. Yeah, someone
6 downloading 250,000 documents that should have
7 tripped a flag, if there were enough audits and if
8 people were paying attention.

9 And that's about, that's an anomaly and
10 that's about the best you can do there.

11 MR. DEMPSEY: With that, I think we will
12 bring this to close right at the top of the hour.
13 Thank you all very much.

14 MR. MEDINE: And we're going to take a 15
15 minute break and then we'll pick up with the third
16 panel. Thank you.

17 (Off the record)

18 MR. MEDINE: So welcome to our third
19 panel on policy issues, and I'll turn it to Beth
20 Cook to introduce the panel.

21 MS. COLLINS COOK: So thank you all for
22 joining us for this third panel of the day, that

1 certainly for me, and I hope for my colleagues and
2 for all of you, has been very informative and very
3 thought provoking.

4 So we turn now to the third panel, where
5 we are joined by six very distinguished experts in
6 this field.

7 And from left to right we have with us
8 Jim Baker, who is a former Department of Justice
9 official and lecturer at law at Harvard Law
10 School.

11 To his left we have Mike Davidson, who
12 served as both minority counsel and then general
13 counsel for the Senate Select Committee on
14 Intelligence.

15 We then have Sharon Bradford Franklin,
16 who is senior counsel with The Constitution
17 Project.

18 Then Liza Goitein, who is the codirector
19 of the Brennan Center for Justice's Liberty and
20 National Security Program.

21 Greg Nojeim, who is the director of the
22 Project on Freedom, Security and Technology at the

1 Center for Democracy and Technology.

2 And Nathan Sales, who is a law professor
3 at George Mason and former Justice Department and
4 Department of Homeland Security official.

5 So we're going to structure our panel
6 just a little bit differently than the first two
7 panels. We're going to start with a question.

8 And the question, and we will allow each
9 of the pnaelists five minutes to respond and then
10 a two minute secondary response, is the following,
11 we begin by asking whether based on the publically
12 available information you have any recommendations
13 for change to the programs or whether you believe
14 the programs appropriately balance the potentially
15 competing interests?

16 And Jim, going alphabetically, I would
17 invite you to start.

18 MR. BAKER: Well, thank you. Thank you
19 very much for the invitation to speak before the
20 board. I appreciate this opportunity.

21 And I just would say at the outset I'm
22 speaking just for myself today, not on behalf of

1 any current or former employer, employers.

2 And so with respect to thinking about
3 these issues, I mean I guess if I could just for a
4 moment take it up a higher level to sort of make
5 sure that we're thinking about these problems in
6 the right way.

7 And I guess one of the disadvantages of
8 going last is that a lot of people have said a lot
9 of things and you guys have talked a lot about a
10 lot of things today. But I also get to sort of
11 react and reflect a little bit on what has been
12 said.

13 And so at the outset, you know, I'm
14 sitting in the back and watching what was going on
15 and thinking about your banner here and thinking
16 about the name of the panel and so on, and it was
17 striking to me that really at the end of this
18 session, I think some of the fundamental, some
19 parts of the name of this board, there is still
20 not agreement on and there was not agreement about
21 today. And I think that complicates your task.

22 So for example, what does privacy mean?

1 I think you saw several different versions or
2 several different visions of that during the
3 discussions today. I don't think there is wide
4 agreement on what that means today. And I think
5 that's one of the issues that we're confronting.

6 And let me back up. There may be wide
7 agreement that there is at least some significant
8 disagreement, let me put it that way.

9 The same is true with respect to the term
10 civil liberties. What exactly does that mean? It
11 ties right into what is privacy and how do people
12 think about this and how do we think about this in
13 the current era in terms of the types and the
14 variety of communication facilities and devices
15 that people use on a regular basis.

16 And then how do we think about that with
17 respect to the changes and the growth in the
18 government's ability to conduct surveillance and
19 to store and analyze and understand data.

20 Another thing that was striking to me
21 obviously with respect to the name is oversight
22 and what does that mean and how do we think about

1 that?

2 And reflecting upon these programs that
3 we're talking about today, I guess my question is,
4 how much more oversight do you want? Because
5 you've got all three branches of government
6 involved in these particular activities we're
7 talking about. You've got the President, you've
8 got Congress, you've got the courts, you've got
9 lawyers all over the place running around doing
10 oversight. And so the question is, you know, how
11 much more really do you want?

12 And that, then I was thinking about,
13 well, okay, so what's going on here? What's
14 really at issue? And so a couple of different
15 things.

16 One is that either people, the people who
17 are critics of these programs either don't like
18 the design that exists today, the design that's
19 come up, that was passed by Congress, signed by
20 the President and put into place, put into
21 practice, implemented by the court, either you
22 don't like the design or you don't like the people

1 that are implementing the design. It's one of the
2 two. I don't know what else there would be.

3 So that is a significant problem. And
4 it's a significant problem that reflects, I think
5 even a deeper issue that you have to try to think
6 about, and I'm not sure how you're going to deal
7 with this.

8 I'm not sure that I have, I certainly
9 don't have the answer, but it's this, at the end
10 of the day if all three branches are involved
11 there remains some fundamental distrust of the
12 government and the structures that the government
13 has put into place and the people who are
14 implementing these things.

15 I mean I think that is what is underneath
16 a lot of the critique and criticism. And I don't
17 know how you deal with that. So that's point
18 number one, I guess just in terms of reflection.

19 In addition, in terms of before I talk
20 about solution, I do want to just mention briefly
21 that these issues are even more challenging than
22 we've talked about today. And I'll just briefly

1 state we have the cyber threat that we have to
2 deal with.

3 All of the things we've been talking
4 about today with respect to terrorism exists even
5 to a more significant degree with cyber because of
6 the volume of communications involved, because of
7 the variety of the different types of
8 communications involved, and because of the
9 velocity of the communications.

10 All of those make all the issues
11 regarding the collection and the analysis of
12 metadata and content even more difficult.

13 So with that said, in terms of trying to
14 think about structural changes and refinements in
15 the law and what you can do to move forward, I
16 don't think that anybody is going to have a
17 perfect solution to you, to describe to you today.

18 You can, I think, do some things at the
19 margins to try to improve these statutes, but you
20 know, I'm just really not sure what you can do to
21 have more oversight of these activities that
22 impact privacy and civil liberties. I think it's

1 just a very tough nut to crack.

2 Having said that, let me just make a
3 comment. One of the things that I recommend that
4 you think about is to try to simplify the range of
5 laws that apply in this area.

6 What we have right now, and others have
7 made this observation, what we have right now is a
8 very complex patchwork of statutes that overlap
9 with each other.

10 And I can tick them off. It's not only
11 FISA, it's Title III --

12 MS. COLLINS COOK: Actually before you go
13 through the full list, we have six panelists so
14 we're unfortunately going to have to be a little
15 bit stricter on this panel than the last panel.
16 Simplicity.

17 MR. BAKER: Okay. Simplicity.

18 And think broadly about the laws that are
19 applied to the surveillance of content and
20 metadata.

21 MS. COLLINS COOK: Thank you.

22 MR. DAVIDSON: Is that a color coded --

1 MS. COLLINS COOK: It is indeed. We have
2 a very helpful green --

3 MR. DAVIDSON: There are not numbers?

4 MS. COLLINS COOK: There are no numbers.

5 MR. DAVIDSON: No numbers?

6 MS. COLLINS COOK: No numbers

7 MR. DAVIDSON: Red means stop.

8 If I could address perhaps a variant of
9 the question that you asked and address it in
10 these opening comments, not the specifics about
11 what might be done with these programs but the
12 conditions upon which they are discussed in
13 several important places, one being the judicial,
14 branch, the second being in the Congress, and then
15 particularly looking forward to the next set of
16 sunset debates, and the third more generally in
17 the public.

18 With respect to the judicial branch
19 there's of course been a discussion that's gone on
20 since, well at least since 2008 about greater
21 public information about the major decisions of
22 the FISA Court, its reasoning as it approached

1 various segments of FISA.

2 And nominees have come before Senate
3 committees and have pledged to proceed on. And
4 that's been going on since 2008, and maybe we're
5 on the verge of a breakthrough.

6 But without even looking to the past as
7 to what the court has done, bear in mind that in
8 the public information about business records it
9 now appears publicly that those orders are 90 day
10 orders.

11 And so there's some cycle going on before
12 the FISA Court, which would mean that in days, or
13 at least within months there will be an occasion
14 for the FISA Court's consideration of the extent
15 of any such orders, the legal basis for them.

16 And then with respect to the development
17 of the program under the FISA Amendments Act,
18 Section 702 of FISA, that's an annual cycle. The
19 statute doesn't limit the government to any
20 particular one year order or how it packages what
21 it does, but it does say that those authorizations
22 are for no more than a year.

1 And each time the FISA Court considers
2 the government's submissions to authorize another
3 year's collection, it has the statutory
4 obligations that it has at the outset.

5 Central to those is to consider the
6 compliance that the government system of targeting
7 and minimization and other aspects of the statute
8 have with both the terms of the statute and with
9 the Fourth Amendment.

10 The statute reiterates the expectation
11 and the requirement that the court will consider
12 the Fourth Amendment in approving or not approving
13 its annual authorizations.

14 And so within weeks or months, but
15 certainly within the year, there will be an
16 occasion before the FISA Court to consider the
17 basic elements of the authorization that's allowed
18 under section 702.

19 I think that this board, given its
20 charter and its stature, can play a very important
21 role in helping to improve that process so that
22 there is a greater confidence that the FISA Court

1 in fact is dealing with the basic issues that have
2 been discussed earlier today, and are being
3 discussed in the larger society, and that there
4 are models out there.

5 So that in 2002, when the FISA Court of
6 Review considered legal issues relating to the
7 wall between intelligence and criminal
8 investigations, the Court of Review had a process
9 in which outside groups came in, filed amicus
10 briefs, and the court in its disposition of the
11 matter addressed issues that had been raised
12 there.

13 And in 2008, when the Court of Review had
14 an appeal from the Protect America Act, which had
15 a resemblance to, but it's far from identical to
16 the system created by the FISA Amendments in 2008,
17 it issued a public opinion. It redacted portions
18 of it, but the public opinion dealt with
19 substantial legal issues.

20 So finding a way for people outside the
21 system to bring before the FISA Court important
22 legal issues and for the FISA Court to then

1 communicate to the public at large is something
2 that's been experienced.

3 Now the modeling of it could very well be
4 different and it would take an initiative, I would
5 believe, by the Department of Justice.

6 And I do believe that the board in its
7 communications with the Executive Branch could
8 help to make the case that we're now at a point in
9 which there should be that form of public
10 discussion.

11 And perhaps it could go to the extent of
12 helping to identify the questions that should be
13 considered on a public record.

14 Now the intelligence community is going
15 to have some choices to make. It is loathe, and
16 understandably loathe, when there have been
17 improper disclosures to acknowledge the validity
18 of those disclosures.

19 But there's also a reality out there. In
20 fact, there appears to be public information about
21 matters that are at the heart of the annual
22 approval, of the targeting procedures of the

1 government, and the minimization procedures of the
2 government.

3 And some way can certainly be found to
4 now call for a process in which those are
5 discussed against the requirements of the statute,
6 which are both statutory and the call for an
7 annual consideration of Fourth Amendment
8 compliance.

9 MR. MEDINE: Let me just make also, in
10 the interest of time and moving on, I think --

11 MR. DAVIDSON: You can interpret that as
12 red?

13 MR. MEDINE: That's our timekeeper. So
14 if you have additional comments you can make them
15 in a later round.

16 MR. DAVIDSON: Sure.

17 MR. MEDINE: We appreciate that. Sharon.

18 MS. BRADFORD FRANKLIN: Thank you very
19 much for the opportunity to appear here today, and
20 I have already filed a lengthier statement on
21 behalf of The Constitution Project so I will be
22 more brief in my comments.

1 The short answer to your question is yes,
2 we do believe that there are changes that should
3 be made. And I just want to make two quick points
4 before I get to summarizing what some of those
5 recommendations are.

6 First, with regard to the PCLOB's role in
7 assessing counterterrorism programs and whether
8 the safeguards for privacy and civil liberties are
9 appropriate, part of that role obviously, and the
10 discussion at this morning's panel was whether
11 existing programs comply with existing law
12 including the Constitution.

13 And that is a very important assessment
14 and we have already filed in our prepared comments
15 our views on some likely legal violations there.

16 But beyond that, the PCLOB's statute
17 talks about assessing whether the protections are,
18 quote, appropriate, and, quote, adequate.

19 The board is not limited to making
20 recommendations for compliance with the
21 Constitution and existing law. And so I would
22 urge you to be forward-leaning in the

1 recommendations that you do make.

2 There will be plenty of voices within the
3 government pushing for strong powers in
4 counterterrorism. And we know now from the recent
5 disclosures that the administration, whatever
6 administration it is, is likely to interpret
7 existing law aggressively to the maximum extent
8 that they believe they can justify under the words
9 of existing statutes.

10 So I urge you to really take seriously
11 the role to push for adequate and appropriate
12 safeguards in law to make sure that we're
13 protecting both our security and our civil
14 liberties.

15 Second, the PCLOB's statute explicitly
16 provides a role for informing the public,
17 including holding forums like today, and in making
18 sure that you're of course including the reports
19 to Congress are available to the public to the
20 greatest extent possible.

21 And I think that this transparency role
22 is really a critical one the PCLOB can play, in

1 addition to making specific recommendations for a
2 forum. And there's been a fair amount of
3 discussion about that in the earlier panels, but I
4 would urge you to take that role seriously, the
5 place where you really can make significant change
6 in pushing for a full disclosure.

7 The administration so far has been trying
8 to release some more information in response to
9 the leaks, but I don't get the sense that we're
10 getting a full picture.

11 They are perhaps, you know,
12 understandably picking the facts to release that
13 they think will support their case. And you are
14 authorized to get a full picture and to hopefully
15 push for more of a full picture to the public.

16 So I'll try to be somewhat brief in
17 summarizing the recommendations. We did outline
18 some in fair detail in our written comments.

19 And I just want to emphasize that a lot
20 of, most of the recommendations that are included
21 in our comments are actually ones that come from
22 The Constitution Project's Liberty and Security

1 Committee, which is a bipartisan committee, well
2 before any of these disclosures.

3 These were things that our committee felt
4 were necessary to better protect privacy and civil
5 liberties, just looking at the statutes before we
6 knew more details about how they are being used.
7 And they fall into a couple of categories.

8 First, tightening the standards for when
9 the government should be able to collect
10 information in the first place. Second,
11 regulating very strictly what uses can be made of
12 the information once it is collected. And third,
13 again, on transparency.

14 As far as tightening the standards, it's
15 very important that we have strict rules to
16 require a sufficient connection to terrorism
17 before this information is collected.

18 The sheer fact that it is useful to the
19 government for counterterrorism cannot possibly
20 comply with Fourth Amendment standards and it's
21 not the kind of society that we live in.
22 Usefulness is not enough. We need to make sure

1 that there's a connection to terrorism.

2 And frankly, this should help the
3 efficiency of the programs too. We want the
4 surveillance to be conducted on the, quote, bad
5 guys and the people we have reason to believe that
6 they are a connection to terrorism.

7 In the context of Section 215, although
8 we do not believe that the existing law does
9 authorize the bulk collection of the telephone
10 metadata that has been reported, although I
11 haven't seen the underlying order, we would urge
12 that at this point Congress should, you should
13 recommend that Congress amend the Act to clarify
14 that that's not permitted under 215 or any other
15 authority, and specifically recommend tightening
16 the standard for issuing an order under Section
17 215 to require a showing to a judge of specific
18 and articulable facts demonstrating that the
19 material sought pertains to a suspected agent of
20 a foreign power or a person in contact with or
21 directly linked to such an agent. So restoring
22 some of the earlier standards.

1 In the context of Section 702, we have
2 similar recommendations to restore the requirement
3 that foreign intelligence be the primary purpose
4 of the surveillance, and also to require the
5 government to make a greater showing to the FISA
6 Court of the actual foreign intelligence purpose,
7 and more of a showing that it is not likely that
8 it will be intercepting large quantities of
9 communications of U.S. persons.

10 We've heard a fair amount of discussion
11 this morning about justifying collection where an
12 American is on the other end, I'll try to be quick
13 here, when we know it is targeted at a foreigner.
14 But we need to make sure that the word incidental
15 has more of its common, everyday meaning in that
16 targeting.

17 Then there should also be strict limits
18 on data once it is collected. We had reference,
19 Judge Robertson mentioned a recommendation that we
20 made for post-collection warrants in the context
21 of 702. I'd be happy to discuss that more in the
22 questioning, if you are going to seek information

1 on a specific U.S. person in an existing database.

2 And finally, we have a series of specific
3 recommendations on transparency, including
4 releasing significant opinions of the FISA Court
5 and more details on the extent of interceptions of
6 U.S. person information that have gone on in the
7 past.

8 And I appreciate the opportunity. Thank
9 you.

10 MR. MEDINE: Thank you.

11 MS. GOITEIN: Thank you very much for the
12 opportunity to participate.

13 On this panel, as you said, our task is
14 to leave aside the question of the program's
15 legality and focus on whether they strike the
16 right balance between our security and our
17 liberties. And I believe that the known threat to
18 liberty from these programs exceeds any known
19 benefit.

20 Now in my line of work I often get
21 accused of invoking phantoms of lost liberty, as
22 John Ashcroft once said. So let me start by

1 saying that I recognize that this is a remarkably
2 free country. The vast majority of Americans go
3 about their lives and speak their minds without
4 fear of persecution.

5 But that has not always been the case at
6 periods in this country's history. Throughout
7 much of the cold war our law enforcement agencies
8 and our intelligence agencies spied on Americans,
9 not solely for the purpose of preserving security,
10 but sometimes for the purpose of impeding social
11 justice movements or harassing political enemies.
12 Innocent Americans had their careers and sometimes
13 their lives ruined.

14 When these abuses came to light in the
15 1970s, Congress and executive agencies implemented
16 a range of laws and policies that establish a kind
17 of golden rule. And that rule was law enforcement
18 and intelligence agencies may not collect
19 information on Americans unless they have some
20 level of individualized, fact-based suspicion that
21 the person is involved in some kind of wrongdoing
22 or is an agent of a foreign power.

1 Now the exact level of suspicion would
2 depend on the kind of information the government
3 wanted to get and how. This golden rule served us
4 well for decades.

5 The 9/11 Commission found fault with a
6 lot of government practices, but it never said we
7 need to collect more information about Americans
8 with less reason for suspicion.

9 Nonetheless, since 9/11 we have seen a
10 steady and rapid erosion of the level of suspicion
11 that is required for our law enforcement and
12 intelligence agencies to collect on Americans.

13 The FISA Amendments Act, national
14 security letters, FBI assessments, electronic
15 border searches, these are all instances in which
16 the required level of suspicion has been lowered,
17 in some cases to zero.

18 The programs we're talking about today
19 fall squarely within this category. Section 215
20 already weakened preexisting law by allowing the
21 acquisition of tangible things with a very low
22 showing of relevance.

1 We've now learned that the government and
2 the FISA Court have interpreted relevance largely
3 out of existence, so there's no individualized
4 showing required to get information, American's
5 information.

6 That means it's up to the Executive
7 Branch to police itself when it comes to actually
8 using that information.

9 Section 702 of the FISA Amendments Act on
10 its face doesn't require any individualized
11 suspicion. Now it targets foreigners overseas
12 nominally, but what we've learned is that the
13 government Section 702 programs tolerate a massive
14 amount of so-called incidental and inadvertent
15 collection of American's information.

16 Again, this incidentally acquired
17 information is nominally master deleted, but that
18 relies on self-policing. And also, if you look at
19 the targeting and minimization procedures, they
20 tell a much more complex story in which there are
21 many loopholes for keeping and sharing this kind
22 of information.

1 When you get rid of the requirement of
2 individualized suspicion for collecting on
3 Americans, you reopen the door to the kinds of
4 surveillance abuses we saw in the 40s, 50s, 60s
5 and 70s.

6 And when you free government officials
7 from the requirement of some sort of factual
8 predicate for investigation, you open the door for
9 them to fall back on conscious or subconscious
10 prejudices, whether racial, or religious, or
11 ethnic, or political.

12 Now if there were evidence that these
13 programs were uniquely effective, then we might be
14 willing to risk these downsides, but the burden
15 should be very high in terms of the proof we
16 require. And to date, all the government has told
17 us is these programs have helped to disrupt
18 terrorist plots.

19 That's not even the relevant question.
20 The question is, have these programs thwarted real
21 significant terrorist attacks that could not have
22 been prevented using more narrower methods or more

1 narrow methods?

2 So I'm very much hoping that the PCLOB
3 will insist on getting the information necessary
4 to make that assessment. And if it turns out that
5 these programs are useful and if it turns out that
6 they comply with the Fourth Amendment, then as a
7 society we'll have a very difficult choice to
8 make.

9 Until then, we are weighing a known and
10 serious risk to liberty against an unknown and
11 unproven benefit.

12 MR. NOJEIM: Hi, I'm Greg Nojeim. I'm
13 with the Center for Democracy and Technology. As
14 it happens one of the PCLOB members is also
15 employed by CDT. We have walled off our work from
16 each other and don't discuss PCLOB issues.

17 I think we've strayed a long way away
18 from the world that was envisioned in our
19 Constitution where you don't have to worry about
20 government surveillance unless there's evidence
21 that you're up to no good. My gosh, we've moved
22 so far away from that.

1 When it comes to these two programs I
2 don't think that they adequately protect privacy,
3 and I will focus with respect to the Section 702
4 program primarily on transparency, where I think
5 PCLOB can play a huge role. And with respect to
6 the 215 program --

7 MR. MEDINE: Move the mic closer to you.

8 MR. NOJEIM: With respect to the 215
9 program, I think that one is illegal and that the
10 PCLOB should make a recommendation that it be
11 discontinued.

12 On 702, there are some critical questions
13 about FISA Amendments Act surveillance that have
14 never been answered that we would urge you to take
15 up in your report, or to encourage government
16 officials to answer.

17 The first is whether the FAA can be and
18 is being used to do bulk surveillance. That means
19 surveillance of a large quantity, a large
20 proportion of the communications between Americans
21 and people who are abroad.

22 Because you can target anyone you

1 reasonably believe to be abroad, just how much of
2 that surveillance is going on?

3 Second, the Washington Post reported that
4 when it comes to targeting that a 51 percent
5 likelihood of foreignness was good enough. Well,
6 it's not good enough for me and I don't think it's
7 good enough for the American people. That's a
8 coin flip level of certainty.

9 I would think that there would be, and
10 the procedures that have been leaked suggest that
11 there is, more attention to foreignness than
12 that. But I think PCLOB could play an important
13 role in clearing up the 51 percent number.

14 I also think that when you look at the
15 purpose for which the surveillance can be
16 conducted in the 702 program, it's very broad.
17 And I would think that all of the surveillance
18 that's authorized under that program is not being
19 conducted because it wouldn't be useful.

20 For example, it appears that because
21 collecting foreign intelligence information is all
22 the purpose that you have to have, that that would

1 cover, for example, collecting up all the email of
2 people that have protested outside a U.S. base in
3 Germany. I don't think that the government is
4 ordering U.S. providers to turn over all the
5 information because I don't think it's really what
6 the government is looking for.

7 What I think is needed for 702, in
8 addition to more transparency, is more FISA Court
9 involvement, not less, where the FISA Court
10 actually authorizes the surveillance, not just
11 guidelines.

12 And I think that the PCLOB should give
13 consideration to the purpose of the FISA
14 surveillance and whether it could be limited to 18
15 U.S.C.(e), I'm sorry, I don't have the exact
16 statutory citation here. But just the first part
17 of the definition of foreign intelligence
18 surveillance, which would make it much more
19 limited.

20 With respect to Section 215, I think that
21 that surveillance is unlawful. It's overbroad.
22 It can't be the case that everyone's telephone

1 records are relevant to an investigation because
2 if that's true, then everyone's records of any
3 type are relevant to an investigation because they
4 fit into a mosaic and could be used to engage in
5 more learning about what might be actually
6 relevant.

7 I think the most important change to
8 Section 215 is the one that Sharon outlined to
9 require that there be a tie to an agent of a
10 foreign power, specific and articulable facts
11 giving reasonable grounds to believe that the
12 information sought pertains to an agent of a
13 foreign power or a person in contact with such a
14 person.

15 I think also the PCLOB should make it
16 clear, I think this is already clear in the
17 statute but apparently not to the NSA, that
18 Section 215 is not about prospective surveillance,
19 it's about records already in existence.

20 Perhaps an exclusive means provision
21 should be added to the pen trap statute to make
22 that entirely clear.

1 There should be clarity about the
2 particularity that's required and more work on
3 transparency with respect to the surveillance.

4 Finally, I will just say this, I don't
5 think that FISC oversight is serving us adequately
6 at this point.

7 It seems to have been the case that one
8 judge of the FISC issued the orders that
9 determined that this information about all phone
10 calls were relevant, and that when those orders
11 were issued, the other judges on the court didn't
12 even know. I mean that is not a system that I
13 think has the oversight that Congress intended.

14 There ought to be explicit authority to
15 consider all constitutional claims, and I think
16 the idea of an ombudsperson is a very good one,
17 and I'd like to discussed that later.

18 MS. COLLINS COOK: Thank you.

19 MR. SALES: Thank you to the members of
20 the board and my fellow panelists for asking me to
21 participate in this important and interesting
22 conversation.

1 I'd like to take a step back and look at
2 the big picture concerning surveillance. It seems
3 that the programs that have been leaked to the
4 press are examples more or less of what we might
5 call programmatic surveillance. Greg called it
6 bulk data collection.

7 Programmatic surveillance is something
8 that's familiar to a lot of intelligence
9 personnel, but those of us who are lawyers
10 probably haven't encountered it all that much.

11 We're more familiar with individualized
12 surveillance where cops think that Tony Soprano is
13 up to no good, they therefore ask a court for
14 permission to wiretap him to come up with evidence
15 that they can use to prove his guilt.

16 You move, with individualized
17 surveillance you move from suspicion, to an
18 individual, to evidence.

19 Programmatic surveillance is in a sense
20 the exact opposite of that. We don't have a
21 particular target in mind. In fact, the whole
22 point of the surveillance is to develop enough

1 information so that we can find the bad guys.

2 So programmatic surveillance therefore
3 relies on bulk data collection and screening it
4 through various algorithms or analytical processes
5 to identify pieces of information, individual data
6 points that might be important.

7 Programmatic surveillance, I think what
8 I'd like to talk about is its potential benefits
9 and how to do it in a way that respects privacy
10 values, and rule of law, and civil liberties
11 values as well.

12 The benefits are fairly straightforward.
13 Programmatic surveillance is an important tool for
14 identifying unknown associates of known
15 terrorists. The process is called, as you know,
16 link analysis.

17 We know that Mohamed Atta is up to no
18 good, let's find out who is in his social network
19 because they may also be up to no good, and we can
20 use that to trigger further investigation.

21 There's a report from 2002 indicating
22 that a rudimentary form of link analysis actually

1 would have enabled investigators to identify all
2 19 of the 9/11 hijackers. Still, we start with
3 two hijackers who were known to have attended a
4 terrorist meeting in Malaysia. Let's look at
5 their passenger reservation data from their
6 various airlines travels and find out what we can
7 learn.

8 Well, it turns out that a number of
9 people had used the same frequent flier number as
10 these two terrorists. It also turns out that
11 other people had used the same addresses and
12 credit cards as these terrorists.

13 Building out from the initial two
14 suspects, it was possible to put together a fairly
15 detailed portrait of their social network leading
16 us to all 19 of the 9/11 hijackers.

17 So programmatic surveillance has the
18 potential to yield some important national
19 security gains, not merely hypothetical ones, but
20 actual concrete national security gains.

21 The question for me is, how do we do it
22 in a way that is consistent with our rule of law,

1 values, and with our commitment to privacy and
2 civil liberties.

3 I want to propose a series of principles
4 that I think can help guide our judgment as to
5 whether any particular program, including these
6 programs, live up to our values in addition to
7 protecting us from national security threats.

8 There's two basic sets of principles that
9 I personally would like to see reflected. The
10 first set has to do with the formation, the
11 architectural considerations. When building a
12 system of programmatic surveillance, how should we
13 design it?

14 And the second set of considerations
15 concerns operational features. What sorts of
16 safeguards should we build into the system so that
17 when it operates it does so in a privacy and civil
18 liberties friendly way?

19 As far as formation goes, one of the most
20 important principles to me is anti-unilateralism.
21 The Executive Branch shouldn't be doing
22 programmatic surveillance on its own. It should

1 rather have to obtain authorization, legal
2 authorization from Congress, perhaps also from the
3 judiciary. There have been examples of the
4 judiciary signing off on and approving in bulk
5 programmatic surveillance programs.

6 I also favor maximum transparency and
7 public debate. The public should be informed of
8 the government's plans as much as is possible with
9 operational security, so that an informed
10 deliberation in the public can take place and so
11 Congress's deliberations can thereby be informed.

12 I also want clear legal authorization for
13 programmatic surveillance. I think it's important
14 for Congress not to hide elephants in mouse holes.

15 If we're going to have a system that
16 authorizes bulk data collection, it should be
17 approved transparently and expressly, rather than
18 something that's simply hidden in the penumbral
19 emanations of various other statutory provisions.

20 I also think it is important to prevent
21 mission creep. These are important tools to be
22 used to protect against existential threats and

1 mass murderers. I don't think we should be using
2 these sorts of tools to go after tax cheats. I
3 want a firewall that prevents those sort of tools
4 from bleeding over into routine ordinary
5 investigations where a lot less is at stake.

6 As far as the operational principles are
7 concerned, the basic idea here I think is to
8 substitute for restrictions on the collection of
9 data, restrictions on the use of data.

10 As the government acquires more and more
11 information on the front end, it becomes more and
12 more important to substitute on the tail end
13 restrictions on who can access it, what can be
14 done with it and so on.

15 I see I'm nearly out of time so let me
16 just finish this thought very briefly. There's a
17 couple different type of checks you could have in
18 mind, external checks, judicial oversight, ex-ante
19 approval before you conduct surveillance or access
20 the data, ex post oversight audits and reviews of
21 surveillance that has taken place in the past.

22 Internal checks are also an important

1 part of the conversation, inspectors general, the
2 PCLOB itself, and other forms of internal
3 Executive Branch oversight can help prevent the
4 sorts of abuses we saw in the 70s and that nobody
5 wants to go back to. Thank you.

6 MS. COLLINS COOK: Thank you all. And we
7 will now ask you to, if you have some thoughts,
8 two minutes each.

9 And one thing I did want to mention, and
10 building on something that Jim had said earlier
11 was that we're really looking for solutions here.
12 We're very much looking for recommendations, we're
13 looking for concrete and specific ideas that can
14 be discussed, that can be assessed, that can be
15 analyzed.

16 And you know, we spent a lot of time
17 today on the framework of what we're talking
18 about, and I hope that over the rest of the day
19 that we can really start exploring some very
20 specific options for how these programs might be
21 done differently if necessary.

22 MR. BAKER: Okay. So let me focus on

1 that and try to get very, there's a lot of stuff
2 to talk about. Let me focus on one thing in
3 particular, transparency.

4 MS. COLLINS COOK: Yes.

5 MR. BAKER: Okay. So back to my earlier
6 comment in terms of that may be one thing that
7 would help enhance trust in government, okay.

8 So with the transparency of the FISA
9 Court orders and FISA Court proceedings, so I've
10 got just a couple of observations.

11 And just by way of background, I was in
12 charge of representing the United States in front
13 of the Foreign Intelligence Surveillance Court
14 from 1998 till 2007. So I dealt a lot with the
15 court in that time period.

16 Two things. One, this will be easier
17 going forward than it will going back. So if
18 Congress were to mandate in legislation that from
19 here on some type of rulings by the FISA Court
20 would have to be disclosed, then that's going to
21 be easier because the judges, I think, will be
22 able to write opinions knowing that that's the

1 case.

2 Going back I think there's two problems.
3 One is the intertwining, I think this is why it's
4 taking so long to declassify all this stuff is
5 that the intertwining of classified facts with
6 legal analysis as you go through makes it
7 difficult to extract the two pieces in a way that
8 will give the American public any real
9 information, as opposed to just pages and pages of
10 blacked out stuff, or text with a lot of blacked
11 out stuff. So going forward I think will be
12 easier than going back.

13 Secondly, you have to understand that not
14 everything that the FISA Court does is reflected
15 in some opinion, I think Judge Robertson was
16 talking about this before, some opinion that's
17 what like you're used to seeing in the normal
18 judicial proceedings with other courts.

19 A lot of it is based on you submit an
20 order, the court says, hmm, you want to do X,
21 well, we think you should have minimization
22 procedure Y to go along with that. The government

1 works that out, okay, fine. Then the next time
2 you file it, you just have X plus Y is built into
3 the package. There was never any opinion. There
4 was never any ruling like that. It's just an
5 order from the court and that's what you have.

6 So there's a lot of back and forth that
7 is not going to be apparent in some kind of big
8 judicial opinion like people think about.

9 MR. MEDINE: Just to clarify the
10 recommendation, so would you envision on the going
11 forward basis that where there are opinions that
12 there essentially be an unclassified summary or
13 syllabus of the decision and there be a
14 classified, more detailed decision addressing the
15 specific facts of the case or something that they
16 need to be classified?

17 MR. BAKER: Basically, yes, because that
18 way if the court is writing the summary, the court
19 can say what it wants to say knowing whether it
20 will become public. As opposed to somebody, I
21 mean I'm sensitive to this, as opposed to somebody
22 else writing some summary of some decision that

1 was written, and whether they get it right or not
2 is another matter.

3 MS. COLLINS COOK: And Jim, on that
4 point, I think one of the things we've struggled
5 with is I think it's too strong to say it's a red
6 herring, the declassification of previous opinions
7 issued.

8 And one thing I would like your opinion
9 on is whether or not it would be likely a more
10 efficient course to simply direct a summary of
11 past opinions, rather than to go through a
12 declassification process of existing documents.

13 MR. BAKER: It would be more efficient,
14 the question is would it be accurate and would
15 people trust it. And would it accurately reflect
16 what the judge's, or that particular judge who may
17 not be on the court anymore, actually thought when
18 he or she wrote that opinion. That's I think the
19 trouble that you'll have.

20 So I'm not sure that that -- I'm not sure
21 it's going to work in terms of summary.

22 You could, I mean I guess you could have

1 some type of analysis, I don't know, by OLC or
2 something, where you mandate an analysis,
3 comparison of the body of FISA Court law with the
4 body of law that's out in the public. I don't
5 know, you could think about things like that as
6 well.

7 MR. DAVIDSON: Well, the government has
8 experience in producing public documents based on
9 underlying classified documents.

10 So in January of 2006, the Department of
11 Justice took a portion of a May 2004 OLC opinion,
12 a portion that then dealt with the January of 2006
13 concern, content collection under the President's
14 surveillance program, and it produced a white
15 paper.

16 That white paper was extraordinarily
17 informative to the debate that then followed in
18 Congress because it pointed to the fact that the
19 government had been relying on the authorization
20 for the use of military force for the content
21 collection part of the President's surveillance
22 program, and it elicited a considerable debate and

1 ultimately legislation on what it took to convey
2 that there was some variant to collection under
3 FISA, to what extent was FISA exclusive in the
4 face of another statute.

5 So it has experience doing that. It has
6 recently produced a white paper on drugs, on
7 targeted killings. So it has done that.

8 And that also gets done in any litigation
9 in which there may be classified information in
10 which the government works with the court to
11 produce an unclassified version.

12 It also need not just be a summary.
13 There may be entire parts of a relatively small
14 number of decisions that are in fact unclassified
15 themselves.

16 And just do this to imagine it, if it is
17 significant what the term relevance means. It
18 wouldn't be surprising to find in a major decision
19 or two how the government asked the court to draw
20 from five different opinions of the United States
21 Supreme Court in order to understand what
22 relevance may mean in certain situations.

1 So just as another example, in the May
2 2004 OLC opinion, which was then made public in
3 2011, at least as to those parts that dealt with
4 content analysis, there's enough of an indication
5 there that relative to the question of
6 reasonableness the Department of Justice looked to
7 border search decisions of the Supreme Court, or
8 other decisions of the Supreme Court about how
9 much of some span of collected material needs to
10 be on point in order for a government search to be
11 a reasonable search.

12 So summaries are a possibility, but there
13 are other mechanisms that are available in order
14 to get the result of a broader public discussion.
15 And I think I've used my two minutes.

16 MR. MEDINE: Yeah, why don't we move on
17 to Sharon. Thank you.

18 MS. BRADFORD FRANKLIN: So two
19 recommendations on how transparency can improve
20 oversight.

21 One is by addressing the problem that
22 many of us have been talking about in terms of

1 secret law. So in the morning panel Ken Wainstein
2 made a comment that when members of Congress are
3 expressing, you know, surprise at how a law's been
4 interpreted, that's not what I thought I was
5 voting for, that's just like any other law.

6 Well, the difference, unlike the RICO
7 example he gave, RICO, there are published
8 opinions on how RICO's being used. You can see
9 what prosecutors are using that for.

10 Here it took a leak of a classified order
11 for us to know how Section 215 was being
12 interpreted. It shouldn't take a leak for us to
13 know the legal interpretations that the Executive
14 Branch and the FISA Court are applying.

15 Now that's different. There are
16 certainly going to be classified information woven
17 into those orders. I don't deny that in any way.
18 But the actual understanding of what the law means
19 should be public in the first place and that will
20 facilitate a meaningful public debate over whether
21 that's an appropriate use of the law in a legal
22 authority.

1 The second is greater transparency for
2 some of the auditing type practices that the
3 second panel was talking about, to some extent
4 that review again be classified. Maybe the FISC
5 can play a greater role, this board can play a
6 greater role, and Congress.

7 But in terms of reporting on the extent
8 to which the minimization procedures are actually
9 successful, to what extent are they limiting the
10 collection of American's information, how much of
11 that is being captured?

12 But to some extent we can have public
13 disclosure there as well on statistics that are
14 anonymized. There can be a much greater level of
15 public reporting on that as well, and that as well
16 can affect the public debate and have an informed
17 consideration over what those authorities should
18 mean.

19 MS. GOITEIN: Two quick responses to what
20 other panelists have said and then some
21 recommendations.

22 First Jim said that, you know, we have

1 all three branches in government engaging in
2 oversight, what more could we want? I think it's
3 important to point out that the oversight that we
4 have right now is a kind of oversight-lite.

5 Oversight by congressional committees in
6 skiffs looking at classified information does not
7 work the same way that regular congressional
8 oversight does because these are elected
9 representatives who answer to their constituents
10 and they answer to their donors.

11 And if those people aren't on the phone,
12 you know, Jack Goldsmith said this himself in his
13 book, Power and Constraint. The institutional
14 incentives are not there for robust oversight in
15 the intelligence committees. It's just not the
16 same as regular oversight in an unclassified
17 setting.

18 Similarly with the FISA Court, for all
19 the reasons we've talked about, it does not
20 operate in the way that a regular court operates.
21 So this is a slightly different version of
22 oversight than what we usually mean when we talk

1 about checks and balances.

2 On the point that programmatic oversight,
3 sorry, programmatic surveillance to try to
4 identify who the terrorists are necessarily means
5 bulk collection, I think we don't want to conflate
6 those things.

7 I agree that contact chaining can be a
8 very important way to find out who known or
9 suspected terrorists are talking to. You don't
10 need my metadata to do that. You don't need
11 Sharon's to do that. You work from the
12 information you have and you branch outward.

13 All of the examples the government has
14 given thus far, the Zazi example and any of the
15 other specific examples of how it's used its
16 authorities are examples that, from at least the
17 information the government has made public, did
18 not require bulk collect versus contact chaining
19 outward.

20 Finally on specific recommendations, I'm
21 talking fast, I agree with Sharon and Greg on how
22 to amend Section 215. I agree with a lot of

1 what's been discussed about the FISA Court.

2 On Section 702, I think it was Ken
3 Wainstein who said, well, it's not workable to get
4 individualized orders, and then we had Steve
5 Bradbury saying this is the way it's been since
6 1978.

7 FISA looked very different before 2007,
8 and it required individualized orders in order to
9 get any international communications involving
10 Americans.

11 Now we heard today that that became
12 unworkable because the FISA Court couldn't deal
13 with the number of orders. We heard that, I think
14 from Steve. I didn't hear Judge Robertson say
15 that. He seemed to be saying that the FISA Court
16 actually worked quite well except for the issue of
17 adversariality.

18 So my recommendation would be to go back
19 to the pre-Protect America Act of individualized
20 orders for any communication involving an
21 American. And I think that would be more
22 constitutionally sustainable as well.

1 MR. NOJEIM: It would be useful if
2 unclassified summaries of significant FISA Court
3 opinions were made public. It is important that
4 if you make that recommendation that you
5 articulate a standard that the summary must meet.

6 For example, in the Classified
7 Information Procedures Act the summary that the
8 defendant must receive has to provide the
9 defendant substantially the same opportunity to
10 defend as would the classified information
11 itself. That's a useful standard.

12 It's certainly not a standard that would
13 be appropriate here, maybe something along the
14 lines of, the summary must inform the public of
15 the nature of the legal question and how it was
16 resolved. That might be useful and that might not
17 even be enough.

18 How would the summary be prepared? In
19 the CIPA context the government prepares it and
20 then there is a fight, a fight about whether the
21 summary meets the standard. I think that then the
22 judge resolves that fight.

1 I think some fighting is good, and that
2 maybe there ought to be an ombudsperson who takes
3 the position that, who tries to take the public's
4 interests into account in having an adequate
5 summary.

6 And one word on programmatic
7 surveillance. We haven't done that on Americans.
8 We don't do that on Americans. We don't collect
9 all records about Americans for the purpose of
10 watching all of us.

11 Programmatic surveillance, if it occurs,
12 is something that's about people who aren't in the
13 U.S., I think. And if that's not the case, well,
14 we need to learn a little bit more about exactly
15 what programmatic surveillance is being conducted.

16 MR. SALES: I think Greg's right but not
17 for the reason he thinks he is. We don't do
18 programmatic surveillance on Americans because we
19 do not in fact look at the data of all Americans.

20 My understanding of the 215 program is
21 there's a distinction between the collection of
22 the data, which then goes into a warehouse like in

1 Indiana Jones, right, next to the Ark of the
2 Covenant.

3 And then the second stage of the process
4 is upon a showing of reasonable suspicion, the
5 individualized determination that we're all
6 calling for, or that some of us are all calling
7 for here, that is the moment at which humans
8 eyeball the data, right.

9 If you're an American, Google right now
10 knows an awful lot more about you than the NSA.
11 And the only circumstances in which the NSA is
12 going to be looking at the data that has been
13 collected under 215 is if there's a reasonable
14 suspicion that the data is relevant to an ongoing
15 investigation to protect against terrorism or
16 espionage.

17 Good, right, if there's relevant data to
18 a terrorism investigation, I think the feds should
19 be looking at it.

20 But I think the critical question is how
21 strong is that firewall that prevents the feds
22 from looking at that warehouse of data in the

1 absence of the necessary predication,
2 individualized suspicion? And that goes back to
3 the questions about oversight.

4 Now as far as specific recommendations
5 are concerned I have a couple. The first one is,
6 has to do with minimization. So I'm concerned,
7 having reviewed the minimization rules that were
8 leaked recently about mission creep.

9 I think the standard for the use of data
10 collected through programmatic surveillance for
11 other purposes is if we find evidence of federal
12 criminal, or actually criminal activity. I think
13 that's far too low a standard. These sorts of
14 tools are incredibly important for protecting
15 against terrorism.

16 The cost benefit analysis looks very
17 different however when we're talking about running
18 down a tax cheat who's two years behind on his
19 1040s, right. I prefer to see a much stricter
20 standard there.

21 You can use this information for
22 investigations of important federal crimes, or

1 crimes involving the threat of death or serious
2 bodily injury, or child exploitation, something
3 along those lines.

4 Also my second recommendation is to
5 consider more thoroughly whether Section 215 is
6 the appropriate vehicle for programmatic
7 surveillance of business records.

8 I can see some potential value in
9 collecting that data, right. In order to do
10 programmatic surveillance, in order to connect the
11 dots, you have to have a big data set. It's no
12 good to say we're only going to collect data on
13 Mohamed Atta if we don't know who Mohamed Atta is
14 in the first place. That's the whole point of the
15 collection is to develop the data field that
16 allows us to identify the bad guys. So it's no
17 good to say you can only collect on bad guys. We
18 don't know who they are.

19 I'm not sure that 215 is the appropriate
20 vehicle for doing this. As several other
21 panelists have said this seems to have been
22 intended to go for individual records rather than

1 bulk records, records already in existence rather
2 than mandating the creation of a huge data set.

3 So I think further exploration of whether
4 Congress should consider additional legislation to
5 put this on a more solid legal footing would be
6 appropriate.

7 MR. MEDINE: In the first panel in
8 particular we heard a lot of questions raised
9 about the FISA Court and how it could operate in
10 more of an adversarial way because that's how our
11 American litigation system works best is when
12 there are people on different sides.

13 And many states around the country have
14 public advocates appear in the utilities context
15 where a utility seeks a rate increase and
16 individual consumers don't come in and oppose it,
17 but there's a governmental entity, a public
18 advocate who comes in to argue the citizen's side
19 of that question.

20 Should there be an institutional, in your
21 view, institutional entity that appears as a
22 government entity or with appropriate security

1 clearances, who appears to oppose FISA Court
2 orders and have the chance to litigate with the
3 government, or should there be some other
4 structure to create more of an adversarial
5 context?

6 MR. BAKER: Sure. So this has been
7 talked about for years number and it's not been
8 adopted, and I can speculate why.

9 But so just a couple of quick
10 observations. So number one is you're trying to
11 balance, I think, the legitimate need for the
12 President to obtain timely and accurate foreign
13 intelligence information with the privacy and
14 civil liberties of Americans, right.

15 And so you're trying to do something
16 quick and well, okay. And so where you have to be
17 careful, I think in this area, this can be done, I
18 think you could create such an entity. You can
19 give, maybe it's a federal employee of some sort
20 and the person has the right clearances and
21 they're dropped into the system somehow. I mean
22 there's probably some way that you could work it

1 out.

2 But there is a lot of process that goes
3 on already within the agency before the request
4 comes over to the Justice Department, at the
5 Justice Department, back and forth with the
6 agency, with the FISA Court, which has obviously
7 the judges on it, but it also has a staff of
8 permanent legal counsel who are senior attorneys,
9 you know, experienced, who go back and forth with
10 the government all the time. You know, this is
11 part of the system now.

12 So if you now interject yet another
13 person into the system you have to think about,
14 okay, what is that going to do to the speed and
15 agility of this program? I don't have a good
16 answer for you, but I think that's part of the
17 reason why it hasn't been adopted before.

18 We got pounded on all the time because we
19 were too slow, we demand too much from the
20 agencies, all kinds of complaints. So that was
21 what was happening at the Justice Department on a
22 regular basis. That's what we were hearing.

1 So if this new person then asks
2 questions, demands answers, you're going to have
3 to think about how it's going to impact the
4 ability of the process to move quickly.

5 MR. DAVIDSON: I think it would be
6 important to separate a large part of the FISA
7 Court's work which does involve individual
8 applications from, let's call it the occasional
9 task to consider a government application, and a
10 consequent order that sets in motion a larger
11 system of collection, whether it be the annual
12 order under the FISA Amendments Act or 90 day
13 orders under Title V, Section 215.

14 You know, in the circumstance of the
15 daily work, and I shouldn't say too much about
16 daily work because that was Jim's bread and butter
17 for many, many years, the system is dealing with
18 the kind of occasion that's presented when a
19 United State's attorney seeks a search order in a
20 particular matter, it's very fact-dependent,
21 moving very quickly, in contrast to the point in
22 the process in which there is intended to be

1 reflection.

2 So one aspect of the FISA Amendments Act
3 is that the government is to make its application
4 for its annual order thirty days before it seeks
5 to put that order, you know, into effect, so that
6 there is a time for process.

7 So then the question would become what
8 would be the role of the individual within the
9 system and what could be the role of people
10 outside of the system if legal issues could be
11 identified for some kind of public briefing?

12 And I think the reality is, but others
13 more involved in the civil liberties community
14 could comment, that unless they have an
15 opportunity to articulate those concerns, the
16 confidence that there's someone from the
17 government who's doing that in a closed setting
18 won't be as strong as if it might be articulated
19 by individuals or groups who take this at heart as
20 central to their purposes.

21 MR. MEDINE: And Judge Robertson did
22 suggest that judges are used to dealing with

1 search warrant requests ex parte and are quite
2 comfortable evaluating them, but it was more
3 problematic to do program approvals.

4 But other thoughts on that? Sharon.

5 MS. BRADFORD FRANKLIN: So I'd just start
6 out by saying that The Constitution Project hasn't
7 taken a specific position on this proposal, but
8 Judge Robertson is a member of our Liberty and
9 Security Committee and I would encourage you to
10 take very seriously his proposal.

11 As he pointed out, it's probably less
12 necessary when you're looking at a traditional
13 individualized FISA warrant, which is more
14 analogous to a traditional warrant in the criminal
15 context, and much more important when you're
16 looking at programmatic surveillance or an
17 argument for a new interpretation of the scope of
18 Section 702, or Section 215, or any other
19 applicable authority and building in some kind of
20 adversariness, particularly in that process I
21 think would be very important and would help.

22 MS. GOITEIN: And I think relevant to

1 that point, I think Ken said that that's what's
2 happening right now in the Section 702 context is
3 pretty much exactly analogous to the criminal
4 context.

5 And of course the major difference is
6 that in the criminal context there's an
7 individualized showing of probable cause to get a
8 warrant. There's no such thing as, judge, approve
9 this one year program in which we will get
10 criminal warrants on the following people, on the
11 following unnamed people using these, you know,
12 targeting procedures, could never happen.

13 So it is very different, the level, you
14 don't have the level of protection that the law
15 affords in a criminal context when you're talking
16 about these orders.

17 So I do think that it is more important
18 for that reason to inject some adversariality into
19 the process. I think the ombudsman idea is a good
20 idea.

21 I think the idea of making the court's
22 role less about programmatic approval and more

1 about individualized warrants goes along with what
2 I was saying before about changes to Section 702.

3 The only other thing I would add is that
4 I actually think a lot of the functions that the
5 FISA Court is performing today are functions that
6 don't have to be in a secret court. These are
7 functions that could be sort of kicked back to the
8 regular courts.

9 I mean if, you know, if the FISA Court is
10 an Article III Court, I guess, and so if there's a
11 case for controversy for the FISA Court's
12 purposes, then there's one for another Article III
13 Court's purposes as well. I don't understand why
14 some of these more significant legal questions
15 can't be brought before a regular court somehow.

16 MR. NOJEIM: Just a thought, in a regular
17 criminal case, yeah, there's a magistrate
18 considers the application of the government for a
19 search warrant, it's ex parte, but there's often a
20 check at the end. You know, you get the evidence
21 and then it's tested, that search is tested in
22 court.

1 We don't have that test in this context.
2 There's no after the search test about whether it
3 was constitutional or lawful. So to make up for
4 that, you could have the process built in up front
5 and make it adversarial.

6 I agree with Mike's point that it doesn't
7 have to be the case that the ombudsman weighs in
8 on every warrant application, every search
9 application that comes in front of the court, and
10 with Jim's point that that could slow it down
11 unnecessarily.

12 But I think you have to leave that to the
13 ombudsperson because to try to articulate, well,
14 don't weigh in unless it's a really important
15 question, you know, it might be an important
16 question that involves one search. And you need
17 to allow for that ombudsperson to decide when that
18 question is important.

19 MR. SALES: I think there's a lot of
20 value to having a devil's advocate, or ombudsman
21 or, you know, whatever the nom de guerre would be
22 for this official, especially in requests to

1 approve surveillance programs, as opposed to
2 individual discreet surveillance requests as
3 individuals.

4 I share the concerns and misgivings about
5 time being of the essence in certain cases, but I
6 think there's a way to write the statute in a way
7 that accommodates those concerns. You know, the
8 devil's advocate shall have a right to participate
9 unless the attorney general certifies that blah,
10 blah, blah.

11 FISA actually has mechanisms like that
12 already and you could import that kind of scheme
13 where the default rule is you have a devil's
14 advocate performing an adversarial check, but
15 there's an exception for truly exceptional exigent
16 circumstances.

17 MS. BRADFORD FRANKLIN: Can I just add to
18 that, I think you could have a system where if it
19 is truly an emergency, if it's certified as an
20 emergency, then the surveillance begins. And at
21 that point the ombudsman shows up, you have the
22 proceedings, and if in fact it turns out that it

1 wasn't permissible, the surveillance ends and none
2 of the information that's been gathered can be
3 used.

4 MS. COLLINS COOK: So I was hoping to
5 turn to a slightly different topic, and building
6 on some of the issues that have been raised
7 earlier about incidental collection, and I think
8 that's been raised as a concern.

9 So I was hoping, and actually just to
10 change things up a little bit, the order, if I
11 could start with you, Sharon, actually because you
12 had referenced this, and thinking about addressing
13 the issue of incidental collection, if it needs to
14 be addressed whether it should be at the
15 collection point, the access point, the use point,
16 and how we should think about it and whether there
17 are different approaches.

18 MS. BRADFORD FRANKLIN: The answer's all
19 the above.

20 On the collection point, the issue goes
21 to the justification for how this complies with
22 Fourth Amendment standards. So we've known all

1 along, long before these recent disclosures, that
2 under the FISA Amendments Act it's legal to
3 collect communications where the target is a
4 foreigner located abroad, or supposed to be
5 foreigners, maybe unknown, located abroad, and an
6 American may be on the other end of the
7 communication. And that was called incidental
8 collection.

9 The problem is that the term incidental
10 suggests de minimis, suggests it doesn't happen
11 very often, suggests it's not that broad in scope,
12 all sorts of things which really are very
13 misleading it appears, in light of recent
14 revelations.

15 We've had some members of Congress trying
16 to get a scent of that and what the real scope is
17 for a long time and haven't still gotten full
18 information on what the scope is.

19 But if it turns out that there are a lot
20 of Americans whose communications are being
21 intercepted under programmatic surveillance where
22 you're not making an individualized showing of

1 suspicion about anyone, right, because you don't
2 even have to have an individual target and show
3 suspicion about Mohamed Atta, or whoever, under
4 the programmatic surveillance, that starts to
5 undermine how you can make an argument that Fourth
6 Amendment rights are being respected for the
7 American on the other end.

8 So at the collection point we would want
9 to make sure you have a much more rigorous showing
10 to the FISA Court that you have procedures in
11 place to really make it incidental and limited to
12 the Americans on the other end.

13 Or you should turn to the earlier showing
14 where you had a showing of actual suspicion. So
15 it's more parallel to the other context where
16 you're talking to somebody who there's a criminal
17 warrant against, a Title III warrant or something
18 against them.

19 Then as far as once post-collection,
20 we've made a recommendation to try and build in
21 safeguards at that point.

22 So let's say you have this database, you

1 know that there are communications where Americans
2 are on at least one end in that database, if you
3 want to go through and search through for
4 information on a specific U.S person with
5 recognized Fourth Amendment rights, at that point
6 you should go make your showing of probable cause
7 to the FISA Court.

8 And we have some more detailed
9 recommendations that we spelled out.

10 MS. COLLINS COOK: Thank you. Did others
11 want to weigh in on this? Go, to your left.

12 MR. SALES: Briefly let me answer that
13 question in the context of the 215 program. So
14 one way to design a program to minimize the
15 privacy and civil liberties hit is to minimize
16 the government role with respect to maintaining
17 the data.

18 So an alternative way of doing the 215
19 program would be instead of the government serving
20 a 215 order on service providers and saying give
21 us your data, an alternative arrangement would be
22 a data retention requirement.

1 Congress writes a statute that says ISPs
2 shall keep whatever type of data Congress
3 specifies for a certain period of time.

4 And you know what, data storage can be
5 costly. Much less so than it used to be, but it
6 still imposes a cost so we're going to provide a
7 subsidy to Verizon to warehouse all this data for
8 a period of five, ten years, whatever Congress
9 thinks is an appropriate amount of time.

10 And that way the only circumstances in
11 which the government then gets the data are
12 circumstances in which there's a demonstration of
13 whatever the legal standard is, relevance,
14 reasonable suspicion, probable cause, whatever the
15 appropriate standard is, that the information is
16 relevant to an ongoing investigation to protect
17 against international terrorism or espionage.

18 So you know, this solves or has the
19 potential to solve the problem of misuse, right.
20 There are good reasons why the government might
21 want to have this information and there are bad
22 reasons.

1 You know, there's a pretty girl in line
2 at the airport security checkpoint, I want to find
3 out, you know, what she's all about. That
4 obviously is a misuse of authority.

5 Well, if the government doesn't have that
6 data in the first place, but rather sort of
7 outsources the responsibility for collecting and
8 maintianing it to the ISPs themselves, then that
9 sort of scenario is a lot less likely to
10 materialize.

11 MS. COLLINS COOK: Aren't there a series
12 of other scenarios that could arise, so that's
13 taking as a given that perhaps that data would
14 only be available through something akin to a FISA
15 order, but I think that you would have to expect
16 that were these repositories of information with
17 the service providers instead, that that would be
18 available through a wide range of legal
19 mechanisms, and whether there's a cost to that
20 that should also be considered.

21 MR. SALES: Absolutely. Yes, so there
22 are at least two mechanisms I can think of for

1 acquiring that data, the FISA pen trap authority
2 or the 215 authority itself.

3 Here you're using those authorities to
4 get individualized data points rather than big
5 bulk databases, right.

6 But part of the cost benefit analysis you
7 have to do is, you know, how nimble is it, how
8 nimble is the process for getting that data?

9 Maybe you need it in exigent
10 circumstances more quickly than upon application
11 to the FISA Court. So you could build in an
12 emergency procedures exception to that process
13 like we have elsewhere in FISA, I think.

14 MR. MEDINE: I wanted to get other
15 panelists' thoughts. I mean the proposal does
16 solve one problem, which is the government doesn't
17 have the data and therefore the potential to
18 misuse the data, but it also makes the private
19 sector keep data a lot longer than it might
20 otherwise have.

21 And one privacy protection is destruction
22 of information, and now if information is being

1 kept, there's also an incentive for the private
2 sector once they've got all this data sitting
3 around that they're paying to keep or being
4 subsidized to keep, they might as well use it for
5 other purposes.

6 And then there's the added complication
7 that this data may only be valuable if merged with
8 data from other companies to paint a fuller
9 picture.

10 So what's the tradeoff here in terms of
11 is it better for the government to have the bulk
12 data under a legal structure with accounting and
13 audits, or is it better for the private sector to
14 have it and only have the government access it on
15 an as-needed basis?

16 Greg.

17 MR. NOJEIM: It's better for the private
18 sector to have the data that the private sector
19 needs to engage in its business. I think that a
20 new data retention requirement imposed by the
21 government on the private sector creates more
22 problems than it solves.

1 As you said, David, if the data isn't
2 there, the bad guys can't get it, it can't be
3 breached, hackers can't get it. If the data isn't
4 there it can't be turned to other purposes.

5 You know, if the data, if there's a five
6 year data retention requirement, imagine all the
7 entities that are going to want that data. Law
8 enforcement is going to want it, and they're going
9 to want it for all kinds of investigations.

10 And as we know from our work in other
11 contexts, the standards for getting that data are
12 way too low. It'll be the first step toward other
13 data retention requirements. I mean today it's
14 the phone records, what's it going to be tomorrow,
15 IP addresses? Is it going to be content? I just
16 think it's a very dangerous line to cross.

17 I think Congress considered it and
18 ultimately decided that it was not the right thing
19 to do.

20 Again, the right data retention rule is
21 that companies should retain the data that they
22 need for business purposes and they should get rid

1 of personally identifiable data as soon as they
2 can when it does not serve a business purpose.

3 MS. GOITEIN: I just want to agree that I
4 think that's not the solution. I think that's
5 equally problematic in its own right to require
6 the telephone companies and the other companies to
7 keep this information.

8 It reminds me a little bit of the Freedom
9 of Information Act. You have a right to ask the
10 government for records it already has. You don't
11 have the right to ask the government to create
12 records for your use.

13 I think, you know, the government has a
14 right under certain circumstances to get, or
15 statutory rights anyway, to get information about
16 Americans. But to require us to generate and keep
17 information about ourselves for the government's
18 convenience, it's a form of that to say that
19 companies have to keep this information on us, and
20 it's a slippery slope.

21 MS. BRADFORD FRANKLIN: And if I could
22 just quickly push back on the notion that the

1 government should ever have access to all this
2 bulk information without the kind of showing of
3 suspicion or contact chaining that Liza was
4 talking about either.

5 Professor Steve Vladeck on a panel once,
6 I don't even remember what the context was, but
7 somebody said wouldn't it just be easier if we
8 could gather all this information. He said, yeah,
9 it would be easier if the police could go and
10 break down everybody's door and scoop up
11 everything in our houses.

12 And you know, it's an extreme example,
13 but the Fourth Amendment is there for a reason.
14 We need to require a sufficient predicate before
15 the government should be able to get this
16 information. The fact that it's easier shouldn't
17 be enough justification.

18 MS. COLLINS COOK: Jim, I think you --

19 MR. BAKER: Yeah, thank you very much.
20 Just one quick comment.

21 I'm not sure where I come out on whether
22 it's better to have the government have it or the

1 private sector and so on. So I'll just put that
2 aside for one second.

3 But if, as you're thinking about that if
4 you decide to recommend that the private sector
5 maintain the data, keep in mind, I think, I
6 haven't looked at it in a while, but there are
7 seven or eight different ways in the Federal Code
8 to get dialing data, and under a whole bunch of
9 different types of predications from probable
10 cause all the way down to relevance and so on,
11 subpoenas, and orders, and all kinds of different
12 things.

13 So if the providers have it and the word
14 gets out in the law enforcement community, which
15 obviously it will, there's lots of ways to get
16 that data that have different levels of oversight
17 connected to them, and so you want to think about
18 that as well.

19 MS. COLLINS COOK: I think we sort of
20 changed the question midstream, but I did want to
21 invite other panelists to weigh in on the question
22 of incidental collection.

1 MR. DAVIDSON: What was the very last
2 thing you said?

3 MS. COLLINS COOK: Incidental. And if
4 anyone else wanted to weigh in on that specific
5 question.

6 MR. BAKER: I was just going to say I
7 mean, I think -- go ahead.

8 Just incidental collection is dealt with
9 and deemed and thought to be consistent with the
10 Fourth Amendment because it's reasonable because
11 in part it's done, it's obtained in connection
12 with a legitimate government purpose for obtaining
13 the information, and then there are minimization
14 procedures connected with the acquisition,
15 retention and dissemination of that information.

16 And so the thinking has been for a long
17 period of time with respect to incidental
18 collection that it's okay because it's reasonable
19 for those reasons.

20 People may disagree. People may not
21 think that's sufficient and so on, but that
22 definitely has been the thinking.

1 MS. GOITEIN: I have one very specific
2 thing to say on minimization because even if you
3 go back to an individualized order requirement for
4 American's international communications, you'll
5 still have incidental collection so you'll still
6 need to have minimization procedures.

7 I do not understand the logic for a rule
8 that if you don't know where a person are, where a
9 person is, then you can reasonably assume that
10 they are a non-U.S. person who is overseas.

11 To me that is not consistent with the
12 statute where you have to have a reasonable belief
13 that the person is a non-U.S. person overseas.
14 And you know, at a minimum I think that the
15 default needs to be changed.

16 If you really have no information, no
17 knowledge, the Fourth Amendment I think requires
18 you to assume that it could be a U.S. person and
19 be more protective, not less.

20 MR. NOJEIM: I think we have to pay more
21 attention to the fact that the statute that we
22 have on the books for FAA surveillance enables the

1 government to compel U.S. companies to collect up
2 communications of people just because they are
3 abroad.

4 When you look at the limits that are in
5 the statute, a purpose of the surveillance has to
6 be to collect foreign intelligence information,
7 but the foreign intelligence information is very
8 broadly defined. And it makes sense, I think, to
9 have a broad definition of FII when you're talking
10 about surveilling agents of foreign powers, which
11 is where that comes from, the traditional FISA in
12 U.S.

13 But when it's just foreignness and
14 collecting information about people who are
15 abroad, I think we might need a more limited
16 collection regime.

17 50 U.S.C., I'm sorry, 15 U.S.C Section
18 1801(e)(1) has the description of what foreign
19 intelligence information is, and I think that
20 collecting information about a potential or actual
21 attack by a foreign power, sabotage or
22 international terrorism, clandestine intelligence

1 activities is already pretty broad and that you
2 might consider whether it is consistent with
3 concepts of international human rights and the
4 necessity that there has to be for collecting
5 information, whether you could limit the
6 collection up front about information about people
7 who are abroad.

8 We have, we, the United States, has
9 embarked on an international campaign to promote
10 Internet freedom around the world. I don't think
11 that part of that campaign ought to be that mere
12 foreignness ought to be enough to allow for
13 surveillance.

14 I don't think that our government would
15 say, for example, that the government of Germany
16 should be able to collect the communications of
17 people in the United States just because that's
18 where we are and that we're not Germans. I think
19 you have to pay some attention to that.

20 MR. DAVIDSON: Can I suggest a focus for
21 the board, and that is the Congress will turn to
22 the many important questions that have been

1 discussed through the day when it has to, and it
2 will have to initially when the sunset for
3 business records is reached in the middle of 2015.

4 I think, and this is an opinion, I think
5 unfortunately the sunsets for the FISA Amendments
6 Act and for business records have not been
7 aligned.

8 An alignment would permit looking and
9 encourage looking at this system in an integrated
10 way. These are all provisions of FISA. Something
11 may have come in through the PATRIOT Act,
12 something may have come in through the FISA
13 Amendments. They're all provisions of FISA and
14 they are intended to, or in fact work in an
15 integrated manner.

16 So at least by the middle of 2015 the
17 Congress will be turning to this. It's actually
18 not too soon to begin to think about what that
19 sunset debate should be. These sunset debates
20 just creep up on people.

21 Important to any debate, which is more
22 than a debate of should we now extend it another

1 four years and get by this temporary crisis and
2 the possible loss of authority.

3 But if it is to become an occasion to
4 think fundamentally about the collection system
5 that we have, then questions need to be identified
6 well in advance in order to determine which of
7 those should be responded to empirically and which
8 of those are philosophical matters that could be
9 discussed, you know, at any time.

10 So for example, you know, questions have
11 been raised about incidental collection. And
12 certainly I know within the Senate there are
13 senators who've articulated the importance of
14 having some process by which the intelligence
15 community helps to identify what the actual impact
16 of its collection system is.

17 Some of those involve privacy concerns.
18 So that one of the problems considered in how
19 deeply one could look at how much incidental
20 collection involving Americans comes in through a
21 system that's not focused on them, but focused on
22 others, is that the process will involve looking

1 at the communications of Americans. One might
2 invade privacy in the course of trying to learn
3 something about privacy.

4 Well, there's a balance there. And an
5 entity that is concerned about the overall issue,
6 you know, of the privacy and civil liberties of
7 Americans could begin a consideration that I think
8 would have importance within the intelligence
9 community and the Congress, which is, how do you
10 find out how a system is working? What are the
11 downsides? What are the risks? What are the
12 benefits?

13 Sometimes, you know, we have to have some
14 infringement on privacy to learn what the
15 infringement on privacy might be.

16 I'm not suggesting the answer to it, but
17 trying to identify those questions now in 2013 and
18 2014, rather than waiting to 2015 might mean
19 there's a possibility that they'll be considered
20 factually and deeply at that time.

21 MS. COLLINS COOK: Thank you. We did
22 want to give an opportunity to the other board

1 members to ask a question, if they did have one.

2 Given the time we have and the number of
3 panelists I would urge something akin to a speed
4 round. So if you could go straight to, maybe not
5 red, but yellow, and let's try to keep our
6 responses to a minute to the questions.

7 Or maybe I'm getting ahead of myself, but
8 I assume you have questions.

9 MR. DEMPSEY: My question is about 702,
10 and in part it's directed largely to what I would
11 consider to be the three civil liberties
12 representatives in the middle of the table,
13 although I know you all care deeply about civil
14 liberties.

15 On 702, I think we have to confront the
16 fact the a number of witnesses this morning talked
17 about the sort of historical perspective. To my
18 mind, what really changed around 2000, 2001,
19 etcetera, was the fact that a large percentage of
20 the communications of foreigners passed through or
21 were available in the United States on U.S.
22 territory, in the hands of U.S. based service

1 providers.

2 Previously when the government wanted to
3 get the communications of foreigners they had to
4 go overseas. And if you read the history of NSA
5 and so on, you find out about all the different
6 methods that the NSA used overseas to collect the
7 communications of foreigners with zero oversight.
8 Zero.

9 Now that comes into the United States and
10 it's available from U.S. based service providers.
11 And I do think that there is, you know,
12 credibility to the argument that 702 is a
13 tightening of rules as to what previously was the
14 practice for the government to obtain the
15 communications of persons reasonably believed to
16 be abroad.

17 And I think that even if you have a tight
18 definition of reasonably believed to be abroad and
19 a tight definition of foreign intelligence value,
20 the numbers would still exceed the capability of
21 any court of any size to do particularized
22 approvals.

1 So I mean I guess my question is, A, are
2 you prepared to accept that premise, assuming my
3 premises are correct?

4 And then if that is the premise, that
5 what used to be truly, truly bulk when you did it
6 overseas, now is subject to limitations, yes, you
7 have the incidental collection problem, but what
8 is your reaction to my statement of the premise
9 and the problem and what I see now as the impetus
10 behind 702?

11 MS. GOITEIN: I would say that it was
12 loosened in one way and tightened in another. So
13 I would say that Section 702 probably did in
14 practice tighten the standard for pure foreign to
15 foreign communications.

16 But for foreign to domestic
17 communications there had been a requirement, had
18 always been a requirement since 1978, of course
19 before then all bets were off, but there had been
20 a requirement that if an American were a party to
21 a communication --

22 MR. DEMPSEY: We had, I mean again, this

1 is ancient history now. We had huge antennas
2 aimed at huge parts of the world collecting
3 everything, including communications from abroad
4 to the United States.

5 MS. GOITEIN: That you're saying were
6 outside of FISA, that weren't covered by FISA?

7 MR. DEMPSEY: FISA had no
8 extraterritorial application.

9 MS. GOITEIN: Right. I mean I think if
10 you interpret FISA as how Congress wanted to
11 regulate the protections that it felt were
12 appropriate for the domestic, I'm sorry, not
13 domestic, the international communications of
14 Americans, then I have to say that I think the
15 government might have found a sort of
16 technological loophole in its ability to, you
17 know, go overseas and catch this information that
18 was falling from satellites, or however it was
19 getting it.

20 But it doesn't seem that it was
21 consistent with the spirit, even if it was
22 consistent with the letter of FISA, it doesn't

1 seem like it was consistent with the spirit
2 because Congress --

3 MR. DEMPSEY: FISA is explicitly orders
4 for collection inside the United States. FISA
5 left totally unregulated, everybody knew that,
6 there's no doubt that everybody knew that it left
7 unregulated what was happening outside the United
8 States.

9 MS. GOITEIN: I understand, that's why I
10 I'm drawing a distinction between the spirit and
11 the letter.

12 And also, I mean I think, the law and our
13 understanding of the law has to evolve along with
14 the technology, right?

15 MR. DEMPSEY: Well, but how do we then,
16 okay, but then technology has changed. What do we
17 do about it, assuming that now things which
18 previously were totally unregulated and truly bulk
19 now fall within some structure of regulation?

20 Again, I'm just not sure that the
21 particularized, saying it has to be
22 particularized, I honestly don't think that

1 scales.

2 MS. BRADFORD FRANKLIN: I want to address
3 that piece and just make clear that actually our
4 Liberty and Security Committee's recommendations
5 do not say end programmatic surveillance.

6 Instead the recommendations are to build
7 in greater safeguards at the front end to limit
8 the scope of the programmatic surveillance to make
9 sure that foreign intelligence is the primary
10 purpose, and to provide more information to the
11 FISA Court Judge so that he or she can really
12 evaluate the targeting and hone it in and make
13 incidental collection be more like the normal
14 traditional meaning of incidental.

15 And then post-collection to have more
16 safeguards in effect for American's rights. So we
17 have not actually recommended eliminating all
18 programmatic surveillance.

19 MR. NOJEIM: So I would accept that as a
20 premise but not the only premise. Another premise
21 is that there is more of that communication and
22 more human interaction that is now available

1 through surveillance than ever there was before.

2 And it used to be much less perfect, the
3 ability of the government to conduct the
4 surveillance. Now it is approaching a near
5 certainty level and it seems to me that something
6 has to substitute for the friction that used to be
7 in the system because there wasn't an ability to
8 collect all this information about all human
9 interaction, or close to all human interaction
10 that we have now.

11 MR. DEMPSEY: Greg, I thought you were
12 going on a different point, which I just want to
13 draw out and then yield to Judge Wald or to
14 Rachel.

15 But the world, another thing that has
16 happened in the past fifteen, twenty years is the
17 world has globalized. I think we now have the
18 largest percentage of people who are lawfully in
19 the United States, the largest percentage of U.S.
20 persons who are foreign-born since maybe the
21 1890s, right.

22 So again, when we were outside the United

1 States targeting people outside the United States
2 thirty years ago, it was sort of rare that any of
3 those would actually be talking to people inside
4 the United States.

5 I do think now with globalization there
6 might be an argument that there's a larger
7 likelihood of picking up, Jim Baker is nodding his
8 head, if I can note that, a larger likelihood of
9 picking up foreign to domestic communications.

10 MR. NOJEIM: I think that's right. And I
11 think it would be useful to have some reporting
12 about the extent to which under FAA that is
13 occurring, FAA, the FISA Amendments Act, that that
14 is occurring.

15 And the government hasn't even conceded
16 that it can make an estimate, that it couldn't
17 even take a sample of FISA Amendment Act
18 surveillance to figure this out, and I think it
19 could.

20 MS. GOITEIN: And I think to the extent
21 that what you're saying is that an individualized
22 court order requirement would be unworkable

1 because now today there are so many international
2 communications that, you know, run through fiber
3 optics and that involve Americans and people
4 overseas, I mean to me that just sort of shores up
5 my point that --

6 MR. DEMPSEY: No, honestly I was making
7 the argument that a large percentage of purely
8 foreign to foreign is also -

9 MS. COLLINS COOK: Right, right, and I'm
10 fine with treating those differently.

11 I'm just saying that to the extent that,
12 because when I talked about an individualized
13 order requirement, I was merely talking
14 communications for which an American was on one
15 end of the communication.

16 And as far as that's concerned, I mean to
17 the extent that that is such a massive part of the
18 surveillance that the government is doing that it,
19 you know, would slow things down too much to get
20 individualized orders, I mean that just reinforces
21 my point that we have a massive Fourth Amendment
22 problem here if the government is collecting that

1 much of American's content, communications,
2 whether those communications are overseas or
3 otherwise.

4 And, you know, whether or not the
5 technology has changed or not, we have to grapple
6 with that Fourth Amendment problem. I realize
7 we're the policy panel.

8 MR. BAKER: Just real quick, I don't
9 necessarily agree with some of the premises of
10 your analysis, so I just wanted to say that. I
11 don't really have the time, and this is not really
12 the place to have a full-blown discussion of that.

13 But let me just say something that I've
14 said publicly before, which is pre-FAA,
15 pre-Protect America Act, before all that, my
16 statement is that FISA worked in wartime. And I
17 think that's worth a longer discussion with you
18 all, but I'm just saying that. That was my belief
19 at the time, that's still me belief today.

20 MR. DEMPSEY: I'm sorry, I didn't hear
21 that.

22 MR. BAKER: That FISA worked during

1 wartime.

2 MR. DEMPSEY: Meaning?

3 MR. BAKER: Meaning FISA, before the FAA,
4 before the Protect America Act, FISA worked in the
5 sense that it protected the privacy interests, the
6 legitimate privacy interests of America, of
7 Americans, and also protected the national
8 security.

9 MS. WALD: Okay. This is sort of half a
10 comment, a question, move on incidental collection
11 of U.S. persons.

12 It's been somewhat, I'm reading a lot of
13 the material that that is out in the public,
14 that's perhaps one of the key points people worry
15 about.

16 And assuming for the moment we're past,
17 that somehow we get past the individualized
18 warrant and they are collecting incidental
19 information on U.S. persons, two things which have
20 been brought up in your panel and this morning's,
21 and I just want to underline it if you have any
22 reaction, and that is a second look at two parts

1 of that.

2 One is the use and dissemination. Now
3 way back in the December reauthorization, this is
4 of course on 702 I'm talking about, there was a
5 debate. Some of the senators were asking, saying,
6 well, can we get some numbers on how many U.S.
7 persons are being collected in the course of
8 this?

9 My remembrance, I hope it's correct, of
10 it was that they said, no, we can't. Okay. Which
11 led me in reading it to wonder what 702(1) in the
12 actual statute, when it tells the inspector
13 general what to do, it tells him with respect to
14 acquisitions authorized under A of that 702, you
15 should review the number of disseminated
16 intelligence reports containing a reference to a
17 U.S. person identity and the number of U.S.
18 persons' identities subsequently disseminated by
19 the element concerned in response to request for
20 identities, and then with respect to acquisitions
21 authorized, the number of targets later to be
22 determined to be in the U.S. in the extent

1 possible, whether they were reviewable.

2 Then all that goes to the attorney
3 general, the DNI, but not to the public. The
4 thought occurs to me, what great risk would there
5 be to national security in disseminating that kind
6 of information if it's already being collected by
7 the inspector general?

8 Because like one of the panel members, I
9 wondered as we went through many, not just these,
10 but many of the broader contexts of many of the
11 acts and found out that when people talk about
12 minimization, as it was brought up in the morning,
13 it can mean many things.

14 In some contexts it means, for instance,
15 if they collected it by mistake when they
16 shouldn't have, it goes out apparently. It's
17 deleted. Well, it's taken to some cloud that's
18 not as accessible as other clouds or whatever.

19 However, if it's incidentally collected
20 it's kept in there. It may be tagged and there
21 may be some attempt to protect the specific
22 identity, but it's kept there and it's used and

1 it's available for, and it can be disseminated, as
2 I understand it, you know, for not just the law
3 enforcement but to, which I've always wondered
4 what it really means, if it's necessary to make
5 foreign intelligence understandable, whatever that
6 means.

7 And so it seems to me that that's an area
8 which I think, or at least initially deserves
9 more, because my guess is we are going to end up
10 collecting, however it goes, your premise or not,
11 a lot of incidental information.

12 And I think that could help, I think, to
13 heighten the trust perhaps if Americans get a
14 better specific notion of both the dimensions and
15 the actual usages. Because I think it's an area
16 of total confusion, at least it's still that for
17 me.

18 That's more of a comment than a question,
19 so I'll go on to Richard.

20 MR. SALES: If I could, just a very quick
21 reaction to that. You may as well put me on red
22 because I'll be very quick.

1 There actually is some precedent for the
2 disclosure of very high level aggregate data about
3 national security operations. So the intelligence
4 budget, the overall sum previously was classified
5 and now has been declassified.

6 In the criminal law context, every year
7 we have a wiretap report that reveals how many
8 Title III wiretaps were issued. So I think it's
9 certainly possible to have that kind of
10 information.

11 MS. WALD: But am I not right that in
12 Title III, it's been a long time since I've been
13 in the criminal area, but in Title III
14 minimization means if you collect information in a
15 telephone call, you know, about his wife having
16 problems, that kind of thing, it gets thrown out?
17 That doesn't happen in many, many of these
18 programs.

19 MR. SALES: I think that's right.
20 Minimization looks different in the Title III
21 programs.

22 MS. WALD: Yeah, it stays. It stays in

1 those data banks. It may be restricted, you know,
2 tagged, but it stays there accessible for
3 whatever.

4 Rachel, I think was the one --

5 MS. BRAND: It's more of a comment. So
6 we, the PCLOB, have to look at all aspects of this
7 issue and our statute specifically mentions the
8 fact that there's nothing that's more harmful to
9 security or to civil liberties than insecurity.

10 So you know, we can't discuss privacy and
11 civil liberties impact in a vacuum. And the
12 discussion here has been a little sterile in that
13 regard. You almost wouldn't know we were talking
14 about terrorism because we haven't been talking
15 about it very much, frankly.

16 So you know, we don't have time to do it
17 now, and I'm, you know, we don't really have time
18 for more questions, but to the extent that you are
19 weighing in with us, providing us advice, it would
20 be useful to know if the broad kind of collection
21 reflected in the alleged 215 order is going to
22 occur, what restrictions or limitations would be

1 useful?

2 So destruction dates, limits on access,
3 you know, targeting guidelines and those sorts of
4 things.

5 You know, just talking about the two
6 sides of the coin here, the government's talked a
7 lot about the benefits of these programs in terms
8 of thwarting plots, and we haven't yet had a
9 chance to fully get into the extent to which
10 that's credible. You know, we'll be getting more
11 information about that from the government as we
12 go along with our analysis.

13 But if it turns out that these programs
14 are unbelievably useful and have thwarted more
15 plots than you can possibly imagine, and that sort
16 of the national security imperative means that we
17 have to keep them, then what?

18 I'm not saying that that's the
19 conclusion. I'm just, it would be useful for us
20 to know what your recommendations would be for
21 cabining the privacy damage that that would cause,
22 so to speak. So that would be useful to us going

1 forward, or to me at least going forward.

2 MR. DAVIDSON: If I could say a word in
3 relation to that. I'm not sure that the test is
4 always or necessarily most importantly whether
5 some particular plot was foiled by the use of a
6 particular authority.

7 I do believe there's a way of looking at
8 metadata collection if everyone would permit, even
9 in terms of privacy and civil liberties. The more
10 that is known about who should be looked at more
11 closely, to narrow down the use of other more
12 intrusive authorities because there's a means of
13 identifying those particular individuals who merit
14 that closer look, that may very well work to
15 reduce the intrusiveness of more robust forms of
16 content collection.

17 And so you wouldn't get out of that
18 benefit that a particular plot was foiled. You
19 may get out of that benefit you didn't have to go
20 out and collect content because you had a way of
21 being reasonably certain that that individual was
22 not in communication with others of concern.

1 So there may be several questions to ask
2 about the benefit of metadata collection.

3 MR. MEDINE: Okay. With that, that's a
4 good endpoint for our discussions, so thank you
5 very much for the panel.

6 We will take a ten break and then welcome
7 any members of the audience who's like to make
8 brief comments on these subjects to come up to a
9 microphone and make those comments. So we'll be
10 back in about ten minutes. Thank you.

11 (Off the record)

12 MR. MEDINE: Okay. Thank you. We're
13 going to resume our final session, which is the
14 opportunity for members of the public to make
15 comments. Just in the interests of time, we're
16 going to limit comments to two minutes. And
17 Diane, who has been our timekeeper will enforce
18 that.

19 So one other thing is that the session is
20 being transcribed and so those who choose to come
21 up and make a public comment have an option to
22 preserve their privacy and be anonymous and don't

1 identify themselves.

2 But if you would like to be identified
3 for the record, we would appreciate it, it's in
4 your interest to identify yourselves. So it's
5 really up to the speakers whether you want to be
6 anonymous or not.

7 AUDIENCE MEMBER: David, thanks. Evan
8 Hendricks, Privacy Times. Thanks for the day,
9 thanks for devoting attention to this.

10 I think when you talk about the
11 collection of phone records of millions of
12 Americans that are not suspected of any
13 wrongdoing, it's an affront to the Fourth
14 Amendment, which means we're supposed to be secure
15 in our papers and effects. And the intention
16 there is our personal information.

17 So I think, to me, the credibility of the
18 board is going to depend on how strongly and how
19 effectively will you advocate against the phone
20 metadata collection program. I think there's no
21 justification for it under the Fourth Amendment.

22 And I think one of the defects in the

1 process is you are finally the only entity to
2 address privacy within this administration's
3 tenure.

4 There's been no privacy counselor to
5 address these issues along the way. There's been
6 no privacy advocate in front of the FISA Court.
7 There's been no privacy advocate or anyone to
8 stand up for the American people in front of the
9 intelligence committees. It's totally been
10 missing in action, and I think that's a huge
11 defect.

12 And on the issue of minimization, I
13 think, I hope you're familiar with William Denny's
14 Thin Thread Program, which he developed back in
15 the early 2000s, which is a way of collecting the
16 information they need and dropping the information
17 on Americans that were not legal to collect at
18 that time.

19 That program, which costs about three
20 million dollars, and it was rejected, and instead
21 they've wasted billions and billions of dollars on
22 dragnet programs that haven't worked.

1 So I think you should also look at which
2 tail is wagging the dog, and that's again, the
3 beneficiaries of all this dragnet surveillance
4 have been military contractors like SAIC and Booz
5 Allen Hamilton that have made billions of dollars
6 and have developed programs that weren't as good
7 as ones that were developed in-house. Thank you.

8 MR. MEDINE: Thank you for your comment.
9 Next.

10 AUDIENCE MEMBER: Hi, my name is Adam
11 Marshall. We were talking a lot about metadata
12 today, and the various privacy implications
13 associated with it. I just thought I'd bring
14 something to the attention of the board that might
15 help you crystallize kind of what metadata can do.

16 So MIT has put out a very interesting
17 tool called Immersion. You can find it just by
18 Googling it. And it basically has you log into
19 your Gmail address and then it scans the metadata
20 of your Gmail account, so only the two from fields
21 and the time. And then you can kind of explore
22 your relationships that your metadata says about

1 you.

2 And after you're done kind of poking
3 around for a while and freaking yourself out, you
4 are then given the option to either delete your
5 metadata from the MIT server or to let it remain
6 of the server. It's, you know, secure and
7 encrypted and such.

8 So I would encourage the members of the
9 board, if you have a Gmail account just to try
10 this out to see what it says about you, and then
11 see whether you feel like deleting it or not. And
12 if you do feel like deleting it, just ask what
13 that says.

14 MR. DEMPSEY: What's the name of the
15 program again?

16 AUDIENCE MEMBER: It's called Immersion.

17 MS. BRAND: With an I?

18 AUDIENCE MEMBER: With an I, yes. It's
19 done by MIT.

20 MR. MEDINE: Thank you for your comment.

21 Is there anyone else who would like to
22 make a comment? Any board members like to make

1 any comments?

2 All right. I wanted to thank everyone
3 for coming today. I wanted to thank the panelists
4 for engaging in some excellent discussion. I
5 wanted to thank the board staff, Sue Reingold and
6 Diane Janosek for helping make this event flow as
7 smoothly as it did.

8 These are tough issues. There are strong
9 interests on both the national security and
10 privacy and civil liberties side and we appreciate
11 the chance to have discussions about them.

12 It does just occur to me in a broader
13 sense, maybe not to lose sight of the fact it's
14 something we take for granted, we have a federal
15 agency here who's hosting a public discussion
16 giving people a chance to critique their
17 government surveillance programs.

18 I think that in a way is a testament to
19 what a great country we have, that we can have
20 this kind of discussion and how important it is to
21 maintain these kinds of values to have an open and
22 free discussion about them.

1 And going forward, the board will take
2 into account what we've learned today, continue to
3 look into these matters and eventually prepare a
4 report for the President and Congress in a public
5 forum on these two programs.

6 With that, thank you very much for
7 coming.

8 (Whereupon, at 4:14 p.m., the meeting was
9 adjourned.)

10

11

12

13

14

15

16

17

18

19

20

21

22

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

CERTIFICATION

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

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

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

Lynne Livingston

Notary Public

My Commission Expires December 10th, 2014

A	17:17,21 71:10	accumulation	221:14 228:13	addition 19:18
aa 143:4	72:17 74:16,20	27:17	232:13 233:9	21:15,19 42:11
ability 9:7 75:15	88:15 96:8	accuracy 7:20	236:13 259:19	106:17 215:19
149:17 154:1	97:18 112:15	170:17 197:5	260:7 268:12	226:1 238:8
180:19 191:11	114:19 140:3	198:19	269:2 276:2	244:6
213:18 268:4	153:4,16,17	accurate 84:4	284:9 291:6,11	additional 6:17
297:16 300:3,7	159:11 160:1	162:4,4 189:10	301:13,17	121:2 137:21
319:8	164:9 166:22	191:11 197:3	303:15 304:4	172:2 223:14
able 23:15 66:5	173:6 174:11	199:12,16	action 43:8 94:1	265:4
77:3,5 105:6	175:15 180:13	251:14 266:12	314:10 319:11	address 20:7
119:6 130:5	205:8 206:13	319:7	actions 4:13,15	28:13 43:22
144:1 159:1	246:13,19	accurately	active 7:5	50:18 104:8
166:6 172:10	275:15 282:14	185:8 251:15	154:20	132:15 151:11
185:7 189:8,9	285:1 310:2	accused 230:21	activities 13:10	153:15 164:18
209:2 227:9	accessed 10:10	accustomed	18:9 29:3	164:20 165:1
248:22 285:15	18:3 19:12	101:7	67:10 105:9	167:17 170:20
290:16	70:13	acknowledge	119:16 141:17	173:10,12,14
abnormal	accessible	222:17	141:19 214:6	178:15 181:16
130:11	306:18 309:2	aclu 2:13 16:5	216:21 290:1	205:21 218:8,9
abroad 41:21	accessing 8:10	37:7	activity 64:16	299:2 314:2,5
236:21 237:1	22:14 77:20	acquire 12:11	134:9 136:6,10	315:19
276:4,5 289:3	206:1,15,21	acquired 17:10	166:6 168:1,16	addressed 43:2
289:15 290:7	accidents	22:12 114:18	182:12 192:3,4	50:21 75:18
295:16,18	181:15	233:16	208:12 263:12	152:9 153:9
297:3	accommodated	acquires 246:10	actors 177:16	221:11 275:14
absence 263:1	35:4	acquiring 281:1	201:19	addresses 145:4
absolutely	accommodates	acquisition 20:9	acts 32:2 187:21	145:10,10
159:21 162:2	274:7	120:10 232:21	306:11	161:17,17
175:8,18 179:5	accomplish 39:8	287:14	actual 77:12	164:7,17 178:1
186:17 198:10	account 30:10	acquisitions	151:13 179:9	178:1 243:11
280:21	30:20 261:4	305:14,20	187:8 229:6	283:15
abundantly	315:20 316:9	act 1:7,8 5:12,13	243:20 255:18	addressing 83:5
52:12	318:2	8:17 9:1 12:2	277:14 289:20	250:14 254:21
abuse 129:20	accountability	28:17 34:11	292:15 305:12	275:12
159:19 160:8	180:3 181:12	36:5 37:19	307:15	adequate 140:13
abuses 46:12	194:7,15 195:4	38:3,13,18	adam 315:10	204:6 224:18
54:10 94:2	195:19 196:3	40:15 52:8	adaptations	225:11 261:4
231:14 234:4	208:9	60:16 64:11	78:22	adequately
247:4	accountable	100:3,11	adapts 78:18,19	236:2 240:5
accept 196:22	99:3 135:1	133:15 134:15	add 63:17 119:1	adhere 125:9
296:2 299:19	155:11 171:12	135:13,18	126:3 160:15	adhered 152:22
acceptable 53:5	207:21	139:18 171:2	272:3 274:17	154:12
access 10:9	accounting	187:19 188:15	added 239:21	adherence 200:4
	282:12	197:1 219:17	282:6	adjourned

318:9	37:7,9	195:18 196:10	akin 280:14	211:16
adjudicating	adverse 91:15	198:12 201:14	294:3	alqaeda 146:14
35:7,9	189:6	267:3,6 317:15	alarm 33:7	alternative
adjudication	advice 309:19	agent 104:22	alarmist 32:15	69:22 278:18
35:11 62:9	advisor 2:18	129:6 228:19	alert 205:22	278:21
administration	16:15 125:6	228:21 231:22	alexander	alternatively
31:19 102:9	139:15	239:9,12	134:12 160:22	127:1
103:5,10,21	advisory 4:21	agents 33:15	algorithms	alternatives
225:5,6 226:7	4:22	38:22 289:10	179:17 192:9	67:1 76:21
administrations	advocate 265:18	aggregate 308:2	242:4	77:15,19
314:2	273:20 274:8	aggressively	alien 12:15	amass 188:10
administrative	274:14 313:19	225:7	aligned 291:7	amend 184:22
5:7 21:12 36:9	314:6,7	agility 267:15	alignment 291:8	228:13 258:22
56:14 82:15	advocates 85:20	ago 48:2 90:7	allegations	amendment
134:14	265:14	100:5 104:14	100:17	18:10 21:5,10
administrator	affect 23:8	137:1 140:5	alleged 59:3	21:19 24:5,14
131:20 132:3,6	256:16	154:6 167:20	67:5,20 89:15	25:1 27:10,13
administrators	affidavit 92:22	185:4 301:2	309:21	34:10 41:17
131:21	affiliation 146:3	agree 58:1,14	allen 315:5	43:15 66:15
adopted 52:7,7	affiliations	73:19 94:15	alleviate 192:21	75:10,13,19,20
57:22 266:8	25:15	113:13 117:4	allies 150:21	75:22 76:12
267:17	afforded 43:4	140:18 158:17	allocate 187:22	78:3,3,4,11
adopting 56:11	affords 271:15	185:18 187:2	allow 62:12	92:16 98:1
adoption 24:5	affront 313:13	191:2 198:16	78:14 81:1	99:21 107:22
advance 190:3	afternoon	208:7 258:7,21	84:13 96:6	108:3 109:21
292:6	123:15,22	258:22 273:6	98:9 102:20	110:1 111:4
advanced	124:1,4	284:3 303:9	112:1,6,14	112:17 113:5,8
162:11	age 24:8	agreed 5:17	157:11 208:2,2	113:10,14
advancement	agencies 13:22	54:13 86:12	208:4 211:8	130:17 168:12
159:16	21:10 56:15	agreeing 5:3	273:17 290:12	168:13 220:9
advances 190:22	134:14 156:13	185:19	allowed 50:13	220:12 223:7
adversarial 62:9	157:17 166:7	agreement	59:18 76:5,8	227:20 235:6
97:19 99:5	171:11 180:20	78:14,15	128:6 156:13	275:22 277:6
120:17 201:8	181:3 195:5	212:20,20	188:19 220:17	278:5 285:13
265:10 266:4	202:10 204:12	213:4,7	allowing 25:16	287:10 288:17
273:5 274:14	231:7,8,15,18	agrees 60:1	232:20	301:17 302:21
adversariality	232:12 267:20	ahead 117:17,18	allows 9:1 25:8	303:6 313:14
259:17 271:18	agency 4:9 36:9	194:17 287:7	42:3 53:8	313:21
adversarialness	134:13,16,21	294:7	167:13 264:16	amendments
119:17	135:7,14	aimed 297:2	alluded 46:5	5:13 36:5
adversaries 35:1	158:21 171:1	airline 57:12	71:16 97:9	37:19 38:3,13
adversariness	177:13,14,18	airlines 243:6	alphabetical	38:18 40:15
270:20	177:20 180:7	airport 135:4	15:21	52:8 60:16
adversary 36:16	182:12 186:21	280:2	alphabetically	76:4 100:3,11

232:13 233:9	292:20 293:1,7	126:13 131:8	256:14	306:16
236:13 268:12	297:14 299:16	134:5 136:22	anonymization	appeal 30:7
269:2 276:2	302:3 303:1	159:1 172:11	139:8	88:11 221:14
291:5,13	304:7 307:13	178:20 185:11	anonymous	appeals 88:10
301:13	313:12 314:17	186:5 188:16	145:8 312:22	appear 157:11
america 221:14	amicus 88:4	197:12 203:18	313:6	163:15 164:7
259:19 303:15	90:19 95:13,14	209:1 216:11	answer 55:2	223:19 265:14
304:4,6	95:21 97:1	242:16,22	90:15,22	appearing
american 23:22	98:10 104:8	249:6 252:1,2	101:18 111:12	100:19
34:1 43:20	221:9	254:4 263:16	112:21 128:10	appears 18:8
50:6 53:18	amnesty 37:1,7	281:6 303:10	128:12,16,16	38:14 89:16
60:6,9 80:7	47:7 49:2	310:12	129:9 131:12	219:9 222:20
103:13 107:5	100:9 111:2	analyst 129:6	134:8 166:15	237:20 265:21
114:1 117:7	amount 22:11	204:7 208:14	196:5 199:2,4	266:1 276:13
135:16 145:11	27:8 46:19	analysts 19:10	204:7,18 215:9	appended
150:21 165:22	128:14 133:22	203:22,22	224:1 236:16	165:17
187:16 199:16	144:21 155:3	analytic 137:8	257:9,10	applicability
229:12 237:7	176:12 179:11	150:8 180:2	267:16 278:12	76:18 113:15
249:8 259:21	180:12 185:21	181:4	293:16	applicable
262:9 265:11	207:1 226:2	analytical 242:4	answered 52:9	270:19
276:6 277:7	229:10 233:14	analytics 77:4	75:6 236:14	application 90:9
296:20 302:14	279:9	analyze 4:13	answering	92:22 93:6
314:8	amounts 31:17	158:7 159:1	79:19 169:16	104:11,15
americans 22:18	44:18 157:12	172:11 186:6	169:17	268:9 269:3
23:9 27:18	157:18 189:21	186:14 190:18	answers 92:5	272:18 273:8,9
29:22 34:3	191:10	213:19	127:19 188:13	281:10 297:8
47:11 48:16,19	analog 137:4	analyzed 186:11	268:2 275:18	applications
49:19 50:20,20	186:3,4,6	247:15	antennas 297:1	35:15 39:19
60:11 61:7	199:13	analyzing 93:9	anticipate	87:15 91:16
74:18 76:5,9	analogous 93:3	anathema 34:3	186:22	93:14 138:1,10
98:2,9 111:18	270:14 271:3	ancient 297:1	antiunilateral...	138:16,18
112:15 113:1	analogue 163:5	animal 94:14	244:20	176:18 268:8
113:19 114:20	analogy 61:21	annual 40:22	anybody 34:16	applied 45:17
144:22 145:8	62:1,20 65:20	176:5 219:18	44:14 84:22	64:5,15,19
145:12 160:7	96:3	220:13 222:21	92:11 155:21	217:19
231:2,8,12,19	analyses 130:4	223:7 268:11	174:6 216:16	applies 50:16
232:7,12 233:4	analysis 10:16	269:4	anymore 251:17	59:16 67:13
233:15 234:3	10:18 11:16	anomalies	anyones 17:20	113:14
236:20 256:10	18:18,22 20:14	180:19	anyway 284:15	apply 39:7
259:10 261:7,8	20:15 27:15	anomalous	apart 99:13,16	59:15 63:21
261:9,18,19	40:13 51:6	208:12	apologize 80:18	75:14 110:1
266:14 276:20	66:2 68:8,10	anomaly 64:20	apparent 250:7	113:6,9 116:16
277:12 278:1	70:21 89:13	206:13 209:9	apparently	116:16 134:20
284:16 288:4	93:15 113:11	anonimized	120:9 239:17	154:10 217:5

applying 59:13 255:14	222:22 246:19 271:22	34:21 59:5 78:5 86:13,15	139:18 149:11 199:8 218:9	associates 242:14
appointed 33:11	approvals 94:17	101:8 111:12	253:19	associations
appoints 99:15	193:17 270:3	113:21 178:19	asking 72:14	25:11 27:22
appreciate	295:22	184:12,14,15	99:8 112:20	49:21
16:21 43:22	approve 36:6	188:6,9 270:17	129:3 169:8	assume 60:12
118:19 211:20	271:8 274:1	277:5 295:12	211:11 240:20	73:11 151:18
223:17 230:8	approved 11:10	301:6 302:7	305:5	158:14 161:3
313:3 317:10	13:19 17:8	arguments	asks 268:1	169:10 190:20
approach 55:16	33:19,21 39:1	100:9 103:12	asneeded 282:15	288:9,18 294:8
79:9 80:11	40:19 58:16,21	ark 262:1	aspect 269:2	assumes 72:15
149:4 173:9	59:17 90:9	arrangement	aspects 6:14	assuming 44:15
180:10	92:18 93:7	57:2 278:21	66:17 220:7	122:1 200:14
approached	176:20,20,21	article 25:18	309:6	296:2 298:17
218:22	176:22 201:3	46:15 92:4	aspired 27:21	304:16
approaches	245:17	100:14 101:4,6	assemble 20:19	assumption
163:11 275:17	approves 34:11	102:17 105:19	asserted 10:6	60:15 98:12,13
approaching	36:10	130:4 272:10	asserting 55:10	171:21 207:19
300:4	approving 10:1	272:12	assertion 47:10	assure 34:1
appropriate	35:16 94:9	articles 125:1	48:22	assumptions
79:4 80:12	179:6 182:3	articulable	asserts 14:7	190:16
99:14 102:5	220:12,12	122:16 228:18	assess 14:4	atta 242:17
118:14 154:4	245:4	239:10	137:9	264:13,13
175:2 177:3	apps 146:11	articulate 98:6	assessed 247:14	277:3
187:13 201:15	apt 62:20	260:5 269:15	assessing 104:15	attach 55:9,11
224:9,18	architectural	273:13	137:7 161:6	attaching 55:16
225:11 255:21	244:11	articulated	224:7,17	attack 74:13
260:13 264:6	area 68:7	269:18 292:13	assessment	289:21
264:19 265:6	161:20 217:5	artificial 3:10	137:12 169:9	attacks 40:4
265:22 279:9	266:17 307:7	125:4	204:1 224:13	57:11 234:21
279:15 297:12	307:15 308:13	ashcroft 85:4	235:4	attempt 138:6
appropriately	arent 23:12 48:9	230:22	assessments	203:8 306:21
4:17 22:17	48:16 101:16	ashkan 3:7	232:14	attempted
211:14	175:2 186:21	124:20 140:15	assign 187:17,21	168:22
appropriaten...	257:11 261:12	148:10 149:14	assigning	attempting
38:7 101:2	280:11	163:9,10 164:2	117:21	110:7
approval 12:8	arguably 128:18	177:9 180:1	assignment	attempts 188:17
13:6,14 18:11	argue 265:18	201:16 208:12	121:14	attended 243:3
19:18 21:12,18	argued 9:4	aside 230:14	assistance	attention 51:4
22:8 35:4,11	26:16 86:11	286:2	201:22	149:22 209:4,5
35:13 39:9	argues 64:22	asked 33:11	associated 10:21	209:8 237:11
40:1 42:6 46:8	arguing 156:7	43:20 51:13	18:6 24:3	288:21 290:19
46:10,15 57:12	183:3	85:6,8,13	151:9 183:15	313:9 315:14
94:10 109:19	argument 27:6	135:10 139:16	315:13	attitude 127:11

attorney 12:10 16:17 40:21 85:4 112:7,12 268:19 274:9 306:2	42:14 46:9 76:8 85:7 94:3 100:6 109:3 133:11 134:2 136:5 142:10 156:12 196:9 205:9 228:15 240:14 255:22 270:19 280:4 281:1,2 292:2 311:6	254:13 280:14 280:18 294:21 295:10 299:22 307:1	55:19	249:19 252:8 294:22 295:10
attorneys 112:9 267:8		avenue 1:16	backs 142:22	basic 76:18 140:9 220:17 221:1 244:8 246:7
attributable 163:20		avoid 6:9	189:15 193:13 193:14,20 202:16 228:4 242:1 264:16 264:17 279:21 283:2	basically 114:17 136:16 158:19 164:11 172:8 201:13 250:17 315:18
attributed 208:20		aware 92:1 187:15	bailiwick 36:12	basis 81:6 84:15 133:17,20 135:7 156:14 176:6 183:16 213:15 219:15 250:11 267:22 282:15
audience 7:1 123:7 312:7 313:7 315:10 316:16,18	authorization 64:7 109:12 110:22 118:8 220:17 245:1,2 245:12 252:19	awareness 27:22 168:7	baker 3:14 210:8 211:18 217:17 247:22 248:5 250:17 251:13 266:6 285:19 287:6 301:7 303:8,22 304:3	
audit 174:1,13 174:21 175:3 177:18 178:7 178:13 196:8 200:1 205:6,10 206:20 207:7 208:1	authorizations 118:13 219:21 220:13	awful 262:10	balance 32:2 39:3 173:2 211:14 230:16 266:11 293:4	bbc 164:9 bear 219:7 beef 88:2 began 56:5 beginning 31:11 51:18 begins 274:20 behalf 211:22 223:21 belief 157:17 207:6 288:12 303:18,19 319:8 beliefs 28:1 believe 79:15 107:11 110:14 122:17 134:3 144:15 158:9 211:13 222:5,6 224:2 225:8 228:5,8 230:17 237:1 239:11 311:7 believed 13:12 41:22 42:9 45:12 109:8
auditing 131:16 180:10 199:4 203:3 256:2	authorize 81:5 220:2 228:9	back 18:17 33:20 41:19 61:15 64:8 72:7 73:10 79:10 80:12,18 85:5 87:3 90:13 93:7 102:22 108:5 114:21 118:21 130:2 133:6 138:22 147:7 159:7 164:3 169:3,22 172:21 179:5 181:13 193:19 194:3 195:8,21 197:4,5 198:13 212:14 213:6 234:9 241:1 247:5 248:5,17 249:2,12 250:6 259:18 263:2 267:5,9 272:7 284:22 288:3 305:3 312:10 314:14	balanced 4:15 balances 29:18 30:2 121:2 258:1 baltimore 319:4 bank 68:2 banks 309:1 banner 212:15 barely 182:2,2 barrier 169:1 base 130:5 238:2 baseball 161:19 based 5:21 7:13 8:16 11:18 12:9 18:9 19:2 81:20 96:16 126:6 133:14 150:12 157:22 161:1,5 166:18 185:9,10 192:2 192:18 211:11	
audits 19:21 180:11 203:9 209:7 246:20 282:13	authorized 8:11 8:22 20:10 21:13 53:3,6 110:18 122:11 176:6 226:14 237:18 305:14 305:21	background 46:5 93:20 166:16 186:16 248:11		
audittype 158:19	authorizes 53:10 55:5 81:9 238:10 245:16	backgrounds		
august 7:10 125:17,21	authorizing 31:14 196:9			
authenticate 167:11 174:8	automatic 128:10			
author 28:16	availability 182:10			
authorities 29:15 73:20 86:20 256:17 258:16 281:3 311:12	available 22:2 42:21 74:20 77:17 96:19 153:14 176:11 176:13 185:13 211:12 225:19			
authority 21:10 21:16 37:19 38:3 42:8,13				

110:3 161:7 169:5,12 295:15,18 bell 124:11 bellovin 3:3 124:9 126:2 160:17 161:13 162:2,9 163:11 173:16 181:19 189:11 199:3 208:19 ben 51:8 beneficiaries 315:3 benefit 15:14 80:19 89:13 230:19 235:11 263:16 281:6 311:18,19 312:2 benefits 242:8 242:12 293:12 310:7 bernstein 51:10 best 8:9 32:8 50:5 130:2 161:10 170:11 173:16 197:20 201:8 209:10 265:11 319:8 beth 4:6 117:14 199:1 204:15 204:20 209:19 beths 119:1 121:14 bets 296:19 better 68:9 171:4 181:12 182:13 184:7 197:4,11 227:4 282:11,13,17 285:22 307:14 beyond 8:10 24:12 54:17	224:16 bible 60:21 big 91:19 94:5 129:16,17 142:14 167:6 183:16 241:2 250:7 264:11 281:4 biggest 127:7 132:1 bill 28:20 billing 17:12 22:3 69:17 71:18 83:15 billion 200:13 billions 61:6 314:21,21 315:5 bipartisan 4:9 227:1 bit 54:14,15 66:1,6 108:5 115:12 120:19 121:4 123:1 142:18 144:17 148:4,22 152:21 186:15 187:10 189:12 194:20 211:6 212:11 217:15 261:14 275:10 284:8 bite 78:10 blacked 249:10 249:10 blackout 161:20 162:22 163:1 blah 198:4,4,4,5 274:9,10,10 bleeding 246:4 blending 180:22 blew 200:10 block 20:16 blocked 104:2	blocks 170:20 blog 141:8 blower 200:9 board 1:3 2:1 4:4,5 5:5 6:16 6:17 14:18 15:1,20 27:19 28:12 32:20 37:15 44:2 72:14 106:14 114:15 115:7 132:7,21 133:9 211:20 212:19 220:19 222:6 224:19 240:20 256:5 290:21 293:22 313:18 315:14 316:9 316:22 317:5 318:1 boards 4:12 5:7 28:5 172:22 bob 93:10 150:4 152:3,4 bodily 14:6 264:2 body 90:13,13 102:3,6 135:4 252:3,4 bombing 57:9 book 257:13 bookmaking 182:20 books 288:22 booz 315:4 border 232:15 254:7 borderless 164:7 166:10 borders 141:14 142:5 boston 57:9,14 58:9 bottom 120:2	bound 103:15 boundaries 149:17 162:17 boundary 138:9 156:21 bounds 43:14 150:2 151:17 bradbury 2:11 15:22 16:20 40:10 44:9 46:21 48:12 56:4 58:6 68:17,20 69:2 71:4 82:7 92:13 96:7 98:11 108:4 111:20 113:3 259:5 bradford 3:17 210:15 223:18 254:18 270:5 274:17 275:18 284:21 299:2 bradlee 51:9 bradley 207:14 208:20,20 brainer 159:3 branch 4:10,13 19:20 30:9,20 43:13 48:6 54:8 94:2 96:18 97:4 218:14,18 222:7 233:7 244:21 247:3 255:14 258:12 branches 43:16 46:13 94:6 214:5 215:10 257:1 brand 2:4 4:6 14:19,20,22 22:19 28:7 32:16 37:13,21	54:11 59:1 62:18 72:8 80:17 97:7 107:9 117:13 117:18 123:3 202:14 204:15 309:5 316:17 breach 141:2 breached 283:3 bread 158:22 268:16 break 6:16 39:17 65:20 123:12 174:10 174:11 209:15 285:10 312:6 breaking 30:18 breaks 145:2 breakthrough 219:5 brennan 3:18 210:19 bridging 124:7 brief 6:20 34:20 98:10 111:6 117:19 126:3 133:7 136:2 223:22 226:16 312:8 briefed 20:4 42:19 94:13 95:10,12 briefing 20:6 42:20 269:11 briefly 153:13 200:18 215:20 215:22 246:16 278:12 briefs 221:10 bright 171:15 bring 94:6 134:4 209:12 221:21 315:13 bringing 41:18
--	---	---	--	---

104:2 184:5 brings 35:12 91:15 britney 146:15 broad 9:5 21:15 56:16,20 57:6 57:20 58:3 59:5 119:5 157:16 237:16 276:11 289:9 290:1 309:20 broader 56:1,2 56:12 58:20 64:16 97:22 110:20,21 149:20 254:14 306:10 317:12 broadest 20:18 broadly 45:17 217:18 289:8 brought 66:18 67:2 92:2 272:15 304:20 306:12 brouhaha 51:14 browser 165:6 browsing 192:3 bs 179:18 budget 308:4 build 80:15 127:15 129:4 169:1 179:2 244:16 277:20 281:11 299:6 building 20:16 177:18,18,19 243:13 244:11 247:10 270:19 275:5 built 126:20 250:2 273:4 bulk 118:13 228:9 236:18 241:6 242:3	245:4,16 258:5 258:18 265:1 281:5 282:11 285:2 296:5 298:18 bunch 286:8 burden 39:13 203:20 234:14 burdens 204:9 bush 103:5,10 bushs 60:18 business 8:18 9:2,15 17:3 20:9 21:8 51:3 69:7,14,16 71:11,13,14 72:1,2,3 81:3 81:11,12 82:1 82:21 83:11 118:18 128:17 143:3 163:13 219:8 264:7 282:19 283:22 284:2 291:3,6 butter 158:22 268:16 C c 1:17 16:1 66:9 99:15 132:16 135:6 238:15 289:17,17 cabining 310:21 cables 108:13 cadwalader 16:14 calculus 168:9 calibrated 43:1 california 163:1 call 9:11,12,13 22:3 23:18 25:13 34:4 53:12 71:18 88:4 129:11	133:17 136:21 143:4,14,14 169:7 179:18 183:17,18,20 183:20,21 190:5 223:4,6 241:5 268:8 308:15 called 17:13 18:14,15 30:10 150:4 161:15 167:21 184:2 185:5 189:19 241:5 242:15 276:7 315:17 316:16 calling 83:5,9 189:18 192:15 192:16 262:6,6 calls 9:10 10:14 17:15,18,20 18:15 26:22 27:1 36:21 53:1 60:11 83:10 105:3 189:2 190:4 192:19 240:10 campaign 290:9 290:11 cancer 183:17 184:1,3,5,18 184:19 cant 78:14 120:22 121:1 174:7 208:3 238:22 272:15 283:2,2,3,4 305:10 309:10 capabilities 29:9 31:2 142:12,14 142:15 147:17 180:2 190:17 capability 295:20	capable 147:19 177:16 capacity 23:6 203:2 capitol 52:5 125:22 capture 144:1 captured 256:11 car 45:3 card 157:2 207:4 cards 15:13 243:12 care 169:10,11 198:18 294:13 career 64:9 careers 231:12 careful 33:13 266:17 carefully 23:7 43:1,9 54:6 207:7 carried 29:20 43:15 108:10 136:19 carrying 91:22 case 24:20 34:18 45:1,3,15,15 45:16 51:6 58:15 65:14 66:12 68:14 69:1,2 73:4,4,7 97:16 105:15 114:12 118:9 122:20 174:11 204:11 208:21 222:8 226:13 231:5 238:22 240:7 249:1 250:15 261:13 272:11,17 273:7 cases 6:7 65:6,7 158:10 170:17	171:15 192:13 197:6 232:17 274:5 casting 27:4 castle 147:22 catch 66:5 174:17 297:17 catch22 37:5 categories 40:18 41:1 227:7 category 39:21 47:17 82:18 112:11,12 232:19 causality 129:22 cause 11:18 19:5 59:22 92:17 95:19 100:18 105:16 110:11 110:13 114:21 199:13 271:7 278:6 279:14 286:10 310:21 caused 150:19 150:21 causes 151:1,2 172:18 caution 28:2 190:15 cautionary 206:19 cdt 235:15 cell 9:21,22 19:1 166:18,19 center 2:14 3:6 3:18,19 16:8 124:17 125:6 210:19 211:1 235:13 central 220:5 269:20 centralized 73:16,17 75:3 century 32:12
---	--	--	---	--

180:2,3 194:16 194:18 206:20 certain 47:22 134:19 151:17 180:12 191:10 191:11,17 195:8 204:3 253:22 274:5 279:3 284:14 311:21 certainly 51:2 128:9 138:9 162:4 168:16 180:13 181:3 190:21 198:9 210:1 215:8 220:15 223:3 255:16 260:12 292:12 308:9 certainty 237:8 300:5 certification 319:1 certifications 41:1,13 certified 274:19 certifies 274:9 certify 319:5,9 certifying 41:2 chaining 137:6 146:2,17 258:7 258:18 285:3 chairman 2:3 125:14 challenge 16:6 37:10 92:1 100:10 135:5 151:16 152:2 152:15,16 154:7 167:17 challenges 124:6 149:3 153:8,15 197:7 challenging	133:11 157:21 215:21 chance 15:20 65:11 66:3 87:5 266:2 310:9 317:11 317:16 change 36:8 39:15 74:14,16 120:12 131:12 134:16 171:16 171:17 211:13 226:5 239:7 275:10 changed 119:13 286:20 288:15 294:18 298:16 303:5 changes 28:14 121:1 134:7 213:17 216:14 224:2 272:2 changing 108:6 149:18 193:16 characteristics 191:18 characterize 154:8 characterized 49:1 charge 248:12 charter 220:20 chases 137:22 cheat 263:18 cheats 246:2 check 272:20 274:14 checkpoint 280:2 checks 29:18 30:2 32:1 121:2 246:17 246:18,22 258:1	chief 5:7,8 99:14 child 184:4 264:2 chill 31:3 chilling 27:13 choice 96:12 235:7 choices 222:15 choose 6:5 138:17 312:20 choosing 35:1 chris 60:22 cipa 260:19 circle 18:11 circuit 66:9 135:6 circumstance 137:3 268:14 circumstances 49:14,17 262:11 274:16 279:10,12 281:10 284:14 circumventing 36:3 citation 238:16 citizen 12:15 13:3 126:5 165:13 167:13 170:7 172:10 citizens 23:4 27:22 145:7 151:1 165:15 167:7 168:11 168:11,22 265:18 city 162:5 civil 1:3 4:4,16 22:17 29:6 32:13 55:22 56:15,18,19 58:21 63:3 119:19,21 121:7 173:3,5	213:10 216:22 224:8 225:13 227:4 242:10 244:2,17 266:14 269:13 278:15 293:6 294:11,13 309:9,11 311:9 317:10 claim 134:4 152:20 201:11 claims 200:14 240:15 clandestine 289:22 clapper 37:1 47:7 49:2 100:10 111:2 clarification 142:19 clarify 115:10 189:11 228:13 250:9 clarity 59:11 240:1 class 185:5 classic 37:5 92:20 115:5 classified 6:2,3 6:5,8 42:19 95:10,15,18 97:18 98:14,14 98:15 102:14 132:2 249:5 250:14,16 252:9 253:9 255:10,16 256:4 257:6 260:6,10 308:4 classify 178:14 clear 49:5 52:12 53:17 59:14 60:8 64:2,19 65:18 86:10	98:12 111:14 115:15 158:10 172:13 181:14 239:16,16,22 245:12 299:3 clearance 96:2,5 clearances 266:1,20 cleared 97:5 clearing 237:13 clearly 24:18 cleartext 165:8 clerk 198:7 clever 142:21 client 112:8,12 131:17 clients 112:10 clinic 183:18,21 clock 107:9 close 118:4 139:12 173:21 208:6 209:12 300:9 closed 98:4 269:17 closely 35:13 133:21 311:11 closer 173:21 236:7 311:14 cloud 162:18 165:3,8 306:17 clouds 306:18 cobwebs 166:16 code 164:21 191:14 286:7 coded 217:22 codirector 210:18 cofounder 125:6 coin 237:8 310:6 cold 231:7 collaborators 57:11 colleague 15:1
--	---	--	---	--

colleagues 15:19 35:3 53:14 80:1 210:1	289:20 290:4 297:2 302:22 304:18 307:10 314:15	collections 117:1	265:18 267:4 273:9 289:11 292:20 295:9	commit 187:18
collect 9:17 49:14,18 59:18 59:19 60:10,12 61:6 95:4 98:1 98:8 112:7 115:14 116:3 143:10 148:2 156:13 183:14 227:9 231:18 232:7,12 258:18 261:8 264:12,17 276:3 289:1,6 290:16 295:6 300:8 308:14 311:20 314:17	collection 8:19 9:5,6 11:21 12:4 13:8,12 13:18 24:11 27:11,14 31:15 31:17 38:8,10 38:14 44:17,18 45:7,20 50:10 52:2,12,19 53:3,4,6,15,21 61:17 67:12 86:21 111:18 116:17,19 118:17 130:9 143:2 153:4,10 156:9,18,21 157:8,11 158:4 158:15 161:9 165:20 168:20 173:6 177:4 216:11 220:3 228:9 229:11 233:15 241:6 242:3 245:16 246:8 252:13 252:21 253:2 256:10 258:5 261:21 264:15 268:11 275:7 275:13,15,20 276:8 277:8 286:22 287:8 287:18 288:5 289:16 290:6 292:4,11,16,20 296:7 298:4 299:13 304:10 309:20 311:8 311:16 312:2 313:11,20	collects 8:20 23:17 27:8 48:19 152:6 183:14 collins 2:7 117:20 209:21 217:12,21 218:1,4,6 240:18 247:6 248:4 251:3 275:4 278:10 280:11 285:18 286:19 287:3 293:21 302:9 collinscook 202:19 color 217:22 columbia 3:3 124:11 combating 77:6 combination 149:9 come 7:19 47:1 52:17 72:7 74:14,15 110:4 118:21 122:9 127:18 133:6 150:18 164:8,8 166:13 173:21 181:20 191:5 194:3 195:21 197:4,5,18 214:19 219:2 226:21 241:14 265:16 285:21 291:11,12 312:8,20 comes 63:13 92:22 174:19 181:12 198:13 206:11 233:7 236:1 237:4	comfort 65:2 comfortable 90:17 270:2 coming 14:21 138:21 186:15 193:18 203:16 317:3 318:7 commencing 1:17 commend 60:21 comment 117:16 135:8 138:22 158:16 164:5 181:17 204:19 217:3 248:6 255:2 269:14 285:20 304:10 307:18 309:5 312:21 315:8 316:20 316:22 commentary 133:22 comments 7:7,9 32:19 44:6,7 45:22 88:2 97:8 123:8 125:12,20 126:12 131:1 132:12 141:8,8 145:3 147:3 157:22 175:1 175:12 218:10 223:14,22 224:14 226:18 226:21 312:8,9 312:15,16 317:1 commission 4:11 135:11 232:5 319:19	commitment 244:1 committe 210:13 committed 110:14,15 committee 33:5 46:17 227:1,1 227:3 270:9 committees 20:1 20:4 42:18 94:12 95:12 96:20 103:22 219:3 257:5,15 299:4 314:9 common 8:1 34:19 64:20 82:14,14 90:3 102:4,6 161:15 229:15 commonly 56:13 161:14 164:10,11 206:10 communicate 222:1 communicating 109:1,15 114:8 116:14 communication 9:19 11:22 53:1,4 108:16 115:21 136:11 136:20 146:6 146:20 213:14 259:20 276:7 296:21 299:21 302:15 311:22 communicatio... 9:8,18 14:8 21:22 26:14 29:10 37:3 38:9 43:5

44:19 47:12	47:18	36:14 41:17	56:9,17 57:5,7	46:7 107:6
48:16,18,19,20	comoderating	66:16 207:8,19	57:18 63:2	228:4 237:16
48:21 49:15	123:19	220:6 223:8	115:4	237:19 261:15
50:1,1 52:2,15	companies 9:16	224:20	concepts 290:3	conducting
52:16 53:11	17:11 67:16	complicates	concern 31:6	42:12 108:14
57:16 61:12,17	69:6,13 71:17	145:18 212:21	53:22 57:10	conducts 44:13
67:8,16 83:4	127:20 128:5	complication	64:4 79:6,12	confidence
83:21 95:4	128:18 151:2	282:6	80:14 106:17	58:13 80:7,9
108:9,21	201:21 202:1,2	complies 275:21	252:13 275:8	106:13 107:5
109:10,13	202:6,10,11,12	comply 224:11	311:22	150:11 152:19
110:1,4 111:19	282:8 283:21	227:20 235:6	concerned 246:7	191:9,20 192:1
111:21 112:8,9	284:6,6,19	compounds	263:5,6 293:5	192:5 220:22
112:13,15	289:1	102:7	302:16 305:19	269:16
113:18 114:20	company 22:2	comprehensive	concerning 79:2	confirm 203:5
115:14 116:3,5	70:1,5 81:6	25:9	116:7 241:2	confirming 6:10
116:7,13 117:7	83:12 127:16	compromise	concerns 4:17	confirms 41:15
117:10 128:1	127:16 128:7	46:13 94:5	10:13 24:3,4	conflate 258:5
135:11,13	128:22 129:4	182:11	28:12 79:21	confront 294:15
137:11 187:12	183:20 190:3	computational	108:3 173:11	confronting
216:6,8,9	compare 186:13	153:14 154:9	173:12,14	213:5
222:7 229:9	compared	204:6	244:15 269:15	confused 142:11
236:20 259:9	112:11	computer 3:3,9	274:4,7 292:17	confusing 50:5
276:3,20 278:1	compares 55:20	124:10,13	conclude 184:17	confusion
288:4 289:2	comparison	125:4 126:16	concluded 134:1	307:16
290:16 293:1	84:17 252:3	127:1,2 132:13	conclusion 25:2	congratulations
294:20 295:3,7	compel 85:15	132:14 133:2	138:12 204:2,3	148:13
295:15 296:15	289:1	142:3 149:6	310:19	congress 4:11
296:17 297:3	compelled	153:15 166:16	conclusions	5:17 8:17 12:7
297:13 301:9	155:21	186:16 197:19	7:19	19:20 20:1,3,5
302:2,14 303:1	competing	206:22	concrete 119:12	30:3 36:4
303:2	211:15	computers	119:22 120:6	38:15,20 39:2
community 9:20	complain 88:14	114:18 140:4,6	120:12 121:12	39:22 40:7,13
14:7 36:20	complaints	143:17 189:15	243:20 247:13	43:9,19 46:16
39:12 47:16	206:9 267:20	conceded 111:2	conditions	51:13 54:7
48:7 72:22	complete 22:2	112:17 301:15	157:4 218:12	55:13,14 56:8
74:15,20	completed 26:22	conceivable	conduct 20:13	56:12 57:22
106:11 119:19	completely	52:9 91:17	39:5 42:4	60:6 63:20
119:21 121:7	62:20 120:4	140:4,6	67:10 103:7	64:3 74:14
128:20 137:18	completeness	conceived 64:5	109:3 168:15	79:19 85:5,20
152:6 154:20	7:20	concentrate	168:17,17	88:22 94:12,12
190:7 222:14	complex 29:11	149:12	213:18 246:19	95:7,8,9 109:5
269:13 286:14	50:15 77:10	concentrated	300:3	110:18 122:14
292:15 293:9	217:8 233:20	149:11	conducted 22:16	139:17 147:5
communitys	compliance	concept 52:18	42:1 43:14	152:18 179:14

214:8,19	240:15 264:5	3:17 22:7	containing	contexts 20:22
218:14 225:19	265:4 268:9	24:12 27:16	305:16	57:20 71:20
228:12,13	290:2 294:11	33:5 44:21	contains 160:5	283:11 306:10
231:15 240:13	considerable	71:6 80:6	contemplated	306:14
245:2,14	136:7 167:16	92:15 100:15	38:15 43:9	continually 29:4
248:18 252:18	252:22	115:2 120:9	47:19 85:16	continue 10:12
255:2 256:6	consideration	210:16 223:21	content 17:17	318:2
265:4 276:15	105:11 113:22	224:12,21	21:22 24:10,16	continued
279:1,2,8	219:14 223:7	226:22 235:19	44:19,20 49:22	150:16 201:4
283:17 290:21	238:13 256:17	270:6	83:21 84:2	contractors
291:17 293:9	293:7	constitutional	136:11,16	315:4
297:10 298:2	considerations	2:10 5:15	137:16,20	contrary 17:22
318:4	244:11,14	14:17 16:6	140:20 143:21	105:20
congressional	considered 4:18	20:8 29:7,18	144:3 145:21	contrast 268:21
87:20 89:4	9:15 43:10	39:6 46:5 66:2	165:11 172:4	contributed
93:11 96:20	63:10 84:22	67:19 70:21	183:8,12,14	132:16
257:5,7	200:21 221:6	72:8 75:17	184:8,12 185:1	contributing
congresss	222:13 280:20	92:1 93:20	186:1 190:12	14:12
245:11	283:17 292:18	100:10 102:20	191:4,7,12,13	control 70:4
connect 20:17	293:19	151:20 157:15	191:15 216:12	153:16 159:11
146:11 264:10	considering	240:15 273:3	217:19 252:13	controlling 71:9
connected 61:18	100:16 101:16	constitutional...	252:20 254:4	71:9 153:17
286:17 287:14	considers 220:1	66:1,18 87:9	283:15 303:1	163:3
connectedness	272:18	91:19,21 100:7	311:16,20	controls 121:3
29:9	consistent 93:15	constitutionally	contentions 52:3	148:9
connecticut 1:16	94:7 97:22	45:19 76:1,14	contents 9:18	controversial
connection	107:7 205:1	259:22	113:19 114:10	109:4 128:2,4
102:21 227:16	243:22 287:9	constraint	136:20	controversy
228:1,6 287:11	288:11 290:2	257:13	context 21:7	272:11
connections	297:21,22	construct 105:7	27:21 36:15	convenience
18:19,20	298:1	consult 131:1	55:21,22 56:12	70:19 71:3
conscious 234:9	consistently	consultant 3:8	61:22 62:1,19	284:18
consequence	46:8	124:22	63:2,3 76:13	conversation
35:22	consists 17:10	consumer	92:21 95:20	78:1 114:3
consequences	constantly 82:19	188:14	96:15 113:12	148:17 240:22
189:6	constituents	consumers	130:20 149:15	247:1
consequent	257:9	135:16 265:16	149:20 205:13	conversations
268:10	constitute 26:2	contact 146:1,17	228:7 229:1,20	107:19 189:17
consider 34:13	66:15	170:13 228:20	260:19 265:14	converse 188:5
95:8 98:7	constituted	239:13 258:7	266:5 270:15	convey 253:1
99:21 100:2,7	24:22	258:18 285:3	271:2,4,6,15	convinced 97:21
101:15 117:22	constitutes	contacts 11:2	273:1 277:15	98:3 183:9
119:20 220:5	25:22	contained	278:13 285:6	convincing 73:1
220:11,16	constitution	136:18	308:6	cook 2:7 4:6

117:20 209:20 209:21 217:12 217:21 218:1,4 218:6 240:18 247:6 248:4 251:3 275:4 278:10 280:11 285:18 286:19 287:3 293:21 302:9 cooperated 35:5 copies 126:7 cops 241:12 copy 129:3 copyright 154:17 correct 44:15 76:21 82:5 86:19 121:18 188:22 189:8 200:15 296:3 305:9 319:6 correlation 129:21 correspond 25:20 corresponds 25:19 corroborate 72:22 corrupt 64:10 cost 71:2 176:8 263:16 279:6 280:19 281:6 costly 69:10 279:5 costs 314:19 couldnt 95:21 98:5 185:15 201:21 259:12 301:16 counsel 2:12 3:16 15:12 16:2 93:11	96:13 210:12 210:13,16 267:8 319:10 counselor 314:4 counterintelli... 208:22 counterparty 106:5 counterterror... 5:1,11 9:3 20:12 110:18 224:7 225:4 227:19 countless 40:11 countries 27:21 28:2 77:8 country 27:5 31:5,8 44:13 52:22 140:12 154:21 160:11 162:5 163:17 164:21 182:21 187:19 188:19 231:2 265:13 317:19 country s 5:1 124:12 231:6 county 319:4 couple 8:1 34:6 66:17 104:12 142:21,22 145:2 160:20 182:6 214:14 227:7 246:17 248:10 263:5 266:9 course 8:13 18:20 31:7 36:18 48:17 50:10 56:7 61:10 70:3 75:12 78:9 92:20 96:11 102:7 105:13	107:18 109:2 134:19 148:1 175:17,17 183:13 201:8 202:8 218:19 225:18 251:10 271:5 293:2 296:18 305:4,7 court 2:16,16 8:6,21 10:1,11 11:18 12:1,8 13:6,19 16:6 16:12 17:5,22 19:15,18 21:7 21:12,18 24:21 33:10,11,17 34:4,11 35:3 36:1,9,22 37:5 37:11 39:1,9 39:13,19 40:1 40:22 41:15,15 42:2,5,7 46:2,8 46:10 47:6 53:10 54:7 57:12 58:16 59:13,17 62:13 62:17 63:9 65:10 66:8,10 68:7,10 72:4 75:5,18 76:13 79:20 86:18 87:12,19 88:3 88:7 89:2 90:4 90:7,12 91:20 92:3 93:3,8,9 93:18,22 94:8 94:10,18,20 95:17 96:19 97:3,6,17 98:5 99:9,12,15,17 99:20 100:3,6 100:12,19,22 101:4,14,21 102:5,18,18	103:1,8 105:19 106:9,21 107:1 109:18 111:6 114:21 118:9 119:16 131:15 133:10,13 134:1,3,4 195:8,16,21,22 196:8 197:16 198:20 200:22 201:15 214:21 218:22 219:7 219:12 220:1 220:11,16,22 221:5,8,10,13 221:21,22 229:6 230:4 233:2 238:8,9 240:11 241:13 248:9,9,13,15 248:19 249:14 249:20 250:5 250:18,18 251:17 252:3 253:10,19,21 254:7,8 255:14 257:18,20 259:1,12,15 260:2 265:9 266:1 267:6 272:5,6,9,10 272:15,22 273:9 277:10 278:7 281:11 295:21 299:11 301:22 314:6 courts 22:3 24:19 29:20 30:5 45:17 46:8,15 47:9 78:21 92:4 94:6 99:20 100:14 101:16 152:17 176:5	214:8 219:14 249:18 268:7 271:21 272:8 272:11,13 covenant 262:2 cover 40:5 238:1 covered 46:19 61:14 87:6 108:10,16 297:6 covering 127:22 cpni 136:21 crack 217:1 crazy 79:18 create 38:20 69:19,21 75:16 77:3 94:11 141:18 143:9 150:9 266:4,18 284:11 created 4:11 40:17 46:13 73:20 81:3,7 82:10,16 101:22 102:7,8 138:15 221:16 creates 282:21 creating 46:16 77:16 102:3 119:15 180:6 creation 29:21 73:16 265:2 credibility 295:12 313:17 credible 310:10 credit 40:7 157:1 188:15 207:4 243:12 creep 245:21 263:8 291:20 crime 14:5 21:17 26:9 64:14 103:9 110:14
--	---	--	---	--

crimes 263:22 264:1	customer 130:5 135:14	149:15 150:17 150:17 151:13	283:11,13,20 283:21 284:1	68:13,18 78:12 90:1 93:12
criminal 26:8,19 27:2 53:8,8,9 53:13 55:19,21 58:22 61:22 62:1,10,19 63:2 64:16 65:1 76:13,16 104:18 105:10 221:7 263:12 263:12 270:14 271:3,6,10,15 272:17 277:16 308:6,13	customers 133:19	151:19 152:6 152:14,20 153:11,18 156:14 158:6,7 158:11,22,22 159:12 160:4,9 160:12 162:16 162:18,19 163:4,8 165:17 165:19,21 166:3 172:12 172:12,17 174:12 176:10 177:4 181:4 182:16 183:2 183:16 187:4,8 187:15,20,22 188:1,2,7,10 188:16,22 189:13,13,18 189:21 190:10 190:10,18 191:1 192:7 196:14 197:12 198:13 205:19 206:1,15,21 213:19 229:18 241:6 242:3,5 243:5 245:16 246:9,9,20 261:19,22 262:8,12,14,17 262:22 263:9 264:9,11,12,15 265:2 278:17 278:21,22 279:2,4,7,11 280:6,13 281:1 281:4,8,17,18 281:19 282:2,7 282:8,12,18,20 283:1,3,5,6,7	database 12:5 18:3,11,17 19:8,11 20:13 21:1,4 45:10 56:21 57:1,3 69:5,6,19,22 70:6 71:13 73:16,17 74:2 74:17,18 75:3 77:3,16 127:10 127:12,15 138:2 145:6 159:22 160:4 165:15 230:1 277:22 278:2	139:10 184:6 209:22 215:10 219:9 247:18 268:12 291:1 313:8 319:13
crisis 292:1	cycle 219:11,18		de 273:21 276:10	days 10:11 17:6 27:3 139:17 152:3 219:12 269:4
criteria 8:6 70:18	D		deal 190:13 197:18 215:6 215:17 216:2 259:12	
critical 20:16 44:20 135:15 187:1 225:22 236:12 262:20	d 1:17 16:1 66:9 132:16 135:6		dealing 89:14 90:17 118:12 171:10 221:1 268:17 269:22	
criticism 215:16	daily 29:11 81:6 268:15,16		deals 35:14 54:20 90:19	
criticisms 121:8	damage 310:21		dealt 221:18 248:14 252:12 254:3 287:8	
critics 120:19 214:17	danger 29:1		death 14:6 264:1	
critique 30:8 215:16 317:16	dangerous 283:16		debatable 28:22 29:2	
cross 283:16	daniel 3:9		debate 23:1 30:4 31:4 32:6 51:17,18 67:14 153:7 183:1 245:7 252:17 252:22 255:20 256:16 291:19 291:21,22 305:5	
crossed 138:13	danny 125:3 148:11 156:5 166:12 169:19 170:8 178:11 179:20 185:18 191:2 202:22 204:19		davidson 3:16 210:11 217:22 218:3,5,7 223:11,16 252:7 268:5 287:1 290:20 311:2	
crucial 24:14 72:18 73:2,8 73:12,12	data 11:1,5,7,10 12:4 17:13,21 18:1,2 19:9 22:11,14 55:11 56:22 67:5,6,7 67:16,17 69:15 69:16 70:12 71:7,8,12 127:8,20,21 128:6,8,9,14 129:11,16,17 130:9,18,20 131:7 137:4,5 137:10,20,22 138:7,11,14 141:18 142:15 144:1 146:20 147:18 148:5		day 5:3 6:22 35:2 65:5,16	
crushed 141:5				decade 79:16
crystallize 315:15				
current 59:3 64:3 134:8 136:12 137:3 157:10 205:12 212:1 213:13				
currently 16:5 124:9 125:3 156:13 202:2				

decades 232:4	91:11 96:4,8	demonstrates	163:16 173:20	14:13 281:21
december 12:7	96:13	42:22	195:8	310:2
89:5 305:3	define 84:9	demonstrating	depends 30:12	detail 25:10
319:19	defined 83:20	228:18	deploy 135:4	31:9 71:18
decide 84:6,7	289:8	demonstration	155:5,7 171:11	115:8 133:17
165:22 195:11	defines 130:10	279:12	203:4,9 205:3	136:7,21 190:5
273:17 286:4	definitely	dempsey 2:6 4:7	deployed 137:9	226:18
decided 98:4	192:12 287:22	117:16 119:8	deputy 16:4	detailed 95:18
132:14 137:2	definition	123:19,22	19:6	131:8 136:9
283:18	107:16 238:17	132:10 140:15	describe 133:7	243:15 250:14
deciding 34:18	289:9 295:18	148:10 155:14	145:2 202:6	278:8
195:13	295:19	155:17 159:18	216:17	details 42:19
decision 24:19	degree 29:3 47:4	160:13,18	described 15:4	95:10,15 123:9
135:3 204:8	145:14,15	161:21 162:7	20:15 38:4	227:6 230:5
250:13,14,22	195:7 201:1	163:6 164:2	41:9 44:17	detainee 96:2
253:18	216:5	166:12 169:3	45:4,14 102:12	detainees 91:9
decisions 218:21	degrees 193:3	172:19 181:17	133:18 165:8	91:10
253:14 254:7,8	deidentification	181:21 183:4	178:12	detect 154:14
declassification	139:7	185:17 188:2	describes 9:10	180:19,20
89:12 251:6,12	delete 316:4	193:5 194:8,12	61:2	detecting 208:12
declassified	deleted 61:20	199:1 200:16	describing	detection 206:13
5:22 131:20	233:17 306:17	201:16,18	83:18	determination
308:5	deleting 316:11	209:11 294:9	description 7:12	95:19,20
declassify 93:13	316:12	296:22 297:7	49:11 61:1,4	134:18 170:1
249:4	deliberately	298:3,15	154:19 156:6	170:14 198:22
decreed 29:19	32:9 113:18	300:11 302:6	289:18	201:12 262:5
dedicated 91:8	deliberation	303:20 304:2	deserves 307:8	determinations
deemed 287:9	245:10	316:14	design 112:16	36:14 100:18
deeper 215:5	deliberations	dennys 314:13	121:10 155:3	157:15 188:18
deeply 33:13	40:13 245:11	deny 255:17	168:6 174:20	197:13
292:19 293:20	delivers 165:6	department 3:4	205:2,21	determine 13:21
294:13	delivery 53:12	16:2,17 33:15	214:18,18,22	41:6 135:11
default 274:13	delve 65:22	91:8,12 124:10	215:1 244:13	151:21 154:2
288:15	demand 56:15	135:2 183:19	278:14	165:13 167:12
defect 314:11	267:19	210:8 211:3,4	designated	208:4 292:6
defects 313:22	demands 22:7	222:5 252:10	18:12	determined
defend 260:10	268:2	254:6 267:4,5	designed 8:2	10:17 240:9
defendant 260:8	democracy 3:19	267:21	86:8 112:14	305:22
260:9	29:4 125:6	depend 29:3	designing	deterrent
defenders 97:9	211:1 235:13	131:13 232:2	173:17 199:5	174:16
120:20	demonstrate	313:18	designs 41:4	develop 119:22
defending 91:10	32:6	dependent	desirable 140:2	171:1 241:22
defense 27:7	demonstrated	181:14	140:9	264:15
29:6 91:7,9,10	207:9,14	depending	destruction	developed 90:4

154:13 314:14 315:6,7 developing 149:5 203:12 development 4:18 152:12 155:2 203:2 219:16 device 45:2,15 166:17 167:3,8 167:10,12 169:9 devices 83:3 166:21 213:14 devils 273:20 274:8,13 devoting 313:9 dhs 189:3 dialed 9:12 26:21 dialing 286:8 diane 5:7 15:12 123:8 312:17 317:6 didnt 26:22 56:8 63:20 64:17 90:10 94:20 111:10 114:1 116:20 122:9 138:4 174:22 186:18,22 197:18 240:11 259:14 303:20 311:19 differ 8:6 difference 44:20 71:7 143:19,20 255:6 271:5 different 17:7 25:3 54:5 61:10 65:1 69:12 71:15,19 77:14,15 83:3 84:11 98:12	100:13 130:11 142:21,22 143:12 160:14 161:16 170:19 174:4 184:15 191:3 213:1,2 214:14 216:7 222:4 246:17 253:20 255:15 257:21 259:7 263:17 265:12 271:13 275:5 275:17 286:7,9 286:11,16 295:5 300:12 308:20 differentiate 166:11 207:12 differently 211:6 247:21 302:10 difficult 111:11 129:10 216:12 235:7 249:7 difficulty 208:17 dig 123:1 digital 24:8 137:3,4 141:17 186:4,7,11,12 187:3,8 189:12 190:18 191:1 digitized 186:10 dimensions 151:6 307:14 direct 251:10 directed 27:2 39:10 294:10 directing 10:4 87:16 directive 12:10 directives 119:3 directly 157:13 228:21	director 12:11 16:5,8 19:6 134:12 144:6 210:21 disadvantages 212:7 disagree 49:10 103:2 287:20 disagreement 213:8 disaster 79:8 disburse 162:21 discern 145:21 disclaimer 126:3 disclose 102:11 107:1 disclosed 7:14 22:22 23:11 47:14 49:4 86:16 98:18,20 98:22 248:20 disclosure 96:12 173:6 226:6 256:13 308:2 disclosures 38:5 43:6 109:4 222:17,18 225:5 227:2 276:1 discontinued 236:11 discovery 65:12 discreet 274:2 discuss 34:12 229:21 235:16 309:10 discussed 15:5 116:11 218:12 221:2,3 223:5 240:17 247:14 259:1 291:1 292:9 discussing 6:8	discussion 5:15 5:21 6:1,4 7:12 86:16 108:6 142:20 218:19 222:10 224:10 226:3 229:10 254:14 303:12 303:17 309:12 317:4,15,20,22 discussions 148:16 213:3 312:4 317:11 disposition 221:10 disputing 177:5 disrupt 234:17 disseminate 112:7 disseminated 13:22 305:15 305:18 307:1 disseminating 306:5 dissemination 14:1 19:16 41:10 287:15 305:2 dissent 31:3 distinct 21:22 distinction 39:17 82:22 143:20 168:12 184:11 261:21 298:10 distinguish 101:20 207:18 208:16 distinguished 15:7 210:5 distinguishes 82:9 136:16 distinguishing 65:19 168:10 district 2:15	16:10 101:9 111:6 197:16 distrust 215:11 division 2:18 16:16 dna 85:9 dni 24:9 40:22 93:11 306:3 doctor 174:15 doctrine 131:3 document 81:4 121:21 122:1,3 documents 6:2,6 6:7,10 21:13 57:4 122:10 135:19 205:19 209:3,6 251:12 252:8,9 doesnt 17:19 59:21 65:17 81:10 88:12 99:20 100:1,6 101:14 114:2 134:21 144:8 144:15 162:16 164:18 168:12 181:8 182:11 186:4 188:8 192:21 201:14 219:19 233:10 273:6 276:10 280:5 281:16 297:20,22 308:17 dog 315:2 doggedly 45:5 doing 29:11 30:20 39:2 60:3 93:16 96:15 101:7 103:12 132:3 135:22 155:8 177:20 178:9 178:17 180:16
--	--	--	---	---

189:3 200:14 205:6 208:14 208:17 214:9 244:21 253:5 269:17 278:18 302:18 doj 2:11,17 3:14 dollars 200:13 314:20,21 315:5 domestic 39:4 39:17 43:4 48:21 94:4 135:9 148:4 296:16 297:12 297:13 301:9 donig 264:20 donors 257:10 dont 21:18 31:16 36:13 44:14 50:18 54:18 59:9 63:4,5 69:8,9 69:14,17,20 70:8 71:6,21 73:8 74:8 77:8 77:18 79:10 82:8,22 84:12 84:17 85:18,19 88:6,15,18,18 90:15,22 91:5 91:16,19 92:5 96:5 98:5 101:18 106:21 109:15,21 117:15 128:4,9 128:22 129:13 130:16 132:2 140:1 141:15 142:4,5,5 143:17,18 146:9 147:13 147:16 155:6 156:19,19	157:19 158:12 161:21 162:13 164:17 169:10 170:4 172:12 175:4,15 176:3 179:17 180:6 187:10 188:20 189:4 190:15 190:19,19 194:3,6 196:5 198:7 199:5 203:19 204:8 204:17 207:22 208:16 213:3 214:17,22,22 215:2,9,16 216:16 226:9 235:16,19 236:2 237:6 238:3,5,15 240:4 241:20 246:1 252:1,4 254:16 255:17 258:5,9,10 261:8,8,17 264:13,18 265:16 267:15 271:14 272:6 272:13 273:1 273:14 277:1 284:10 285:6 288:8 290:10 290:14 298:22 303:8,11 309:16,17 312:22 door 234:3,8 285:10 doors 98:4 dots 20:17 108:22 264:11 doubt 77:2,7 298:6 downloading	209:2,6 downsides 234:14 293:11 draft 125:19 126:7,11,11,15 141:8 drafted 116:18 dragnet 24:2 44:17,18 314:22 315:3 drain 202:15 dramatic 186:3 draw 59:4 138:12 149:15 149:17 168:12 253:19 300:13 drawing 298:10 drawn 105:9 drive 10:16 driving 187:4 dropped 266:21 dropping 314:16 drove 79:18 drug 183:21 192:17 drugs 253:6 duces 81:16 due 63:6,6 dug 121:20 duration 17:14 27:1 dying 202:13,13 202:15 dynamic 171:7	248:5 275:7 277:13 early 54:15 139:17 314:15 easier 95:3 248:16,21 249:12 285:7,9 285:16 easily 71:21 126:9 129:7 131:10 143:22 149:18 163:20 eavesdropped 114:4 echo 140:17,17 164:4 edna 167:21,22 education 107:3 effect 27:13 269:5 299:16 effective 69:11 80:9 87:8 139:11 147:11 150:12 178:4 179:12 181:5,7 188:10 192:12 192:14,14 199:9 203:3 234:13 effectively 313:19 effectiveness 159:2 176:14 177:21 181:1 192:20 effects 313:15 efficacy 103:19 efficiency 70:14 128:13 203:13 204:6 228:3 efficient 69:10 70:9 83:13 128:15 251:10 251:13	efficiently 189:20 effort 159:15 efforts 5:1,9 14:11,14 eight 90:6 286:7 either 28:14 125:19 158:12 182:5 185:14 200:3 214:16 214:17,21 285:4 316:4 elaborate 66:4 93:6 elected 257:8 electronic 3:5 11:16,22 29:10 38:21 124:16 174:5 175:21 232:14 element 305:19 elements 147:14 196:15 220:17 elephants 245:14 elicited 252:22 eliminate 140:8 157:8 eliminating 299:17 elizabeth 2:7 3:18 eloquent 152:3 eloquently 201:6 email 24:1 71:16 71:17 135:22 143:21 144:3 145:4 164:17 164:18,19,22 165:3,3,5,6 166:9 178:1,14 238:1 emanations
---	--	---	---	---

245:19	encryption	enter 44:4	essential 20:13	everybodys
embarked 290:9	139:7 159:10	entering 187:17	essentially 4:21	285:10
embraced 56:12	ended 52:6,7	entire 55:10	97:10 177:13	everyday 229:15
56:13	120:3 179:3	56:21 253:13	178:6 250:12	everyones
emergency	endpoint 312:4	entirely 22:16	establish 73:1	238:22 239:2
174:9,11	ends 275:1	239:22	106:13 111:4	evidence 14:4
274:19,20	enemies 231:11	entities 155:9	231:16	65:10 234:12
281:12	enforce 131:14	180:14 201:20	established	235:20 241:14
emphasize	312:17	283:7	125:10	241:18 263:11
226:19	enforcement	entity 265:17,21	establishes	272:20
emphasized	154:16 166:7	265:22 266:18	51:15	evidently 69:22
24:9	168:16 176:2	293:5 314:1	establishing	evolve 298:13
empirically	180:3,5 194:16	envelope 136:17	91:3 171:7	evolved 136:15
292:7	231:7,17	136:19	177:6	ex 34:7 35:9
employed	232:11 283:8	environment	estimate 301:16	88:3,4 92:21
235:15	286:14 307:3	150:9,9 190:17	etcetera 46:3	102:8 104:21
employee 79:17	engage 59:8	192:8	62:7 70:13	105:10 175:14
266:19	120:15 239:4	envision 250:10	71:10 81:10,16	194:21 246:20
employees 97:11	282:19	envisioned	83:6,8 94:13	270:1 272:19
employer 212:1	engaged 30:13	235:18	109:17 121:3	exact 232:1
employers 212:1	47:10,15	epic 132:19	294:19	238:15 241:20
empowered	119:15	133:1 134:10	ethnic 234:11	exactly 38:15
142:10	engagement	136:1 139:3	eu 127:21	43:8,19 47:16
enable 17:19	43:16 121:15	equal 191:6	euphemisms	49:5 51:13
18:18 46:14	engages 30:3	equally 158:13	115:6	64:5 78:5
150:2 154:14	134:15	284:5	europe 128:6	79:11,15 91:1
enabled 243:1	engaging 120:16	equipment	evaded 200:3	104:17 115:7
enables 20:19	257:1 317:4	143:6,22	evaluate 86:14	168:5 177:20
51:6 109:18	engines 126:10	164:14 165:9	196:9 198:10	213:10 261:14
137:5 288:22	enhance 196:2	equipped 88:18	198:13 299:12	271:3
enabling 29:20	248:7	era 213:13	evaluating	examine 154:1
enacted 55:15	enhanced	eric 90:1,2	270:2	186:13
76:12 108:8	200:19	erosion 29:17	evan 313:7	examines 27:9
encompass	enlarged 200:22	232:10	evening 7:5	example 11:9
56:21	enormous 46:19	ervin 28:16	event 5:9 317:6	56:15,21 57:9
encounter 166:5	133:22 176:12	especially 29:15	events 65:17	58:6 64:9 84:1
encountered	ensure 4:17	36:19 50:1	eventually 318:3	91:7 94:16
241:10	30:18 70:11	55:19 86:19	everybody	130:2 142:13
encourage	80:7 109:19	89:13 163:12	37:15 47:15,20	145:6,9 152:13
236:15 270:9	207:7	163:14 189:17	52:13 58:13	182:15,18
291:9 316:8	ensuring 4:14	190:13 273:22	60:1 69:1 87:5	193:22 196:18
encrypt 153:18	13:11 42:8	espionage	90:6 122:8	203:8 212:22
encrypted 160:1	71:10	262:16 279:17	124:1 125:21	237:20 238:1
172:12 316:7	entail 207:15	essence 274:5	155:19 298:5,6	254:1 255:7

258:14 260:6 285:12 290:15 292:10 examples 58:5 192:15 241:4 245:3 258:13 258:15,16 ex ante 246:18 exceed 295:20 exceeded 136:5 201:2 exceedingly 190:9 exceeds 230:18 excellent 317:4 exception 274:15 281:12 exceptional 274:15 exchange 6:21 exchanges 143:8 165:10 exclude 39:22 exclusive 103:6 239:20 253:3 exclusively 64:13 excuse 19:13 executive 4:9,13 19:20 30:9,20 35:4 43:13 48:5 54:8 67:9 94:2 96:18 97:4 222:7 231:15 233:6 244:21 247:3 255:13 exercise 59:7 75:21 exigent 274:15 281:9 exist 62:11,12 77:15 existence 30:3,5	30:13 72:2 75:2 82:2,20 86:19 116:8 140:22 233:3 239:19 265:1 existential 245:22 existing 67:7 82:18 83:13 203:10,10 206:12 224:11 224:11,21 225:7,9 228:8 230:1 251:12 exists 160:4,9,12 161:4 214:18 216:4 exnsa 114:16 expand 99:6 142:18 144:4 expansion 29:14 202:4 expect 5:21 171:11 197:11 280:15 expectation 22:4 25:5 131:13 198:17 220:10 expectations 24:17 180:19 expecting 141:10 expend 194:2,5 expending 39:18 expensive 159:12 experience 90:8 90:15 105:18 252:8 253:5 experienced 222:2 267:9 experiences 28:1	expert 124:18 201:9 expertise 198:10 experts 15:8 124:5,12 133:2 153:21 210:5 expires 319:19 explain 93:14 148:8 explaining 52:5 111:6 explanation 147:12 148:1 explicit 240:14 explicitly 103:6 225:15 298:3 exploitation 23:7 264:2 exploration 265:3 explore 315:21 exploring 247:19 exposes 140:21 141:2,4 express 190:14 expressed 78:13 expressing 33:6 38:9 47:4 255:3 expressly 14:2 245:17 extend 125:22 291:22 extended 25:7 extension 130:12 extensive 66:11 125:1 extent 50:14 80:20 92:15 93:15 94:6 106:12,19 153:11 219:14	222:11 225:7 225:20 230:5 253:3 256:3,7 256:9,12 301:12,20 302:11,17 305:22 309:18 310:9 exterior 136:18 external 200:7 201:19,20 202:18 246:18 extract 249:7 extraordinarily 22:12 252:16 extraordinary 22:11 102:4 extraterritorial 297:8 extreme 285:12 extremely 49:21 50:15 56:16 57:6 189:19 202:20 eyeball 262:8	fact 26:3 33:18 34:19 45:18 60:14 66:8,10 67:9 68:2,2 73:8,12 76:2 77:8 85:3 101:15 102:3,6 102:9 105:12 111:5 137:16 138:4 141:20 144:18 146:1 147:16 148:2 152:21 165:2 166:2 174:14 179:2 184:18 189:10 192:18 202:15 205:10 207:19 221:1 222:20 227:18 241:21 252:18 253:14 261:19 274:22 285:16 288:21 291:14 294:16,19 309:8 317:13 factbased 231:20 factdependent 268:20 factors 62:2 71:3 169:16,17 facts 122:16 126:13 226:12 228:18 239:10 249:5 250:15 factual 234:7 factually 293:20 fade 140:7 fair 59:20 155:3 188:15,17 226:2,18 229:10 fairly 64:20 242:12 243:14
F				
faa 38:18 40:17 42:11,15,22 43:10,21 54:4 236:17 288:22 301:12,13 304:3 face 50:6 140:13 233:10 253:4 facebook 185:7 facets 66:2 facial 100:2 facilitate 255:20 facilities 70:10 94:13 100:21 213:14 facility 110:15 facing 124:6				

faith 195:12	94:7 95:14,22	50:15 301:18	262:21	42:2,7 43:4
fall 184:12	97:13	figured 205:3	firewalls 153:19	46:12,12 52:8
227:7 232:19	feature 65:19	figuring 204:22	159:11	54:7 55:7
234:9 298:19	164:6	fii 289:9	firm 16:1	60:16 62:13
fallen 158:8	features 244:15	file 98:10 250:2	133:16	63:9 68:6,19
falling 297:18	fed 179:5	filed 111:5	first 4:5 6:13,15	72:4,6,7,9,10
familial 25:10	federal 5:10	133:10 221:9	8:16 13:7	76:4 79:20
familiar 35:18	7:14,17 17:5,8	223:20 224:14	14:16 15:2	81:19 83:20
241:8,11	21:11 22:8	filter 169:6	18:10 24:6	86:12,18,20
314:13	97:9 134:14	final 125:19	27:12 30:2,16	87:3,19 88:3,7
familiarity 90:5	135:10 263:11	138:21 185:5	33:3 34:7	88:11 89:2
family 149:5	263:22 266:19	187:9 201:5	38:19,22 44:11	90:4,7,14,20
famous 90:11	286:7 317:14	312:13	54:20 72:17	91:16,19 92:2
fan 158:18	feds 262:18,21	finally 30:9	75:20,22 78:2	92:3 93:3 94:5
far 69:10,10	feed 200:6	32:10 61:8,21	89:22 98:19	94:18 97:17
70:9 72:22	feedback 179:13	93:7 95:13	99:21 108:8	99:8,9,12,15
74:6 135:19	188:21 193:9	125:3 131:19	126:19 127:14	99:17 100:3,11
136:9,9 168:9	feel 48:1 80:2	135:17 147:2	133:7 136:3	101:14,21
184:7,7 185:22	88:14,18	230:2 240:4	139:14 144:5	102:18 103:6,8
189:4 221:15	142:10 147:4	258:20 314:1	150:1 151:7	103:15 104:11
226:7 227:14	150:19,22	find 11:13 31:10	155:18 160:18	105:19 106:9
235:22 244:19	151:1,2 178:16	73:21 79:2	169:6 170:7	106:21 107:1
246:6 258:14	316:11,12	89:1 117:9	174:19 181:20	108:7,11,16
263:4,13	feels 155:20,21	126:9 129:22	199:8 211:6	110:9 114:21
277:19 302:16	feet 172:22	138:3,4 146:7	224:6 227:8,10	114:22 116:18
fascinating	feinstein 66:21	152:7 181:2	236:17 238:16	116:20 119:16
175:8 186:17	fellow 4:5	186:22 188:7	244:10 255:19	168:14,19
186:17	125:13 240:20	191:12,21	256:22 263:5	175:12 176:16
fashion 99:5	felt 87:12 227:3	192:7 199:19	264:14 265:7	177:7 179:8
180:12	297:11	242:1,18 243:6	280:6 283:12	182:3 194:22
fast 258:21	fewer 11:9 19:8	253:18 258:8	firsthand 33:22	195:8,16,20,22
fastidious 33:14	fiber 108:12	263:11 280:2	fisa 5:13 10:1	197:15 198:6
father 86:2	302:2	293:10 295:5	12:8 13:6 17:5	217:11 218:22
fault 232:5	field 210:6	315:17	19:3,13,20	219:1,12,14,17
favor 184:20	264:15	finding 150:4	32:11 33:10,11	219:18 220:1
245:6	fields 17:13	199:9,10,19	33:17 34:1,4,7	220:16,22
favorite 126:9	315:20	221:20	34:10,11 35:2	221:5,16,21,22
fbi 19:2 33:15	fifteen 40:9 52:4	finds 129:21	35:4,9,10,13	229:5 230:4
50:13 232:14	300:16	fine 35:14 55:4	36:3,4,8 37:11	232:13 233:2,9
fcc 135:15	fifty 132:4	207:22 250:1	37:19 38:2,12	236:13 238:8,9
fear 231:4	fight 260:20,20	302:10	38:18 39:1,9	238:13 248:8,9
feasibility 70:22	260:22	finish 163:10	39:16,19 40:1	248:19 249:14
71:5	fighting 261:1	246:16	40:14,22 41:14	252:3 253:3,3
feasible 67:12	figure 29:5	firewall 246:3	41:15,17,19	255:14 257:18

259:1,7,12,15	14:17 16:22	force 64:8	89:8,8,11	40:4 101:11
260:2 265:9	23:14 37:18	252:20	222:9 242:22	103:15 127:9
266:1 267:6	38:2 49:17	foreign 1:7 2:16	284:18	138:11 159:14
268:6,12 269:2	50:3 123:17	8:5,22 10:22	forma 200:4	159:17 172:6
270:13 272:5,9	159:20 230:15	11:21 12:2,12	formal 134:11	182:15 192:13
272:11 274:11	236:3 247:22	12:16 13:8	154:9	223:3 232:5
276:2 277:10	248:2 290:20	14:3 16:11	format 186:12	297:15 306:11
278:7 280:14	focused 23:1	18:6 29:2	formation	founding 139:4
281:1,11,13	45:12,16,18	35:17 38:22	244:10,19	four 54:5 124:4
289:11 291:5	59:2 64:13	39:16 40:19	former 16:10	141:7 292:1
291:10,12,13	71:11 82:18	42:4 43:11	35:2 63:19	fourteen 17:7
297:6,6,7,10	94:3,19 95:3	46:6,11 48:14	64:3 80:1	52:4
297:22 298:3,4	109:9,20 110:5	52:14,20 93:21	120:21 121:9	fourth 21:5,9,19
299:11 301:13	110:15 151:12	94:20 95:3	125:5 139:14	24:5,14 25:1
301:17 303:16	204:19 292:21	101:5 109:14	144:5 210:8	27:10 41:17
303:22 304:3,4	292:21	110:19 112:2,4	211:3 212:1	43:14 66:15
314:6	focuses 43:11	113:11 133:12	formerly 2:11	75:9,13,19
fisc 34:5 36:6	163:8 169:4	168:20 228:20	2:15,17 3:14	78:3 92:15
59:8 157:1	focusing 15:2	229:3,6 231:22	3:16	98:1 107:22
179:14 201:2	52:14	237:21 238:17	forms 247:2	108:3 109:21
240:5,8 256:4	foiled 311:5,18	239:10,13	311:15	109:22 111:3
fit 239:4	folks 56:18	248:13 266:12	formula 52:7	112:17 113:5,8
five 15:7,10	118:22	289:6,7,10,18	191:5	113:10,14
18:18 25:3	follow 19:14	289:21 295:19	forth 93:7 250:6	130:16 168:11
54:5 74:10	36:11 196:19	296:14,15,16	267:5,9	168:13 220:9
112:5 125:10	202:22	299:9 301:9	forty 137:1	220:12 223:7
155:18 180:17	followed 125:11	302:8,8 307:5	140:5	227:20 235:6
196:19 197:3	252:17	foreignborn	forum 226:2	275:22 277:5
211:9 253:20	following 45:5	300:20	318:5	278:5 285:13
279:8 283:5	68:7 118:3	foreigner	forums 52:10	287:10 288:17
fix 159:8 197:4	132:12 136:15	229:13 276:4	225:17	302:21 303:6
flag 209:7	160:19 200:1	foreigners 49:15	forward 28:5	313:13,21
flat 52:3	211:10 271:10	50:5 233:11	44:1 120:1	fraction 19:9
flaw 184:10	271:11	276:5 294:20	121:8 136:19	27:9
flexible 54:15	followon 57:10	295:3,7	173:15 216:15	framework
flier 243:9	follows 7:12	foreignness	218:15 248:17	173:14 247:17
flight 58:8	followup 6:18	237:5,11	249:11 250:11	frameworks
flights 57:13,16	11:15 59:2	289:13 290:12	311:1,1 318:1	175:21
flimsy 103:12	70:16 121:13	forever 74:19	forwardleaning	franklin 3:17
flip 174:1 180:8	122:6 156:4	112:3 172:20	224:22	210:15 223:18
237:8	181:21 188:4	forget 103:5	foster 5:14	254:18 270:5
flow 317:6	197:14 199:2	161:22 200:9	fought 23:9	274:17 275:18
flying 57:13	200:16	forgot 103:13	found 18:20	284:21 299:2
focus 5:10 6:13	footing 265:5	form 40:14 53:5	26:1,3 39:18	frankly 33:12

89:22 90:5	fundamental	305:13 306:3,7	226:10 235:3	316:9
228:2 309:15	134:22 212:18	generally 67:11	281:8 283:11	go 57:7 61:15
freaking 316:3	215:11	112:13 147:21	294:7 297:19	62:13 73:10
free 39:12 231:2	fundamentally	218:16	310:10	80:17 83:13
234:6 317:22	30:12,16 50:17	generate 25:8	gigabytes	104:18 107:10
freedom 135:18	102:16 292:4	77:5 203:15	141:22 178:2	108:5 114:20
139:6 210:22	further 26:8	284:16	girl 280:1	117:17,18
284:8 290:10	60:20 138:10	generated 19:16	give 15:8,10,16	130:2,21
freely 39:5	138:10 178:18	143:16	17:16 51:10	132:14 147:15
frequent 243:9	183:5 242:20	generates	66:3 89:12	157:1 163:10
frequently	265:3 319:9	137:20	106:2 123:9	164:2 165:4
56:13	future 80:14	generating	130:2 135:8	169:19,22
friction 300:6	81:7 138:15	39:19 143:14	143:13 147:22	172:19 190:2,5
friendly 244:18	fuzziness 208:2	143:15	159:22 166:14	193:6 194:12
friendship	208:2,4	generations	169:14,15	204:18 217:12
185:10		23:8	179:8 182:13	222:11 231:2
front 15:13	G	generous 155:17	199:7 238:12	246:2 247:5
139:3 152:4	gag 202:2	genuine 150:10	249:8 266:19	249:6,22
205:7 246:11	gains 243:19,20	geographically	278:20 293:22	251:11 259:18
248:12 273:4,9	gambling	162:12,21	given 86:19 89:6	264:22 267:9
290:6 299:7	161:19	geography	89:9 95:9 96:8	278:3,6,11
314:6,8	gap 124:7 203:1	141:14 144:8	118:9 150:7	285:9 287:7
frontier 58:19	gaps 208:7	144:12,16,20	153:18 154:12	288:3 294:4
frontiers 58:19	gather 189:21	147:1 160:20	167:16 170:18	295:4 297:17
frustration 47:4	285:8	160:20,21	196:10,10,11	307:19 310:12
48:1	gathered 49:19	161:2 163:4,7	197:1 220:19	311:19
full 155:19	138:14 176:9	163:8 169:4	258:14 280:13	goal 150:5,7
217:13 226:6	275:2	170:8 172:1,15	294:2 316:4	188:6
226:10,14,15	gathering	geolocatable	giving 28:9 42:7	goals 149:1,8,22
276:17	110:19	181:16	68:14 122:16	197:8
fullblown	gay 185:9	geolocation	124:2 131:4	goes 65:9 92:7
303:12	gaydar 185:6	161:15 162:9	204:16 239:11	93:6 163:4
fuller 32:20	gee 63:20 64:17	164:13 196:18	317:16	195:6 244:19
282:8	127:3	geolocations	glass 174:10,11	261:22 263:2
fully 53:17 97:4	geeks 147:21	164:12	glean 185:21	267:2 272:1
310:9	general 12:10	george 3:20	global 29:9	275:20 306:2
function 34:14	15:12 19:21	211:3	144:8 206:16	306:16 307:10
99:4 102:5	24:4,8 40:21	germans 290:18	206:16	going 11:7 16:22
174:21	45:20 67:14	germany 238:3	globalization	18:17 23:14
functional 149:1	85:4 87:10	290:15	301:5	44:3,8 46:18
149:8	93:10 98:21	getting 52:18	globalized	49:18 53:11
functions	134:12 160:22	68:10 73:14	300:17	64:12,18 65:11
152:17 171:9	181:22 210:12	83:21 88:17	gmail 165:4,6,7	68:5,11 69:21
272:4,5,7	247:1 274:9	149:3 192:16	315:19,20	70:5,6 74:9

78:2,10,15	298:9 301:20	29:14,21 30:18	269:3,17	grateful 125:20
80:17 91:5,18	gold 191:4,16	31:1 32:8	272:18 278:16	great 36:17 63:8
96:9 98:7	golden 231:17	39:18 40:4,9	278:19 279:11	89:14 95:6
108:4 116:3	232:3	41:4,12 42:3	279:20 280:5	115:5,8 121:6
117:21 123:11	goldsmith	42:12 43:16	281:16 282:11	133:2 141:2
123:15 126:6	257:12	45:5 47:7	282:14,21	148:18 179:16
130:21 131:7	good 4:2 14:21	48:13 49:1	284:10,11,13	190:12 197:18
141:6,11 143:3	34:8 37:14	50:11,18 51:2	285:1,15,22	207:17 306:4
143:13 144:4	65:10 97:17	55:10 59:17,19	287:12 289:1	317:19
148:5 149:6	107:2,3 122:4	61:5 67:4 68:9	290:14,15	greater 106:13
151:13,14,19	123:15,22	69:15,21 70:3	295:2,14	218:20 220:22
151:22 153:9	153:16,17,22	70:10 71:8,9	297:15 300:3	229:5 256:1,5
163:2 169:19	178:5 185:17	72:15 73:4,9	301:15 302:18	256:6,14 299:7
171:16 173:15	188:3,7,15	74:3 75:8,14	302:22 310:11	greatest 6:20
174:9,13 181:3	194:12 195:11	75:16 77:2	317:17	43:13 225:20
184:5 193:21	197:21 199:15	79:17 81:2	governmental	green 15:13
199:3 202:14	200:3 204:22	84:13 86:11,18	87:21 265:17	218:2
204:13 206:2	235:21 237:5,6	88:12 89:7	governments	greg 3:19
209:14 211:5,7	237:7 240:16	92:21 96:4,9	9:4,7 11:20	210:21 235:12
211:16 212:8	241:13 242:18	96:11 97:3,12	13:15 27:17	241:5 258:21
212:14 214:13	242:19 261:1	98:1 100:18	29:7 38:8 39:5	282:16 300:11
215:6 216:16	262:17 264:12	106:19 111:1,4	53:11 65:2	gregs 261:16
217:14 219:4	264:17 267:15	111:22 112:1,6	99:22 101:2	grist 68:14
219:11 222:14	271:19 279:20	112:15,17	105:22 114:9	ground 5:20
229:22 237:2	312:4 315:6	114:19 117:5,8	184:14 188:9	35:19
245:15 248:17	google 262:9	120:21 121:9	213:18 220:2	grounds 239:11
248:17,20	googling 315:18	151:18 152:12	245:8 284:17	group 91:8
249:2,11,12	gosh 235:21	183:14 214:5	310:6	154:6
250:7,10	gotten 190:9	215:12,12	governs 67:10	groups 52:11
251:21 255:16	198:4 276:17	219:19 220:6	gps 9:22 45:2	221:9 269:19
262:12 264:12	gov 7:6,9	223:1,2 225:3	166:20	growing 90:14
267:14 268:2,3	govern 74:16	227:9,19 229:5	grain 126:14	growth 213:17
279:6 283:7,8	governing 153:3	232:2,6 233:1	grained 208:1	guantanamo
283:8,14,15	government	233:13 234:6	grand 21:15,17	91:9
287:6 300:12	7:14,17 8:9,20	234:16 235:20	57:6,11 58:7	guarantee
307:9 309:21	9:2,14 10:5,7	236:15 238:3,6	65:1,7,8,15,20	138:19
310:22 311:1	12:5,13 13:22	246:10 248:7	81:16 84:16,18	guarantees
312:13,16	17:1,16,19	249:22 252:7	grandfather	140:14
313:18 318:1	18:5 19:13,14	252:19 253:10	86:2	guerre 273:21
goitein 3:18	21:8,10,20	253:19 254:10	granted 118:8	guess 63:16
210:18 230:11	23:3 24:10,15	257:1 258:13	162:14 317:14	64:21 79:2
256:19 270:22	25:8,17 26:9	258:17 260:19	granular 120:5	108:4 119:20
284:3 288:1	26:12 27:14	265:22 266:3	grapple 303:5	121:14 155:1
296:11 297:5,9	28:17,19 29:1	267:10 268:9	grappled 109:5	173:8 197:10

198:5 204:12 212:3,7 214:3 215:18 251:22 272:10 296:1 307:9 guidance 142:8 guide 173:9 244:4 guidelines 172:6 172:7 238:11 310:3 guilt 241:15 guilty 172:8 gun 78:6 guys 51:10 141:9 146:10 148:18 178:8 178:15 179:17 202:19 212:9 228:5 242:1 264:16,17 283:2	happened 31:7 36:2 89:10 118:6 300:16 happening 60:17 104:1 186:8 267:21 271:2 298:7 happens 53:5,9 74:1 235:14 happy 87:19 229:21 harassing 231:11 hard 106:16 158:6,6,7 171:15 187:2 harder 129:2 189:22 190:12 190:13 206:16 harm 14:6 207:17 harmful 188:18 309:8 harms 32:3 197:8 harvard 210:9 hasnt 75:6 89:10 148:9 267:17 270:6 301:15 hats 126:3 havent 81:7 106:22 147:8 177:7 205:3 228:11 241:10 261:7 276:17 286:6 309:14 310:8 314:22 hayden 144:6 haystack 11:13 11:14 55:16 59:5 150:5 152:8,8,10 haystacks 58:3 58:4	head 16:1,16 124:16 141:4 182:5,8 301:8 header 136:17 143:21 healthy 133:4 hear 30:6 34:17 34:20 37:1 196:16 201:11 259:14 303:20 heard 63:19 101:10 119:12 129:14,15 173:4 229:10 259:11,13 265:8 hearing 65:13 93:11 267:22 hearings 66:21 128:5 139:17 hears 35:10 heart 222:21 269:19 heighten 307:13 held 1:15 4:3 24:21 30:20 75:13 76:13 99:2 137:17 152:20 help 106:12 132:15 196:2,8 196:9 222:8 228:2 244:4 247:3 248:7 270:21 307:12 315:15 helped 80:7 121:10 234:17 helpful 169:22 183:6 189:13 201:10 202:20 203:22 218:2 helping 220:21 222:12 317:6	helps 292:15 hendricks 313:8 heres 168:8 208:19 herring 251:6 hes 52:18 152:3 152:4 205:15 hey 143:13 194:4 hi 235:12 315:10 hidden 245:18 hide 189:9,22 245:14 high 192:1 234:15 308:2 higher 212:4 highlight 148:21 highly 111:16 140:9 184:17 hijackers 243:2 243:3,16 hill 40:12 52:5 125:22 hindered 88:14 116:20 hint 84:21 hired 97:11 historical 18:18 38:13 294:17 historically 143:5 194:1 history 31:10 32:4 42:22 49:9,11 84:21 84:22 108:5 122:7 231:6 295:4 297:1 hit 108:19 278:15 hits 194:3 hmm 34:21 249:20 hold 90:16 155:9,14	172:10,17 holder 88:13 holding 167:9 225:17 holes 245:14 homeland 2:18 16:15 135:3 211:4 homes 76:5,9,10 homework 117:21 119:11 121:14 204:16 hon 2:15 hone 299:12 honestly 107:6 159:19 298:22 302:6 honored 70:12 hood 148:3 hook 202:18 hope 7:4 23:15 28:12 68:21 139:20 140:1 200:7 210:1 247:18 305:9 314:13 hopefully 118:22 148:19 226:14 hoping 195:22 235:2 275:4,9 hospitals 174:6 206:8,9 hostile 13:9 hosting 317:15 hotel 1:16 hour 123:12 209:12 hours 40:11 house 2:18 105:2 125:5 housed 70:1 71:7,8 houses 42:18
H				
hackers 283:3 half 79:18 304:9 hamilton 315:5 hand 166:7 196:13 319:12 handled 8:12 92:3 handles 163:21 handling 41:9 190:11 hands 67:7 73:17 77:21 294:22 hanging 141:3 happen 52:16 65:17 74:2 94:10 110:4 155:9 163:2 271:12 276:10 308:17				

285:11	identify 8:3 9:7	illegal 166:6	283:6 310:15	72:13 99:1,10
huge 108:19	11:2 145:11	236:9	immediately	101:20 105:4
236:5 265:2	197:7 222:12	illustrated 49:8	206:4	109:13 110:16
297:1,2 314:10	242:5 243:1	im 11:19 14:22	immense 27:8	120:14 124:3
hulu 164:9	258:4 264:16	16:22 23:14	immersion	132:7 134:5
human 290:3	292:15 293:17	38:1 46:18,20	315:17 316:16	139:9 149:13
299:22 300:8,9	313:1,4	53:9 54:21	imminent 14:5	151:4,5 153:1
humans 262:7	identifying 41:1	58:13 68:5,14	impact 75:21	204:5 218:13
hundred 121:17	100:19 188:11	78:10,15 80:17	122:18,19	220:20 221:21
hypothetical	242:14 311:13	87:16 90:17	204:1 216:22	224:13 227:15
58:7 243:19	identities 187:12	91:18,20,22	268:3 292:15	237:12 239:7
	305:18,20	95:13 97:21	309:11	240:21 242:6
I	identity 9:18	98:2 101:12	impeding 14:12	242:13 243:18
icon 165:5	140:8 166:9	102:4 108:4	231:10	244:20 245:13
id 23:10 37:15	167:1 169:11	126:4,6,16	imperative	245:20,21
37:18 38:2,17	305:17 306:22	130:22 131:3	310:16	246:12,22
51:21 53:19	ignore 30:10	141:6,10 144:4	imperfect 162:3	257:3 258:8
55:19 63:16	ignores 163:7	156:5 158:18	impetus 296:9	260:3 263:14
64:21 65:22	ignoring 174:18	163:9 169:8,19	implanted 143:7	263:22 268:6
81:17 104:8	ii 3:1	171:14 173:17	implement	270:15,21
115:10 122:22	iii 3:12 46:15	173:19 177:1	173:17 198:21	271:17 273:14
136:3 141:11	53:7,10 92:4	180:22 183:9	implementation	273:15,18
142:18 191:3	100:14 101:4,6	184:5 192:22	4:18 42:20	290:22 291:21
229:21 240:17	102:17 104:20	195:11 198:5	implemented	317:20
241:1 242:8	105:19 116:22	199:3 211:21	26:12 118:9	importantly
270:5 315:13	175:13 176:1	212:13 215:6,8	145:22 214:21	54:7 103:4
idea 31:20 34:2	201:3 217:11	216:20 235:2	231:15	311:4
60:9 97:7	272:10,12	235:12,12	implementing	impose 116:10
104:8,9 105:10	277:17 308:8	238:15 246:15	178:12 215:1	116:12 118:14
106:5 120:8,17	308:12,13,20	250:21 251:20	215:14	imposed 40:1
240:16 246:7	ill 15:9 68:22	251:20 258:20	implicates 111:3	78:21 118:10
271:19,20,21	73:18 78:11	263:6 264:19	implications	131:15 282:20
ideas 141:14	79:17 86:22	285:21 289:17	15:4 52:11	imposes 279:6
247:13	87:1 92:13	293:16 294:7	98:8 99:22	imposing 39:9
identical 221:15	117:16 119:18	297:12 298:10	147:14 315:12	impossible
identifiable	120:13 123:20	298:20 302:9	import 274:12	159:13
168:3 284:1	133:6 138:21	302:11 303:18	importance 14:4	impressed 33:13
identification	141:9 160:17	303:20 304:12	49:8 80:3	impression
13:7	164:2 166:13	305:4 309:17	292:13 293:8	195:3 197:17
identified	169:19 174:4	310:18,19	important 5:5	improper
269:11 292:5	209:19 215:22	311:3	21:5 29:12	222:17
313:2	226:16 229:12	imagine 74:13	37:16 42:7	improperly
identifiers 11:10	286:1 307:19	93:13 139:1	46:4 48:12	145:22
145:7,20	307:22	205:16 253:16	49:13,16 54:9	improve 121:12

182:9 216:19 220:21 254:19 improvements 121:2 improving 192:8 inability 203:4 inaccurate 32:7 inadvertent 111:16,20 148:5 233:14 inadvertently 145:16 inappropriate 120:3 inattentive 209:1 inbound 192:18 incentive 172:5 282:1 incentives 257:14 incident 61:19 incidental 52:19 53:15 111:16 111:20 229:14 233:14 275:7 275:13 276:7,9 277:11 286:22 287:3,8,17 288:5 292:11 292:19 296:7 299:13,14 304:10,18 307:11 incidentally 233:16 306:19 include 47:17 166:21 174:21 included 226:20 includes 17:12 18:17 83:21 including 14:10 40:10 49:20	77:13 88:1 121:10 187:16 224:12 225:17 225:18 230:3 244:5 297:3 incomplete 32:6 incorporate 141:12 incorporated 57:21 increase 29:8 198:20 265:15 increases 29:1 increasingly 40:5 207:1 incredibly 263:14 incumbent 119:19,21 independent 3:7 4:9 105:22 124:20 178:7 178:17 180:13 indepth 178:5 index 129:4 187:18 indiana 262:1 indicate 23:20 26:22 116:8 206:2 indicates 14:5 indicating 242:21 indication 60:20 165:14,16 254:4 indicators 161:11 indices 128:14 128:19 indicted 112:10 indictment 65:9 indifferent 27:16 122:5	indiscriminate 26:13 individual 18:4 21:1 35:14 41:6 45:3,5,6,8 45:16,18 47:1 56:7 59:6 87:14 140:14 161:3,4,6 164:15 167:2,3 178:15,16 191:18 199:16 241:18 242:5 264:22 265:16 268:7 269:8 274:2 277:2 311:21 individualized 19:5 21:7 42:2 42:5 94:19 100:16 108:17 110:9 231:20 233:3,10 234:2 241:11,16 259:4,8,19 262:5 263:2 270:13 271:7 272:1 276:22 281:4 288:3 301:21 302:12 302:20 304:17 individuals 13:11 24:22 25:7 48:10 160:6,6 179:10 187:16 188:17 189:7 269:19 274:3 311:13 industries 56:16 ineffective 164:12 166:10 inevitably 6:1 107:18 infer 142:16	147:9 164:19 184:1 185:7,16 192:2 inference 184:9 inferences 185:20 189:10 192:10 influence 64:10 influenced 30:4 inform 260:14 information 3:5 5:22 6:3,6,11 7:13,21 8:10 8:12 9:5,21,22 10:5,8,16 11:21 12:7,12 12:21 13:16,17 14:1,3,10 17:11,17,18 19:2 21:21 22:1 26:10 27:8,11,15,18 32:7 41:10 49:19 50:11,17 50:19 53:22 54:1 56:22 62:16 70:7 71:13 72:17,18 73:2,6,8,11,14 74:19 75:8,14 75:16 77:5 83:5,9,15 95:18 96:13,18 97:18 102:11 106:8,10 108:1 112:2,3,4 114:18 118:1 124:17 135:18 136:9,18,21 137:9 138:2 139:22 140:21 140:22 144:19 144:21 145:8,9 145:12,17	148:2 150:8,17 150:18 153:4,5 154:2,9,12,16 155:10 157:2,2 157:12,18 159:2,5 165:11 168:7 170:21 171:2 172:2,8 173:7 175:16 176:9,12,13,17 178:3 182:11 185:12,21 186:4,6 191:8 191:9,11,17,19 192:9 193:2,3 202:5,7 204:22 207:1 208:9 211:12 218:21 219:8 222:20 226:8 227:10 227:12,17 229:22 230:6 231:19 232:2,7 233:4,5,8,15 233:17,22 235:3 237:21 238:5 239:12 240:9 242:1,5 246:11 249:9 253:9 255:16 256:10 257:6 258:12,17 260:7,10 263:21 266:13 275:2 276:18 278:4 279:15 279:21 280:16 281:22,22 284:7,9,15,17 284:19 285:2,8 285:16 287:13 287:15 288:16 289:6,7,14,19 289:20 290:5,6
--	--	--	---	---

297:17 299:10	inquiry 21:14	14:4,7 16:11	interact 173:13	124:18
300:8 304:19	insecurity 309:9	19:22 29:3	interaction	internet 23:21
306:6 307:11	inside 18:21	35:17 36:18	299:22 300:9,9	25:15 31:18
308:10,14	41:22 49:20	39:12 42:18	interactions	38:8,14 60:13
310:11 313:16	75:8 109:16	46:6,11,17	146:3	61:13 125:2
314:16,16	114:8 116:5	47:16,18 48:7	intercepted	127:13 141:15
informative	170:6 298:4	67:10 72:21	276:21	141:22 143:7
210:2 252:17	301:3	74:15,20 93:21	intercepting	144:11,16
informed 30:13	insider 132:9	94:11 95:11	229:8	145:10 146:8
32:7 182:22	208:8	106:10 110:19	interceptions	146:12 160:21
245:7,9,11	insight 14:9	112:3,4 113:11	230:5	161:17 162:20
256:16	insist 235:3	128:20 129:6	interest 18:22	165:9 168:2
informing	inspector	133:13 152:6	62:15 72:16	171:8 172:1,15
225:16	305:12 306:7	168:20 171:1	88:19 133:8	290:10
infrastructure	inspectors 19:21	171:11 177:13	136:14 137:16	interpret 223:11
144:8 208:13	247:1	177:14 180:2,7	146:2,4,5,6	225:6 297:10
infrastructures	installation	181:1 190:7	153:11 187:7,8	interpretation
147:18	26:18	210:14 221:7	193:1 223:10	65:3 86:17
infringed 25:4	instance 96:2	222:14 229:3,6	313:4	137:12 270:17
infringement	306:14	231:8,18	interested 54:22	interpretations
293:14,15	instances 232:15	232:12 237:21	55:20 111:22	255:13
ingest 147:19	institution 91:4	238:17 241:8	136:1 319:11	interpreted 7:15
ingredients	207:20,21	248:13 257:15	interesting	81:1 233:2
87:11	institutional	266:13 289:6,7	130:7,13 175:9	255:4,12
inherent 67:22	37:9 90:19	289:19,22	240:21 315:16	intersection
68:3 144:16	91:14 257:13	292:14 293:8	interests 88:5	124:14
164:22	265:20,21	295:19 299:9	110:6 135:16	intertwining
inherently 81:22	institutions	305:16 307:5	168:21 211:15	249:3,5
142:4 164:18	196:6	308:3 314:9	261:4 304:5,6	interval 192:1
172:15	instructive	intend 63:20	312:15 317:9	interview 144:6
inhouse 315:7	24:20	intended 39:22	interject 267:12	intricacies 52:6
initial 76:22	insufficient	95:2 113:18	internal 87:21	intriguing 106:6
87:7 195:12	112:22 113:1	115:13 240:13	152:17 195:5	intrinsic 199:20
243:13	insurance	264:22 268:22	200:7,8 206:4	introduce 4:5
initially 64:11	183:20	291:14	246:22 247:2	15:9 209:20
101:8 291:2	integrated 291:9	intensive 150:8	internally 93:9	introduced 36:5
307:8	291:15	180:10	international	168:19
initiative 222:4	integrity 34:2	intent 41:20	37:2,8 47:11	introduction
inject 97:7	intel 178:8	79:1 117:8	48:20 108:8,15	168:22
271:18	intelligence 1:8	122:14	259:9 279:17	introductions
injury 264:2	2:16 3:10,14	intention 313:15	288:4 289:22	123:21
innocent 160:6	8:5,22 9:3,20	intentionally	290:3,9 297:13	intrusions
172:9 231:12	11:21 12:2,11	13:3,4	302:1	207:16
input 11:3	12:12,16 13:8	intentions 8:9	internationally	intrusive 66:22

67:6,11 69:5,9 76:21 77:1 194:2 311:12 intrusiveness 69:8 311:15 invade 110:7 293:2 invading 24:17 invasions 139:21 inventions 140:10 investigation 20:10 21:2 26:8,19 55:7 57:19 82:15 122:11,15,18 159:6 175:17 176:11 199:17 208:5 234:8 239:1,3 242:20 262:15,18 279:16 investigations 11:15 20:12,16 176:2 178:3 182:18 187:13 221:8 246:5 263:22 283:9 investigative 56:15 79:4 80:13 105:8 187:14 investigators 243:1 investigatory 70:7 invisible 131:11 invitation 22:20 211:19 invite 211:17 286:21 inviting 28:4,8 37:16	invoking 230:21 involve 46:14 94:8 268:7 292:17,22 302:3 involved 9:19 16:5 33:16 45:4 56:19 88:6 214:6 215:10 216:6,8 231:21 269:13 involvement 93:19,22 103:1 109:18 238:9 involves 11:20 273:16 involving 45:15 108:1 259:9,20 264:1 292:20 ip 143:15,21 145:10 161:15 161:16 162:9 164:6,12 170:20 178:1 181:16 283:15 ipbased 164:12 irrelevant 112:18 113:5 isnt 24:15 27:16 59:14 60:3 67:15 130:8 171:21 178:11 188:3 208:5 283:1,3 isomorphic 167:4 168:4 isp 164:5 isps 279:1 280:8 issue 21:11 25:14 35:8 40:8 50:8,20 78:11 102:1 107:22 128:9 129:8 134:2	143:12 175:6 205:22 214:14 215:5 259:16 275:13,20 293:5 309:7 314:12 issued 10:2,11 65:8,15 102:2 133:12 221:17 240:8,11 251:7 308:8 issues 5:16 6:13 7:8 15:8 23:1 32:5,11 37:17 44:1 50:6 75:18,19,20 87:14 90:20 93:9 106:7 123:18 124:3 124:13,13,19 124:21 125:2 173:5,15 193:11 209:19 212:3 213:5 215:21 216:10 221:1,6,11,19 221:22 235:16 269:10 275:6 314:5 317:8 issuing 228:16 item 82:9 items 56:22 82:9 82:16 182:6 itll 283:12 ive 20:14 32:10 64:8 65:15 126:12 129:15 132:3,16,18 133:1 137:22 141:7 187:10 192:1 194:11 248:9 254:15 303:13 307:3 308:12	J jack 257:12 jaffer 2:13 16:4 22:20 47:3 58:1 59:9 72:11 84:5 97:16 111:1 jameel 2:13 16:4 22:19 31:1 44:11,12 47:2 49:12 51:5 75:15 76:21 78:13,15 83:17 122:22 jameels 51:22 james 2:6,15 3:14 16:10 janosek 5:8 15:12 123:8 317:6 january 252:10 252:12 jerome 139:13 jim 4:6 50:22 87:4,12 88:1 117:15 119:7 123:3,19,20 126:2 156:3 187:1 192:6 210:8 211:16 247:10 251:3 256:22 285:18 301:7 jims 68:8 196:18 268:16 273:10 job 178:9 197:21 john 85:4 167:9 167:10 230:22 joined 210:5 joining 209:22 jones 24:20 26:2 26:4,7 45:1	51:5 66:7 69:2 262:1 journal 102:13 125:1 judge 16:11 22:9 33:1 34:16,17 35:6 35:6 37:13 44:9 45:22 62:10 69:4 86:12 92:18 93:1,5 94:15 99:7 101:9,19 101:22 104:8 104:14,19 119:14 121:17 193:11,15 194:4,13 196:4 196:9,10 197:2 198:20 200:18 201:5,13 228:17 229:19 240:8 249:15 251:16 259:14 260:22 269:21 270:8 271:8 299:11 300:13 judgement 111:6 170:8 judges 17:5,8 34:4,15 35:19 36:13,13 93:8 99:16 101:6 102:2 104:18 105:14,14,19 105:20 106:9 119:3 179:6 193:11,16 197:1,12,15,15 197:16 198:6 240:11 248:21 251:16 267:7 269:22 judging 35:1
--	---	--	--	--

judgment 199:17 244:4	K	304:14	62:5 68:1,3	155:7 157:19
judgments 101:1	kate 2:14 16:8	kick 123:21	101:6 128:16	158:21 160:4,5
judicial 34:14	28:7 45:22	kicked 148:16	128:19 129:5	160:9 162:13
39:3 87:8,8	49:6 53:20	272:7	130:4 145:10	166:4 167:19
92:14,18 99:3	67:19 88:22	kidding 91:2	153:15,20	168:4 173:18
119:2 197:13	104:5 106:17	killings 253:7	234:3 267:20	173:18 174:8
201:7 218:13	107:14 115:11	kind 23:3 37:9	283:9 286:11	175:7,14,19
218:18 246:18	116:1 117:2	46:14 53:16	317:21	176:5 177:16
249:18 250:8	118:4	55:15 59:21	knew 80:8	178:1,5 179:9
judiciary 19:22	kates 64:22	60:4 66:12	197:17 227:6	179:18 183:17
97:10,11 245:3	keep 6:6,19	70:19 71:2,12	298:5,6	183:22 187:9
245:4	54:17 99:10	73:5 75:3	knit 51:11	188:14 189:2
july 1:10	104:12,14	76:19 80:16	know 30:1,6	190:19 191:22
junctions 143:8	105:5 116:9	87:18 88:3	31:16,18 32:16	192:2,17 193:8
juries 21:15	118:1 144:7	98:3 102:17	33:22 47:22	195:10,13
57:6	181:9 279:2	103:7 116:13	48:2 53:20	196:12 197:4,6
jurisdiction	281:19 282:3,4	141:7 142:6,20	58:2,12 59:20	197:15 198:7
91:21 99:20,21	284:7,16,19	142:21 144:13	60:15 63:4,4,9	200:15 201:10
100:1,8 101:15	286:5 294:5	144:14,17,19	63:18,20 64:1	202:6 203:16
jurisprudence	310:17	145:1,18	70:8 73:10	204:5,16 205:5
37:5	keeping 69:18	147:12 148:9	74:9 75:5 76:3	205:11 206:9
jury 21:17 57:11	106:4 190:5	149:3 150:8	78:13 84:9,11	206:19 207:3
58:7 65:1,7,8	233:21	151:10,17	85:8,13,18	212:13 214:10
65:15,20 81:16	keeps 77:22	158:22 166:1,2	88:6,18 90:15	215:2,17
84:16,18	103:19	169:22 171:12	90:22 91:6,16	216:20 225:4
justice 3:18 16:2	ken 16:13 37:13	177:13,16	92:5 95:15	226:11 229:13
16:17 25:6	37:21 46:5	178:4,5 179:15	96:5 99:6,8,14	240:12 242:15
33:14 99:14	49:8 51:12,20	191:7,9 192:8	101:18 103:17	242:17 247:16
210:8 211:3	86:22 104:5	194:2,4,5	105:15,20	252:1,5 255:3
222:5 231:11	108:6 117:3	195:10,19	106:18,21	255:11,13
252:11 254:6	120:13,15	200:5 202:8	108:7,20	256:22 257:12
267:4,5,21	150:9 255:1	205:22 206:3	109:13,15	264:13,18
justices 25:2,3	259:2 271:1	206:16 208:9	111:10 114:2,6	267:9,10
66:8 210:19	kennedy 139:15	227:21 231:16	114:7 115:12	268:14 269:5
justification	kenneth 2:17	231:21 232:2	116:18 117:14	271:11 272:9
7:22 275:21	kept 13:21	233:21 250:7	117:15 121:4	272:20 273:15
285:17 313:21	19:11 135:20	257:4 268:18	127:6 128:9	273:21 274:7
justified 147:10	282:1 306:20	269:11 270:19	129:13 130:16	278:1 279:4,18
justify 225:8	306:22	274:12 285:2	132:2,16 133:9	280:1,3 281:7
justifying	key 62:2 135:19	306:5 308:9,16	136:14,22	283:5,10
229:11	136:2 143:7,8	309:20 315:15	142:5 145:5,20	284:13 285:12
	147:22 168:2	315:21 316:2	146:1,9,19	288:8,14 292:9
	175:3 177:1	317:20	147:4,6 148:15	292:10,12
		kinds 61:10,14	151:13 155:3,5	293:6,13

294:13 295:11	47:10 77:3	161:1 163:6,7	league 161:19	20:20 29:15
297:17 302:2	127:12,15	166:7 168:15	leak 13:20 104:4	63:13 89:13
302:19 303:4	128:7,14 130:9	169:4 173:11	205:17 206:10	93:15 97:22
307:2 308:15	153:11 155:6,7	173:12,13	206:11 255:10	98:7 102:14,15
309:1,10,13,16	157:12,18,19	176:1 177:9	255:12	103:1,12
309:17,20	157:20 162:19	179:20 181:20	leaked 6:2 10:3	106:20 129:10
310:3,5,10,20	165:9 187:15	188:14 198:7	81:5 82:4	130:19 131:2
316:6	187:21 188:1	210:9,9 211:2	237:10 241:3	133:11 134:2
knowing 116:2	188:16 190:18	216:15 224:11	263:8	135:19 136:5
248:22 250:19	191:1 192:7	224:21 225:7	leaking 205:15	139:11 140:11
knowledge 12:9	196:14 205:3	225:12 228:8	leaks 8:14 31:13	141:4 142:10
43:15 197:19	207:20 222:1	231:7,17	51:15 103:16	156:12,16,17
197:19 288:17	229:8 236:19	232:11,20	205:13 226:9	156:20 157:11
319:8	236:19 268:6	242:10 243:22	leaping 194:17	175:6 177:2
knowledgeable	294:19 302:7	252:3,4 255:1	learn 25:17	194:20 195:16
196:1	largely 233:2	255:5,18,21	129:19 186:18	195:17 207:7
known 4:8 13:5	294:10	271:14 283:7	205:2 243:7	219:15 221:6
30:19 82:18	larger 48:6	286:14 298:12	261:14 293:2	221:19,22
117:7 162:12	112:12 149:5	298:13 307:2	293:14	224:15 245:1
170:18,19	149:15,16	308:6	learned 31:12	245:12 249:6
190:7 206:10	153:6 178:21	lawful 22:16	34:15 79:15	255:13,21
230:17,18	203:4 221:3	26:17 79:3	80:3 165:2	260:15 265:5
235:9 242:14	268:10 301:6,8	112:19 134:9	233:1,12 318:2	267:8 269:10
243:3 258:8	largest 164:5	273:3	learning 129:11	272:14 276:2
275:22 311:10	300:18,19	lawfully 300:18	129:21 130:8	279:13 280:18
knows 28:18,19	latch 202:18	laws 4:19 48:8	193:8,10 239:5	282:12 314:17
47:20 81:21	late 36:3	136:15 168:14	learns 171:9	legality 15:3
115:6 132:3	latitude 43:13	187:7 188:14	leave 44:14 72:4	38:7 59:3
170:21 189:15	law 3:20 12:13	217:5,18	78:11 230:14	230:15
262:10	12:19 13:2	231:16 255:3	273:12	legislate 138:7
<hr/> L <hr/>	15:22 29:19	lawyer 96:8	leaving 39:11	legislation 43:1
I 305:11	30:11,18 31:16	126:17 132:15	87:20	78:18,20 79:1
lab 3:10 125:4	31:20 34:15	lawyers 91:10	lecturer 210:9	80:5 95:7
labeled 32:15	36:15 46:1	214:9 241:9	led 24:5 46:12	248:18 253:1
labs 124:12	61:16 76:16	layer 96:4	94:2 109:2	265:4
lack 101:11	90:3,13 102:4	lead 160:3	305:11	legislative 43:20
142:11 147:20	102:6,19 106:3	leaders 20:3	leery 180:22	80:5 84:20,22
148:8 150:15	127:21 128:10	99:2	left 68:5 210:7	122:7 140:11
lacks 144:11	130:14 132:14	leading 8:11	210:11 278:11	151:21 157:14
160:21	134:7,8 136:12	124:5,12	298:5,6	legitimate 87:13
language 59:15	136:12 138:6	243:15	legal 2:10,11	127:8 266:11
81:8 82:3,5	142:4 143:18	leads 35:21 62:5	3:16 5:8,15	287:12 304:6
large 10:13	149:9 150:3,3	182:22	6:13 7:21	lend 186:5
	154:15,17	leadup 116:11	14:17 16:2,4	length 9:13

54:16	lifetime 31:7	264:3	local 166:22	164:20 174:12
lengthier 223:20	light 65:5,16	link 20:13 167:7	located 12:15	186:19 233:18
lesson 179:4	82:2 162:12	168:1 185:11	13:13 42:10	237:14 241:1
letter 176:17	231:14 276:13	242:16,22	50:2 113:19	243:4 261:19
297:22 298:11	likelihood 156:8	linked 228:21	166:18 276:4,5	289:4 292:19
letters 232:14	187:18 237:5	linking 137:6	locating 166:17	304:22 309:6
level 7:11 162:5	301:7,8	187:12	location 9:21	311:14 315:1
162:6 185:19	limit 9:6 31:4	list 18:13 169:15	24:22 26:1,7	318:3
185:20 191:19	41:9 60:2	170:10 217:13	26:10 66:11	looked 122:2
212:4 231:20	85:11 101:20	listen 17:19	164:15 169:12	133:21 148:2
232:1,10,16	144:21 156:18	146:10	196:20	165:20 166:3
237:8 256:14	162:13 165:20	listened 105:3	lock 165:5	174:6 185:6
271:13,14	219:19 290:5	175:7	log 315:18	254:6 259:7
300:5 308:2	299:7 312:16	litigate 266:2	logged 209:4	286:6 311:10
levels 42:11	limitation 156:9	litigating 55:22	logging 208:21	looking 49:9
43:17 191:10	limitations 10:7	63:3	logic 288:7	77:11,13,15
192:5 205:9	22:13 82:3	litigation 56:18	logically 142:16	83:15 102:18
286:16	99:11,17 142:6	56:19,20 57:1	logs 175:3	118:5 121:8
levers 170:19	153:10,10	82:14 253:8	178:13 203:15	132:5 165:18
liberties 1:3 4:4	157:9 158:4,5	265:11	203:16,16,17	170:2 172:3
4:16 22:18	158:8 159:9	litt 93:10 150:4	203:18 206:20	180:11 185:16
23:8 29:6	160:1,10,12	little 54:14,15	207:7	187:20 196:18
32:13 119:19	190:20 296:6	66:1,6 86:7	long 10:10 66:13	218:15 219:6
119:21 121:7	309:22	108:5 115:12	69:15 107:4	227:5 238:6
173:3,5 213:10	limited 11:4	120:18 121:4	124:15 125:7	247:11,12,13
216:22 224:8	17:21 61:2	123:1 129:2	127:20 167:22	257:6 262:12
225:14 227:5	110:17 146:22	148:22 155:17	176:7 235:17	262:19,22
230:17 242:10	200:22 224:19	171:14 180:22	249:4 276:1,17	270:12,16
244:2,18	238:14,19	189:12 194:19	287:16 308:12	291:8,9 292:22
266:14 269:13	277:11 289:15	202:17 211:6	longer 103:14	311:7
278:15 293:6	limiting 256:9	212:11 217:14	128:8 281:19	looks 263:16
294:11,14	limits 67:22	261:14 275:10	303:17	308:20
309:9,11 311:9	68:3 85:7	284:8 309:12	longterm 24:21	loophole 297:16
317:10	100:7 131:14	litts 152:3,4	25:21 26:1	loopholes
liberty 4:17 33:4	158:1,2,15	live 152:1	look 28:5 44:1	233:21
210:19 226:22	229:17 289:4	227:21 244:6	53:7 54:4	loosened 296:12
230:18,21	310:2	lives 27:18	74:10 80:22	lose 187:11
235:10 270:8	line 41:19 59:4,7	29:22 231:3,13	84:20 105:14	317:13
299:4	59:10 120:2	livingston 1:22	106:15 114:15	loss 292:2
lichtblau 90:1	139:3 171:15	319:3,16	126:17,18	lost 230:21
lichtblaus 90:3	204:18 230:20	liza 210:18	127:12 131:1,5	lot 56:18 65:15
lies 191:14	280:1 283:16	285:3	132:8 147:4,5	68:14,20 71:3
life 29:11 49:22	lines 180:1	loan 188:20	149:19 150:14	82:11 98:16
66:14 79:18	183:5 260:14	loathe 222:15,16	153:14 161:18	106:7 131:11

148:5,6 151:7 158:7 163:3,12 163:19 181:11 182:4 186:8,9 187:11 190:21 194:14 201:21 208:2 212:8,8 212:9,10 215:16 226:19 232:6 241:8 246:5 247:16 248:1,14 249:10,19 250:6 258:22 262:10 265:8 267:2 272:4 273:19 276:19 280:9 281:19 304:12 307:11 310:7 315:11 lots 57:20 94:2 95:18 181:4 286:15 love 63:9 low 156:16 232:21 263:13 283:12 lower 45:17 47:8 lowered 232:16 lunch 6:16 123:12 lynne 1:22 319:3 319:16	272:17 magnitude 58:20 89:15 mail 7:10 maintain 71:18 83:14 128:7 286:5 317:21 maintained 69:6 maintaining 43:3 71:14 79:5 278:16 maintains 57:2 145:6 maintianing 280:8 major 116:22 161:19 218:21 253:18 271:5 majority 11:7 66:8 89:2 185:13 231:2 makers 147:5 147:16 179:6 198:15 making 5:9 9:11 23:21 28:13 80:4 96:19 100:17,22 101:1 151:9 170:1 184:13 224:19 225:17 226:1 271:21 276:22 302:6 malaysia 243:4 man 53:12 manager 201:14 managing 188:16 mandamus 133:10 mandate 248:18 252:2 mandates 19:20 mandating	265:2 manifests 57:13 58:8 manner 22:16 291:15 manning 207:14 208:20,20 manpower 39:19 mantra 121:20 map 28:3 mapping 167:5 168:4 marc 3:5 124:15 132:10 136:1 142:13 156:2 158:13 164:3 166:12,13 169:3 181:22 182:1 183:10 185:17 189:12 200:16 208:7 208:15 marcs 140:18 184:21 margins 216:19 marshall 315:11 martin 2:14 16:8 28:8 49:7 60:5 63:4 75:4 78:8 86:10 101:18 113:13 117:3 maryland 26:18 45:14 137:2 319:4 mason 3:20 211:3 mass 14:13 44:18 246:1 massive 24:2 29:21 31:14,17 74:18 75:17 163:22 198:1	233:13 302:17 302:21 master 233:17 matching 137:7 material 228:19 254:9 304:13 materialize 280:10 materials 57:8 82:13 matter 30:15 75:5 76:15 221:11 251:2 268:20 matters 30:16 222:21 292:8 318:3 maximum 225:7 245:6 mayflower 1:15 mean 48:15 58:9 62:22 68:1 71:2 88:10 95:17 96:2,3 113:4 130:20 144:9,9 147:9 156:10 159:18 174:22 178:22 181:8 182:15 183:17 185:18 186:16 194:20 195:5 197:20 212:3,22 213:10,22 215:15 219:12 240:12 250:21 251:22 253:22 256:18 257:22 266:21 272:9 281:15 283:13 287:7 293:18 296:1,22 297:9 298:12 302:4 302:16,20	306:13 meaning 21:9 229:15 299:14 304:2,3 meaningful 42:13 54:9 150:13 177:6 201:12 255:20 means 34:8 72:12 73:13 115:7 126:17 130:12,16 161:3,22 208:17 213:4 218:7 233:6 236:18 239:20 253:17 255:18 258:4 306:14 307:4,6 308:14 310:16 311:12 313:14 meant 26:7 30:22 84:13 113:7 measure 177:20 measures 106:2 144:21 mechanism 179:13 mechanisms 131:16 158:20 163:13 175:20 177:19,19 194:16 195:4 195:19 208:1 254:13 274:11 280:19,22 media 6:2 medical 25:14 174:5 medine 2:3 4:2 107:13 113:2 117:2 119:1 123:11,15
--	--	---	--	---

M

m 1:17 318:8
mac 145:9
machine 129:11
129:20 130:8
193:8
macro 185:20
magazine 130:3
magistrate

125:14 172:21 177:9 178:18 179:20 188:4 209:14,18 223:9,13,17 230:10 236:7 250:9 254:16 265:7 269:21 281:14 312:3 312:12 315:8 316:20 medium 141:18 meet 75:9 77:14 108:3 260:5 meeting 4:3 40:12 51:15,19 243:4 318:8 meetings 52:10 meets 260:21 member 33:3,4 146:14 270:8 313:7 315:10 316:16,18 members 2:1 4:6 6:16,18 7:1 14:18,22 20:3 20:5 40:12 42:21 48:6 56:7 63:19,19 64:3,12 74:13 78:4 85:20 95:9,11 97:15 103:21 107:11 125:16 183:7 185:13 193:6 194:8 235:14 240:19 255:2 276:15 294:1 306:8 312:7,14 316:8,22 memories 140:7 memos 93:9 mention 215:20 247:9	mentioned 19:7 32:18 49:12 63:18 104:13 106:17 108:6 115:3,11,17 116:6 122:22 123:6 160:20 182:1 195:20 203:1 204:20 229:19 mentions 309:7 menu 189:14 mere 60:14 290:11 merely 7:16 27:15 243:19 302:13 merged 282:7 merit 311:13 message 136:17 met 41:3 197:7 metadata 8:21 9:9 10:14,19 11:4,12,16 17:1,10 18:17 20:11,18 21:21 22:10 23:18,21 24:10,11,16 25:16,21 27:7 31:15,18 44:16 44:19,21 45:7 45:20 49:20 51:7 60:11,13 61:12,17 66:12 67:21 68:1 71:17 84:3 98:2,9 127:13 128:1 130:22 131:1 133:19 136:8 137:14 140:19 142:14 143:2,9,15 165:11 184:16 184:22 185:2,2	185:16,22 190:8 191:4,6 193:2 196:15 216:12 217:20 228:10 258:10 311:8 312:2 313:20 315:11 315:15,19,22 316:5 method 171:22 methods 36:21 139:9 180:4,5 234:22 235:1 295:6 mic 37:21 236:7 michael 3:16 micro 185:19 microphone 312:9 middle 291:3,16 294:12 midstream 286:20 migrated 108:12 migrations 163:2 mike 210:11 mikes 273:6 military 64:8 252:20 315:4 mill 68:15 million 314:20 millions 26:14 61:6 160:5 196:15 313:11 mind 6:7 56:8 78:1 99:10 104:12,14 105:5 106:4 116:9 144:7 241:21 246:18 286:5 294:18 mindful 143:11 146:22	minds 231:3 mine 105:7 185:4 219:7 minimis 276:10 minimization 13:19 41:8,14 49:3 101:3 108:2 111:8,11 111:13,15 112:1,22 115:4 115:5 121:16 122:2 139:8 172:6 220:7 223:1 233:19 249:21 256:8 263:6,7 287:13 288:2,6 306:12 308:14,20 314:12 minimize 19:15 278:14,15 minimum 288:14 mining 18:1 129:11 130:20 158:22 minority 210:12 minute 45:21 125:10,12 151:15 155:19 209:15 211:10 294:6 minutes 15:10 15:16,19 34:13 44:5 54:17 69:1 155:18 183:18,19 211:9 247:8 254:15 312:10 312:16 misbehavior 199:21 misgivings 274:4	misidentify 196:20 misinterpreted 185:3 misleading 111:17 184:17 191:14 276:13 misled 48:7 52:1 misnomer 12:3 missed 188:13 missing 188:12 314:10 mission 245:21 263:8 missions 4:12 misspoke 113:4 mistake 306:15 mistaken 158:14 misunderstan... 121:18 misunderstands 157:7 misuse 80:14,16 132:9 141:2 148:6 158:11 207:8 279:19 280:4 281:18 misused 79:7 misuses 180:20 mit 3:9 125:4 139:14 149:5 154:7 185:6 315:16 316:5 316:19 mitigate 14:14 model 93:4 97:13 modeling 222:3 models 221:4 moderate 6:16 14:19 moderating 15:2 modern 51:6
--	--	--	---	--

141:16 146:7 190:10 modification 176:21 modified 176:20 mohamed 242:17 264:13 264:13 277:3 moment 15:9 38:17 138:14 138:17 153:18 155:22 156:11 167:3,8 212:4 262:7 304:16 moments 104:13 money 181:4,6 204:13 monitor 165:10 177:14 monitored 37:4 43:17 month 26:11 60:8 150:15 months 40:9 52:4 183:22 219:13 220:14 morning 4:2 14:21 37:14 125:10,15 175:7 229:11 255:1 294:16 306:12 mornings 142:20 194:19 224:10 304:20 mosaic 239:4 mother 184:3 motion 268:10 mouse 245:14 move 169:20 172:19 216:15 236:7 241:16 241:17 254:16 268:4 304:10	moved 117:22 235:21 movements 25:7 28:1 231:11 moving 48:1 119:22 152:13 162:18 223:10 268:21 multiple 43:17 69:12 143:6 multipoint 118:6 murderers 246:1 music 146:10 mustnt 103:5 <hr/> N <hr/> naked 28:20 name 12:5 164:21 200:10 212:16,19 213:21 315:10 316:14 narcotics 182:18 narrow 9:6 74:5 101:12 112:11 235:1 311:11 narrower 26:4 234:22 nathan 3:20 211:2 nation 4:14,20 160:11 177:4 national 2:14,17 12:11 16:9,16 29:5 36:20 43:12 69:18 70:7 72:16,19 93:16 94:7 96:17 105:8 134:13 135:7 135:14 148:17 162:17 186:21	205:14 210:20 232:13 243:18 243:20 244:7 304:7 306:5 308:3 310:16 317:9 nationality 164:19,21 nationally 124:17 nationals 48:14 nations 192:16 naturally 57:19 142:16 nature 205:15 260:15 nctc 152:12 near 58:10 300:4 nearly 149:18 246:15 necessarily 130:14 167:10 190:16,20 205:11 258:4 303:9 311:4 necessary 14:3 28:14 70:21 87:8 92:19 127:21 175:3 177:3 183:2 227:4 235:3 247:21 263:1 270:12 307:4 necessity 70:20 290:4 need 4:15,16 11:14 20:17 23:6 31:22 36:19 39:3,5 42:5 43:2 51:4 51:16 54:18 62:17 70:8 79:14 93:19	96:22 102:16 114:1,20 126:12 127:15 128:16 130:18 140:13 144:17 148:17 152:10 156:8 158:1,9 167:6,7,17 168:17 172:2 174:8 175:6 177:12,15 184:14 186:6 187:6 188:10 198:5,6 199:8 201:11 227:22 229:14 232:7 250:16 253:12 258:10,10 261:14 266:11 273:16 281:9 283:22 285:14 288:6 289:15 292:5 314:16 needed 108:20 168:21 238:7 needle 11:13 150:4 152:7 needs 32:2 34:17 37:6 40:6 50:21 55:11 59:6 69:16 75:9 78:19 90:6 128:20 132:7 203:19 204:7 254:9 275:13 282:19 288:15 neither 27:19 nervous 171:14 net 27:4 network 83:7 164:14 185:6,9 185:14 242:18 243:15	networks 14:9 163:15 never 11:7 61:5 65:16 76:9 86:4 98:19 232:6 236:14 250:3,4 271:12 new 7:15 23:7 36:5 40:17,18 58:18,19 101:9 102:13 103:14 104:16 130:3 138:3,5 139:21 140:10 149:4 164:6 181:4 268:1 270:17 282:20 news 17:22 23:20 nice 202:17 nimble 281:7,8 nodding 301:7 nojeim 3:19 210:21 235:12 235:12 236:8 260:1 272:16 282:17 288:20 299:19 301:10 nom 273:21 nominally 233:12,17 nominees 219:2 nonabusive 159:20 noncontent 183:8,11,15 nondiscrimin... 154:15 nonincrimina... 176:9 nonnational 174:5 nonprivacy 154:17
--	---	---	---	--

nontechnologi... 161:22	167:15 169:22 170:21 178:6,7	objection 32:14 63:14	301:13,14	271:19 273:7
nonu 12:14 42:9	178:12 179:15	objections 62:6	occurs 261:11	273:20 274:21
45:12 52:20	187:4 200:9	objective 39:8	306:4	ombudsperson
94:22 107:17	202:16 205:6	obligation	offered 20:5	240:16 261:2
109:7 110:2	239:17 262:10	134:17	27:6	273:13,17
168:11 288:10	262:11 295:4,6	obligations	offering 121:11	once 10:13
288:13	nsas 19:6	220:4	office 2:11 3:14	36:15 132:1
norm 34:19	nuclear 13:10	obliged 155:20	16:1 79:22	138:1,13
105:12	number 9:11,11	observation	91:15,15 97:10	186:12 227:12
normal 130:10	10:21 18:6,8	119:10,11	officer 5:7,8	229:18 230:22
130:11 249:17	18:14 19:4	193:5 217:7	97:2	277:19 282:2
299:13	45:9 61:3 83:6	observations	officers 18:12	285:5
normally 141:1	83:9 93:4 96:7	248:10 266:10	offices 76:6,9,10	oncology 183:19
northeast	119:14 150:6,7	observed 25:6	official 28:20	183:21
162:22	154:13 176:6	obtain 9:2 12:20	210:9 211:4	ones 171:16
notarial 319:12	178:1 179:9,10	13:6 75:8,16	273:22	226:21 243:19
notary 319:3,17	189:19,19	113:18 117:6	officials 7:18	315:7
note 23:22 32:10	198:3 201:2,3	117:10 245:1	40:10 48:6	ongoing 55:6
190:15 206:19	202:3 215:18	266:12 295:14	114:16 120:21	81:2,22 82:13
301:8	237:13 243:8,9	obtained 12:8	121:10 234:6	84:14,18 85:14
noted 28:17	253:14 259:13	81:15 82:21	236:16	133:16,19
131:21	266:7,10 294:2	287:11	oftentimes	203:13,18
notice 76:14	294:16 305:15	obtaining 12:17	145:13,15	262:14 279:16
notify 98:6	305:17,21	287:12	191:12,21	online 121:21
134:17 176:3	numbers 11:17	obvious 60:3	oh 71:22 171:3	122:1
notion 79:3	17:13,14 18:4	72:12	okay 37:14	oops 170:5,6
102:22 104:14	18:14,15,21	obviously	54:11 65:22	open 51:17 55:1
116:16 168:19	19:16 20:14	116:21 170:21	67:21 87:3	87:4 125:17
196:2 284:22	26:21 33:18	175:2 189:1	89:17 104:5,7	234:8 317:21
307:14	145:9 149:18	207:13 213:21	108:18 117:18	opening 15:10
npr 129:15	196:19 218:3,4	224:9 267:6	147:21 148:10	16:22 56:5
nra 78:4,5	218:5,6 295:20	280:4 286:15	160:18 181:21	87:6 115:3
nsa 18:12 19:12	305:6	occasion 219:13	194:12 201:18	125:10 218:10
23:17,20 27:8	numerous 40:9	220:16 268:18	214:13 217:17	operate 180:21
33:15 36:3	52:13	292:3	247:22 248:5,7	257:20 265:9
44:13 47:10,15	nurse 174:15	occasional 268:8	250:1 266:16	operated 1:6
48:19 49:14,18	nut 217:1	occur 309:22	267:14 287:18	operates 142:17
50:12 73:18	nw 1:16	317:12	298:16 304:9	156:18 244:17
115:19 131:20		occurred 18:16	305:10 312:3	257:20
134:11,20	O	21:17 86:4	312:12	operating
141:20 143:3,7	object 61:22	93:22 128:12	olc 252:1,11	162:19 207:10
144:6,19 145:6	63:15	194:10 205:12	254:2	operation 41:19
157:1 162:10	objected 76:7	occurring 83:4	old 184:3,4	150:11 198:1
			ombudsman	203:18 206:17

operational 41:5 43:2 203:7,13 207:12,15 244:15 245:9 246:6	136:20 137:4 179:2 206:3 249:9 250:20 250:21 274:1	309:21	outlined 31:1 132:19 239:8	50:2,5 52:14 52:16,20,22 115:20 116:2,4 116:15 117:9 117:12 233:11 288:10,13 295:4,6 296:6 297:17 302:4 303:2
operations 308:3	opposite 137:16 241:20	ordering 238:4	output 11:3	oversee 173:1
operators 142:9 142:9	optic 108:12	orders 8:5,6 10:2,11 24:8 35:16,17 46:3 58:20 61:1,3,6 82:12 88:17 89:9 94:19 108:17 110:10 201:2 219:9,10 219:15 240:8 240:10 248:9 255:17 259:4,8 259:13,20 266:2 268:13 271:16 286:11 298:3 302:20	outset 186:19 211:21 212:13 220:4	overseen 19:15 54:6
opinion 31:14 66:9 90:11 93:1 221:17,18 249:15,16 250:3,8 251:8 251:18 252:11 254:2 291:4	option 195:12 312:21 316:4	ordinary 59:16 84:10 105:12 246:4	outside 12:16,20 13:13 39:20 41:7 42:10 45:13 48:14,18 94:22 107:17 108:22 109:8 109:20 110:3 142:1 161:7,12 169:5,13 178:7 195:18 196:6 198:8,12 221:9 221:20 238:2 269:10 297:6 298:7 300:22 301:1	oversight 1:3 4:4,22 19:19 42:13,14 43:18 46:16,17 54:3 54:5,8 79:16 79:17 80:4,8 80:15 87:20 99:9 103:19,21 132:21 133:9 149:2 150:12 152:15,17 175:20 177:7 213:21 214:4 214:10 216:21 240:5,13 246:18,20 247:3 254:20 257:2,3,5,8,14 257:16,22 258:2 263:3 286:16 295:7
opinions 30:7 66:7 79:12 89:3,9 90:9 93:5 100:4 102:14,15 106:22 107:2 118:22 230:4 248:22 250:11 251:6,11 253:20 255:8 260:3	order 6:4 8:22 10:2,3,3,6 11:18 12:20 13:6 15:22 17:3,8,16,22 19:3,19 20:17 21:7 22:10 30:17 35:21 42:2 45:11 55:5 60:4 62:13,14,15 67:9 69:7 75:7 81:5 82:4,17 82:22 83:11,19 86:14 88:11 89:8 103:8 116:21 117:6,9 131:9 133:12 133:14,18 134:2 143:9 156:22 179:8 219:20 228:11 228:16 249:20 250:5 253:21 254:10,13 255:10 259:8 264:9,10 268:10,12,19 269:4,5 275:10 278:20 280:15 288:3 292:6 301:22 302:13	org 136:1	outsources 280:7	oversightlite 257:4
opponent 90:19		organization 18:7 64:11 139:3	outward 258:12 258:19	overview 87:10
opponents 31:3		organizational 132:6 199:5	overall 293:5 308:4	overwhelmed 94:19
opportunities 147:6		organizations 10:22 14:11 152:16	overarching 28:12	ownership 78:6
opportunity 16:21 20:6 28:9,11 43:22 73:18 95:9 133:1 135:8 138:15 186:13 211:20 223:19 230:8,12 260:9 269:15 293:22 312:14		organized 64:14 128:15	overbroad 238:21	
oppose 97:11 265:16 266:1		origin 163:17	overcollected 179:12	P
opposed 87:14		original 41:19 43:4 79:1,1 88:16 138:22 181:13	overcome 160:11	p 146:11,11 318:8
		origins 105:9	overlap 217:8	paces 106:1
		ought 149:22 240:14 261:2 290:11,12	overlapping 86:20	
		outcome 176:7 319:11	overreach 29:2 169:1	
		outer 85:6,11	overriding 72:16	
		outline 226:17	overseas 39:6,12 42:4 49:15	

package 250:3	253:6	167:20	104:10 131:3	239:15 247:2
packages 219:20	papers 93:14	participating	296:20	309:6
page 116:1	313:15	97:4	pass 55:3 86:22	pclobs 7:5 224:6
126:8	papps 146:9	participation	91:18,21 95:8	224:16 225:15
pages 249:9,9	paradigm 105:4	95:13	160:17	pen 26:18,20
paint 282:8	117:1 136:15	particular 10:21	passage 43:21	81:19,21 83:2
panacea 159:9	163:18 186:3	11:17 45:2,3,6	64:6	83:6 86:20
panel 2:9 3:1,12	paradox 36:17	55:12,17 56:22	passed 36:4	239:21 281:1
6:15,17 14:16	parallel 277:15	57:14 58:9	38:16 39:16	penumbral
14:19 15:2,6,7	parallelize	74:22 85:21	40:15 43:10	245:18
15:14,18 44:5	203:17	87:18 92:16	64:11,17 95:7	people 25:19
54:12 58:14	parallels 105:9	95:16 96:10,13	214:19 294:20	26:15 33:15
59:2 78:12	parameters	104:11 127:10	passenger 243:5	34:1 43:20
92:10 97:14	74:15,16 98:21	128:13 136:13	passengers	48:18 50:2,7
107:11 117:14	paranoid 47:13	143:12 163:21	57:13	53:18 57:15
118:20,21	48:3 49:2	181:15 182:12	passes 181:8	60:6,9 64:17
123:7 125:19	part 19:2 48:5	214:6 219:20	passing 55:15	71:16 72:21
151:7,11 175:7	51:19 60:17	241:21 244:5	87:13	76:10 80:8
193:6 194:9,19	72:10 87:4	248:3 251:16	pat 4:6 14:19	84:5 88:5,10
201:7 204:16	89:19,22 91:11	265:8 268:20	15:17 54:11	91:8 103:13
209:16,19,20	92:7,9,11	311:5,6,13,18	patchwork	105:21 116:4
209:22 210:4	97:10 111:8	particularity	217:8	117:10 120:14
211:5 212:16	119:20 127:10	130:17,20	patent 162:10	147:13 150:19
217:15,15	134:5 141:17	240:2	162:14	161:2 174:2,17
224:10 230:13	149:5 224:9	particularized	patricia 2:5 15:1	183:1 186:20
255:1 256:3	238:16 247:1	76:6,7 92:17	patriot 1:7 5:12	188:21 189:7
265:7 285:5	252:21 267:11	109:22 120:11	8:16 133:15	192:18 194:21
303:7 304:20	267:16 268:6	295:21 298:21	291:11	197:22 199:19
306:8 312:5	281:6 287:11	298:22	pattern 48:5	200:1 202:3
panelist 15:15	290:11 294:10	particularly	patterns 192:16	206:10,15
panelists 5:2	302:17	40:3 54:22	192:16	209:8 212:8
6:19 15:17,21	parte 34:7 35:9	109:9 163:18	pay 51:4 70:2	213:11,15
32:18 44:7	88:4,4 92:21	175:11 218:15	149:22 288:20	214:16,16,22
123:5 124:1,4	102:8 104:21	270:20	290:19	215:13 221:20
125:11,12,13	105:10 175:15	parties 57:2	paying 209:3,5	228:5 236:21
173:4 217:13	194:21 270:1	319:10	209:8 282:3	237:7 238:2
240:20 256:20	272:19	partner 15:22	pclob 4:8,21	243:9,11 250:8
264:21 281:15	participant	16:13	5:16 7:19 37:8	251:15 257:11
286:21 294:3	125:7	parts 207:20	91:4,4 124:7	261:12 265:12
317:3	participate 5:3	212:19 253:13	152:16 177:17	269:9 271:10
panels 6:12	16:21 22:21	254:3 297:2	180:15 225:22	271:11 287:20
211:7 226:3	28:5,9 230:12	304:22	235:2,14,16	287:20 289:2
paper 185:5	240:21 274:8	party 56:20	236:5,10	289:14 290:6
252:15,16	participated	62:14 83:6,9	237:12 238:12	290:17 291:20

300:18 301:1,3 302:3 304:14 306:11 314:8 317:16 peoples 75:21 205:18 percent 121:17 141:21 162:3 170:17 197:5 237:4,13 percentage 159:4 176:8 294:19 300:18 300:19 302:7 perfect 120:22 163:12 168:5 209:1 216:17 300:2 perfectly 65:19 128:21 performing 272:5 274:14 period 25:7 26:11,15 27:3 57:14 58:9 61:2 66:13 90:10 248:15 279:3,8 287:17 periodic 19:21 periods 231:6 permanent 12:15 77:20 78:6 97:1 267:8 permissible 275:1 permission 241:14 permit 6:20 13:2 31:21 115:22 138:18 291:8 311:8 permits 12:13 20:8 82:5	permitted 10:18 18:2 78:8 100:14 228:14 persecution 231:4 person 12:14 13:4,4,16 41:21,22 44:5 52:2,20,20,21 104:10 105:1,2 110:2,6 114:4 114:11 115:14 116:14 136:10 144:14 161:8 161:11 163:9 163:21 167:9 167:12 169:9 169:11,12 170:5 171:4 185:8 195:2 196:21 206:21 207:2 208:3 228:20 230:1,6 231:21 239:13 239:14 266:20 267:13 268:1 278:4 288:8,9 288:10,13,13 288:18 305:17 personal 25:14 29:22 66:14 137:9 313:16 personality 127:3 personally 169:21 183:9 244:9 284:1 personnel 241:9 persons 9:19 13:1,13 14:2 25:17 26:10 39:11,20 41:11 42:9 45:12 53:4 62:15,16	66:14 94:22 107:17,19 108:1 109:7 161:2,3 169:5 178:2 198:19 229:9 295:15 300:20 304:11 304:19 305:7 305:18 perspective 2:10 3:13 126:18 130:15 131:2,3 131:6 148:7 173:22 191:3 197:11 202:21 294:17 perspectives 14:18 pertains 228:19 239:12 perverse 172:5 pet 192:3 petition 133:10 134:11 136:6 phantoms 230:21 phase 44:4 phenomenon 64:20 philosophical 292:8 phone 9:21 17:11,13,20 18:4 20:14 22:2 23:18 60:11 127:13 127:15,16,19 128:18,22 129:4 145:9 166:18 189:15 190:3,4 240:9 257:11 283:14 313:11,19 phrase 118:17	129:14 133:18 phrasing 115:12 physical 208:22 piano 141:3,5 pick 46:22 209:15 picked 197:15 picking 83:5 152:2 226:12 301:7,9 picture 182:13 226:10,14,15 241:2 282:9 piece 43:1 131:6 185:1 191:7 299:3 pieces 191:6 242:5 249:7 pizza 53:12,13 place 24:6 25:13 26:5 38:11,20 42:15 48:9,10 49:5 70:10 72:17 74:8 75:11 78:18 79:4 87:17 97:20 98:20 99:2 108:2 111:3 113:17 138:19 141:17 144:9,10,10,11 145:19 152:14 161:4 176:1,7 196:7 206:12 214:9,20 215:13 226:5 227:10 245:10 246:21 255:19 264:14 277:11 280:6 303:12 placebo 159:8 placed 22:13 83:10 places 218:13	plaintiffs 37:2 101:10 plan 61:19 planning 14:11 109:16 plans 14:10 245:8 plausibly 129:7 play 97:19 100:14 120:22 121:11 122:4 220:20 225:22 236:5 237:12 256:5,5 playing 100:12 plays 135:15 please 126:1 135:22 182:7 pledged 219:3 plenty 225:2 plot 116:8 311:5 311:18 plots 8:4 234:18 310:8,15 plus 250:2 pnalists 211:9 pocket 105:22 point 35:13,20 51:12 53:19 64:21,22 72:11 73:3 74:22 78:17 85:8 101:12,12 105:13 106:18 115:11 119:2 133:6 136:3,8 137:14,19 138:13,21 141:5 142:13 142:19 144:5 147:3 156:21 164:16 165:12 165:18,21 171:20 175:4
---	---	---	---	--

177:1 181:13 185:17 187:1,9 194:4 199:11 200:14 201:5 215:17 222:8 228:12 240:6 241:22 251:4 254:10 257:3 258:2 264:14 268:21 271:1 273:6,10 274:21 275:15 275:15,15,20 277:8,21 278:5 300:12 302:5 302:21 pointed 73:4,9 252:18 270:11 points 34:6 44:10 48:12 51:2 63:17 83:1 104:12 106:4 136:2 138:9 140:18 141:1,7,13 142:3 148:21 156:4 162:12 183:3 224:3 242:6 281:4 304:14 poking 316:2 police 27:4 168:15,17 233:7 285:9 policies 4:19 231:16 policy 3:13,15 5:16 6:14 15:4 23:2 36:13,14 124:8,14 125:5 129:10 133:5 140:21 147:5 147:16 148:7 153:6 159:9	173:17 174:19 179:6 181:20 187:3 192:21 197:8,13 198:15 204:1 207:18 209:19 303:7 political 25:10 25:15 29:22 31:2,3,4 99:1 231:11 234:11 pool 197:16 poor 163:5 portion 11:5 252:11,12 portions 221:17 portrait 243:15 pose 6:17 118:20 poses 77:12 129:10 187:19 position 6:9 9:14 47:18 50:19 121:5 205:17 261:3 270:7 possibilities 194:20 possibility 61:15 62:8 85:1,17 161:22 254:12 293:19 possible 5:9 6:20 8:4,8 51:7 59:10 67:18 77:3,4 122:14 127:18 128:12 140:1,2 168:1 188:11 198:6 201:22 203:11 203:15,17 225:20 243:14 245:8 292:2 306:1 308:9	possibly 68:7 104:9 157:3 227:19 310:15 post 237:3 246:20 postcollection 229:20 277:19 299:15 posted 7:4 potential 108:21 109:16 203:6 242:8 243:18 264:8 279:19 281:17 289:20 potentially 21:16 57:4,8 146:5 160:2 211:14 pounded 267:18 power 23:4 28:18,20 228:20 231:22 239:10,13 257:13 289:21 powerful 129:19 184:13 188:3 powers 38:22 225:3 289:10 practical 71:5 106:7,15 158:5 158:8 practicalities 114:14 practice 11:4 134:16 204:15 214:21 295:14 296:14 practices 232:6 256:2 preceded 66:9 precedent 90:14 91:13 308:1 precise 25:9 166:15 208:1,6	precisely 25:18 130:10 preconditions 199:13 predicate 234:8 285:14 predication 263:1 predications 286:9 preexisting 232:20 prefaa 303:14 prefer 263:19 preferred 79:22 prejudices 234:10 premise 296:2,4 296:8 299:20 299:20,20 307:10 premises 296:3 303:9 prepare 93:14 318:3 prepared 207:21 224:14 260:18 296:2 prepares 260:19 preprotect 259:19 303:15 prescribed 42:15 54:4 presence 19:1 present 62:2 196:17 presented 37:11 268:18 presenting 195:17 preserve 312:22 preserved 71:10 preserving 29:7 231:9	president 5:17 24:9 46:7,9 60:18 109:12 124:16 139:13 139:14,15 148:17 214:7 214:20 266:12 318:4 presidents 109:2 110:21 252:13 252:21 press 30:14 103:16 129:14 206:12 241:4 pressing 72:21 pressure 74:13 presumably 31:19 116:16 127:13 205:5 pretty 60:8 86:10 127:3 195:4 271:3 280:1 290:1 prevail 74:21 prevent 8:4 30:17,22 80:16 156:20 158:10 197:9 207:8 245:20 247:3 prevented 234:22 preventing 54:10 prevention 13:9 prevents 117:5 246:3 262:21 previous 192:3 192:3 251:6 previously 16:15 295:2,13 298:18 308:4 primarily 33:8 64:13 236:4 primary 4:12
--	---	---	--	--

127:7 135:4 182:19 229:3 299:9 primitive 26:21 45:15 principally 23:14 principle 67:14 207:10 principles 244:3 244:8,20 246:6 prior 42:17 94:18 108:7 187:21 prism 12:3,4 38:6 43:7 privacy 1:3 3:5 4:3,16 22:17 24:17 25:5 28:17 43:3 48:10 52:11 74:7,9 94:22 110:6 113:1 124:16,18,21 125:2 127:5,7 128:8,11 131:13 132:9 135:16 136:14 137:15 139:2,5 139:18,20,22 140:14 148:16 150:5 153:6,8 164:1 168:14 168:21 173:2,5 180:4 181:2,8 184:10 187:5,6 188:14 192:22 193:1 199:20 200:11 205:18 206:5 207:16 212:22 213:11 216:22 224:8 227:4 236:2 242:9 244:1,17	266:13 278:15 281:21 292:17 293:2,3,6,14 293:15 304:5,6 309:10 310:21 311:9 312:22 313:8 314:2,4 314:6,7 315:12 317:10 private 22:5 49:22 70:1 126:5 128:5 163:15 281:18 282:1,13,17,18 282:21 286:1,4 privately 185:15 privileges 131:22 privy 205:5 pro 200:4 probable 11:18 19:5 59:22 92:17 95:19 100:18 105:16 110:11,13 114:21 199:13 271:7 278:6 279:14 286:9 probably 32:12 33:3 80:2 97:2 101:20 141:10 146:18 162:3 178:16 180:7 180:16 197:21 241:10 266:22 270:11 296:13 problem 40:3 50:18 73:15 78:3,3,4 90:22 102:8 108:19 127:7 132:17 157:5 158:14 162:16 166:1,9 167:4,16 168:4	168:8 173:20 187:3 196:12 206:21 208:8 215:3,4 254:21 276:9 279:19 281:16 296:7,9 302:22 303:6 problematic 101:17 143:17 145:14,16 270:3 284:5 problems 75:2 131:18 133:5 139:2,19 173:10 207:19 212:5 249:2 282:22 292:18 308:16 procedure 52:6 249:22 procedures 13:11,15,19 19:14 41:5,8 41:14 42:14 49:3 101:3 108:2 109:19 111:8,11,14,15 112:1,6,16,22 122:2 134:15 222:22 223:1 233:19 237:10 256:8 260:7 271:12 277:10 281:12 287:14 288:6 proceed 219:3 proceeding 63:13 88:7 125:17 201:8 proceedings 4:1 248:9 249:18 274:22 319:6,7 process 34:2,7 35:4,6,10,11	35:13 36:4,16 36:18 37:6 38:21 39:4,14 40:1,18,18,21 41:18 43:21 65:8 95:2 97:5 97:19 99:3 106:14 119:17 120:15,17 134:11 137:13 143:16 150:3 151:20,21 157:14 166:6 174:13 175:13 175:14 188:21 189:20 193:9 200:6 201:7 220:21 221:8 223:4 242:15 251:12 262:3 267:2 268:4,22 269:6 270:20 271:19 273:4 281:8,12 292:14,22 314:1 processed 165:21 166:3 processes 151:9 242:4 processing 166:8 189:16 190:10,22 produce 253:11 produced 252:14 253:6 producing 252:8 production 81:2 81:9,14 82:11 82:13 84:14,19 85:9,14,16 professional 25:11	professor 124:10 211:2 285:5 profile 187:16 profiling 137:6 profitably 115:8 program 5:11 5:13 8:7,19 9:17 10:1,12 10:19 11:4,11 11:19 12:4 14:8 17:1,2 20:4,19 22:15 23:15,17 24:2 26:13,17 27:7 38:6 43:7,10 44:4 47:14 58:10 60:18 63:11 67:5,20 71:1 87:9 89:14,15 98:22 107:14,16 119:5 120:3 123:16 135:9 182:12 194:7 195:22 197:5 199:14 210:20 219:17 236:4,6 236:9 237:16 237:18 244:5 252:14,22 261:20 267:15 270:3 271:9 278:13,14,19 313:20 314:14 314:19 316:15 programmatic 34:11 46:2 68:10 87:13 94:17 101:2 118:12,17 193:17 241:5,7 241:19 242:2,7 242:13 243:17
---	--	--	--	--

244:12,22	308:21 310:7	35:22 96:10	178:8 260:8	218:21 219:8
245:5,13 258:2	310:13 314:22	prosecutor	279:6 299:10	221:17,18
258:3 261:6,11	315:6 317:17	104:20,22	provided 14:9	222:1,9,13,20
261:15,18	318:5	prosecutors	40:14 58:6	225:16,19
263:10 264:6	progress 189:3	255:9	140:10,11	226:15 245:7,7
264:10 270:16	prohibited 14:2	prospective	provider 12:9	245:10 249:8
271:22 276:21	prohibits 12:19	239:18	providers 10:4	250:20 252:4,8
277:4 299:5,8	12:22	prospectively	11:22 67:8	254:2,14
299:18	project 3:17	190:1	143:8 165:3	255:19,20
programmed	33:5 115:2	protect 4:14,16	238:4 278:20	256:12,15,16
140:5,7	120:9 182:4	4:20 23:9	280:17 286:13	258:17 260:3
programs 1:5	185:5 200:10	36:20 48:10	295:1,10	260:14 265:14
5:5,11,16,18	210:17,22	113:1 116:13	provides 41:20	265:17 269:11
7:2,13,16,21	223:21 270:6	139:4 221:14	119:2 225:16	304:13 306:3
8:2,13,15	projects 144:15	227:4 236:2	providing	312:14,21
14:18 16:7	226:22	245:22 262:15	146:12 309:19	317:15 318:4
22:22 23:11	proliferation	279:16 304:4	provision 9:1	319:3,17
31:11 32:14	13:10 14:12	306:21	81:12,19 82:3	publically
33:7 36:7 49:9	promise 89:6	protected 18:10	85:21 86:3	211:11
54:6 59:3 66:3	102:10	304:5,7	115:16 117:5	publication
95:11 98:16,17	promote 6:4	protecting 72:18	118:15 239:20	131:21
99:2 107:4	139:4 290:9	225:13 244:7	provisions	publicly 7:14
120:19,20	proof 234:15	263:14	103:11 245:19	98:6 185:14
121:11 147:7	properly 98:15	protection	291:10,13	219:9 303:14
147:10 149:12	property 164:17	271:14 281:21	proviso 81:13	publics 261:3
149:14 150:11	proportion	protections 39:6	provoking	published 255:7
150:16,19	236:20	43:3 68:11	210:3	pull 37:21
151:10 152:12	proposal 98:8	70:12 158:3	public 4:3 5:15	172:21 207:2
152:13 173:1	156:6 270:7,10	224:17 297:11	5:18 23:1 30:4	punish 174:17
178:20 179:7	281:15	protective 22:12	30:8,14 32:19	puppies 191:22
182:14 187:4	proposals	288:19	43:6 48:8	192:4
188:6 197:1	114:15	protested 238:2	50:14 62:5	pure 296:14
201:21 203:12	propose 147:13	protocol 161:17	97:9 98:7,21	purely 21:21
203:13 211:13	191:3 244:3	prototypes	98:22 100:5	302:7
211:14 214:2	proposed 99:22	154:14	104:3 106:13	purports 81:4
214:17 218:11	100:20,20	prove 37:2	107:3,5 122:21	purpose 5:14
224:7,11 228:3	proposing 204:2	172:2,9,17	125:16 134:17	10:9 11:1
230:14,18	208:10	241:15	135:1,8 150:10	19:12 50:4
232:18 233:13	proposition	proven 172:8	150:15 152:5	70:22 72:3
234:13,17,20	86:7 184:21	provide 5:17	152:18 176:11	73:21,22 76:22
235:5 236:1	prosecute 96:12	29:5 40:22	176:13 180:12	110:19 115:20
241:3 244:6	prosecuted	80:20 81:6	182:10,13	117:12 146:12
245:5 247:20	91:11	118:1 133:16	183:1,7 200:19	156:8 176:14
274:1 308:18	prosecution	140:2,13 178:4	205:11 218:17	204:4 206:3

229:3,6 231:9 231:10 237:15 237:22 238:13 261:9 284:2 287:12 289:5 299:10 purposes 9:3 12:17 13:8 17:12 22:3 24:14 46:7 65:4 69:14,17 71:14,19 83:16 85:2 86:8 128:17 167:14 263:11 269:20 272:12,13 282:5 283:4,22 pursuant 1:6 8:21 12:1 42:1 103:8 pursue 177:3 pursued 135:17 push 102:22 142:22 144:17 147:7 159:7 225:11 226:15 284:22 pushed 138:10 pushing 225:3 226:6 put 45:2,9 78:16 78:18 87:17 99:2 106:1 121:4 138:19 146:16,16 153:19 196:6 213:8 214:20 214:20 215:13 243:14 265:5 269:5 286:1 307:21 315:16	27:17 229:8 quantity 236:19 quarter 32:11 quarters 38:7 quartite 92:12 queried 10:20 11:2 67:7 queries 11:8 18:4 19:8,17 70:5 74:4,4,5 128:16,19 query 18:10,13 67:15 77:17 204:2 querying 27:12 70:4 question 24:15 30:6 31:22 49:13,16 50:9 50:10 52:9 54:20 55:1,3 60:5 61:8 62:18 63:5,8,8 63:10,13 65:7 67:19 68:6,13 68:18,18,19 69:4,8 70:14 70:17,17 72:13 72:13,13 73:11 73:13,15 76:20 76:22 77:9,11 80:22 85:13 87:4,7,10,17 87:22 88:21 89:11,19 90:16 90:18 91:18 92:12 98:3,6 99:8 101:13,19 107:13,21 112:18,21,21 113:15 114:13 117:14,15,22 118:11 119:3 121:16 127:14	128:11 134:8 139:10,18 152:9 158:12 160:19 161:10 165:12 169:4 169:14,16,18 170:4,22 171:6 171:17 173:8 181:1,18,22 192:11,12,21 192:22 193:18 195:11 198:19 199:8 200:5,20 206:6 211:7,8 214:3,10 218:9 224:1 230:14 234:19,20 243:21 251:14 254:5 260:15 262:20 265:19 269:7 273:15 273:16,18 278:13 286:20 286:21 287:5 294:1,9 296:1 304:10 307:18 questioning 229:22 questions 6:17 6:18 8:11 15:18,20 28:6 38:6 44:2 47:1 54:12,16 72:4 75:6 76:17 79:19,21 92:6 94:16 97:22 99:13,16 102:19 103:22 104:2 107:12 124:6 125:13 126:19 129:1,5 129:11 156:1 156:11 181:9 199:7,22	222:12 236:12 263:3 265:8 268:2 272:14 290:22 292:5 292:10 293:17 294:6,8 309:18 312:1 quick 44:10 51:1 59:1 63:17 83:17 113:3 117:2 158:16 171:19 181:21 193:5 201:17 224:3 229:12 256:19 266:9,16 285:20 303:8 307:20,22 quickly 53:20 160:16 207:11 268:4,21 281:10 284:22 quint 89:19 quite 23:5 30:1 34:19 48:12 60:2 74:4 101:5 148:4,5 148:6 151:4 153:16,17 157:21 163:2 259:16 270:1 quiz 80:19 quote 20:9 25:8 139:13 144:5 162:18 208:19 224:18,18 228:4 quoted 33:18 quoting 28:15 160:21	56:4 61:9 300:14 309:4 racial 234:10 racketeering 64:10 radio 129:15 raise 28:11 180:18 raised 10:13 32:13 38:6 63:12 66:20 67:20 88:22 96:3 103:22 187:6 221:11 265:8 275:6,8 292:11 raises 24:3 75:17 88:22 94:15 107:21 random 18:1 range 217:4 231:16 280:18 rank 186:13 ranking 137:7 rapid 232:10 rare 301:2 rarely 74:4 159:13 rate 265:15 rating 137:7 rational 11:11 raw 147:14 reach 24:12 142:1 reached 25:2 291:3 reaching 204:3 react 212:11 reaction 122:3 296:8 304:22 307:21 read 25:18 34:20,22 35:2 61:4 84:12
<hr/> Q <hr/> quantities 10:14			<hr/> R <hr/> rachel 2:4 4:6 14:19,22 16:20	

85:19,21 86:12 90:1,2 130:3 133:22 295:4 reading 130:14 304:12 305:11 reaffirmed 32:2 real 44:10 50:6 71:5 79:13 81:22 83:8 132:8 151:3 170:22 171:19 189:6 204:1 207:13,15 234:20 249:8 276:16 303:8 reality 53:16 222:19 269:12 realize 148:3 171:3 206:22 303:6 realizes 174:7 really 70:14 86:6 87:12 97:1 115:6 119:12,18,20 120:5,20 121:6 121:20 141:15 149:8 153:3 156:8 174:7 177:7 181:11 181:14 187:10 188:5 199:18 201:11 207:4 212:17 214:11 214:14 216:20 225:10,22 226:5 238:5 247:11,19 273:14 276:12 277:11 288:16 294:18 299:11 303:11,11 307:4 309:17 313:5	realm 187:12 reanalysis 199:21 reapproved 17:4 reason 38:19 69:18 113:22 122:16 127:8 128:3 182:19 204:9 228:5 232:8 261:17 267:17 271:18 285:13 reasonable 10:20 18:5 22:4 24:17 25:5 57:21 86:18 95:19 111:7 113:10 128:21 151:8 171:10 174:14 239:11 254:11 262:4,13 279:14 287:10 287:18 288:12 reasonableness 111:5 254:6 reasonably 13:12 42:9 107:6 109:7 110:2 169:5,12 237:1 288:9 295:15,18 311:21 reasoning 218:22 reasons 22:15 25:3,22 30:16 70:13 157:18 183:13 257:19 279:20,22 287:19 reauthorization 42:17 89:5	305:3 reauthorized 8:17 12:6 20:2 42:16 rebuttal 113:2 receive 260:8 received 23:18 receives 24:1 97:6 receiving 104:15 recipe 79:8 recipient 62:12 62:14 recognition 153:8 190:22 recognize 153:2 168:16 231:1 recognized 39:2 124:18 171:18 278:5 recognizes 44:21 recommend 217:3 228:13 228:15 286:4 recommendat... 119:13 179:16 229:19 236:10 250:10 259:18 260:4 264:4 277:20 recommendat... 5:19 28:14 115:2 119:22 132:20 211:12 224:5,20 225:1 226:1,17,20 229:2 230:3 247:12 254:19 256:21 258:20 263:4 278:9 299:4,6 310:20 recommended 4:10 200:19	299:17 record 21:1 25:9 38:13 52:10 55:12,17 59:6 69:16 88:16 122:21 123:14 125:16 182:7 189:8 209:17 222:13 312:11 313:3 319:7 recorded 7:3 recording 190:3 records 8:19 9:2 9:15 17:3 20:9 21:8,16 25:13 51:3 61:7,11 61:14 68:2,3 69:7 71:11,18 72:1 78:6 81:3 81:6,11,12 82:1,16,18,21 83:11 84:14 88:13 118:18 127:13,16,17 133:17 135:14 143:3,4,14,14 160:6 174:6 179:10,11 190:5 219:8 239:1,2,19 261:9 264:7,22 265:1,1 283:14 284:10,12 291:3,6 313:11 red 15:13 178:5 205:22 218:7 223:12 251:5 294:5 307:21 redacted 89:8,8 221:17 redress 139:21 reduce 311:15 redundancy 162:22	refer 12:4 59:11 141:9 reference 6:5 229:18 305:16 referenced 111:9 275:12 referred 8:18 12:3 refinements 216:14 reflect 112:16 187:7 212:11 251:15 reflected 120:9 244:9 249:14 309:21 reflecting 214:2 reflection 215:18 269:1 reflections 15:16 reflects 25:9 215:4 refreshed 82:19 refuse 37:1 regard 60:7 67:3 110:22 173:5 177:2 224:6 309:13 regarding 1:5 7:20 38:5 175:12 216:11 regime 289:16 region 206:14 regions 182:20 register 26:19 26:20 registers 83:2,6 regular 213:15 257:7,16,20 267:22 272:8 272:15,16 regulate 56:16 168:14 297:11
--	---	--	---	--

regulating 168:18 227:11	63:12 65:4 81:20 82:12	207:4	reporting 19:22 182:10 188:15	76:15,15 92:14 96:20 108:17
regulation 4:19 298:19	122:8,8,11 130:19 232:22	remarkably 231:1	200:19 256:7 256:15 301:11	232:11,16 233:4 240:2
regulations 7:6 7:9 50:12,15 50:16	233:2 253:17 253:22 279:13 286:10	remarked 141:20,21	reports 6:3 18:1 23:20 33:19	259:8
reinforces 302:20	relevant 20:10 20:11 21:2,4	remarks 7:17 15:11,16 16:22	202:8,9 225:18 305:16	requirement 39:10 40:2
reingold 5:6 123:8 317:5	21:13,16 55:6 56:10,11 57:8	37:18 38:2 56:6 87:6	repositories 280:16	61:19 109:22 113:8,16
reiterate 49:7	57:16,18 59:7	115:3 125:11 126:7,11	representation 186:7,11	116:10,12,21 118:10,14
reiterates 220:10	61:2 63:1,5 82:13 84:17	148:20,22 154:18	representative 86:1	220:11 229:2 234:1,7 278:22
rejected 314:20	96:9 122:17 130:7,7,13	remember 21:5 110:16 285:6	representatives 9:20 257:9	282:20 283:6 288:3 296:17
relate 198:8	159:5 234:19 239:1,3,6	remembering 27:20	294:12	296:18,20 301:22 302:13
related 4:19 14:13 34:6	240:10 262:14 262:17 270:22	remembrance 305:9	represented 195:1	requirements 41:2 71:5
35:13 48:11 55:8 71:1	279:16	remind 38:17 reminds 51:8	representing 88:5 105:1	75:10 167:18 223:5 283:13
relatedly 55:13 55:18 81:18	reliability 162:21 170:19	284:8	248:12	requires 11:18 18:11 19:13,14
relates 178:3	reliable 169:15 169:17 170:3,3	renaissance 1:15	reputation 202:14	22:8 29:16 59:15 77:11
relating 5:16 41:10 101:3	170:10,10,13 170:14 171:21	render 164:11 renders 166:9	request 21:8 51:3 89:5	83:1 92:16 110:9 111:4
221:6	172:16 207:9	reopen 234:3 repeated 147:6	95:16 267:3 305:19	130:9,17 131:8 133:15 137:12
relation 311:3	reliably 172:9 172:17	repeatedly 47:8 47:9 48:7 50:3	requests 119:4 135:18 270:1	172:3 180:6,9 180:10 288:17
relationships 25:14 185:10	reliance 29:10 relief 40:14	103:22 104:1	273:22 274:2	requiring 66:15 67:11,17
315:22	relies 30:2,5 233:18 242:3	replace 158:9 replacing 93:18	require 8:4 20:22 21:6,18	156:16
relative 184:18 254:5	religious 25:11 25:15 234:10	replied 35:6 reply 104:6	21:20 59:21 61:16 67:5	research 149:6 154:6,13,19
relatively 58:2 185:7 253:13	rely 173:12 relying 178:9	report 5:18 33:6 33:8 115:2	81:5,14 82:12 84:14,18 85:9	researcher 3:7 124:21
release 226:8,12	252:19	120:10 176:5 195:7,13,14	85:14 174:7 227:16 228:17	researchers 154:20
releasing 230:4	remain 6:8 78:22 125:17	202:3 236:15 242:21 308:7	229:4 233:10 234:16 239:9	resemblance 221:15
relevance 20:20 54:21 55:9,11	138:20 316:5 remains 215:11	318:4 reported 1:22	258:18 284:5 284:16 285:14	reservation 243:5
55:16,20 56:1 56:17 57:5,7	remarkable	228:10 237:3	required 41:16	
58:2,16 59:11 59:13,21 60:1 60:3,7,10 62:20 63:1,2,8				

resident 12:15 23:19	173:1	returned 197:12	ridiculous 131:12	300:21 301:10
resisted 35:3	responsibility 134:22 280:7	returns 196:8	right 14:20	302:9,9 308:11
resolved 109:6 260:16	responsive 11:7 15:16	reveal 25:14 192:17 193:2,2	34:21 56:20	308:19 317:2
resolves 260:22	rest 92:10 247:18	202:15	62:17 74:3,8	rightly 48:13
resources 159:14 187:22	restore 229:2	revealed 60:19 76:10 202:7	79:10 81:20	116:15
194:3,6 198:21	restoring 228:21	revealing 25:16 49:21 61:11,13	96:7 104:6	rights 28:21
respect 4:22	restraints 62:6	129:5 136:10	106:6 109:11	75:22 277:6
59:16 60:4	restrict 138:7	183:11,11	112:20 114:7	278:5 284:15
63:6,6 71:16	restricted 309:1	184:8 185:1	121:22 126:13	290:3 299:16
97:21 100:12	restrictions 112:9 205:8	reveals 38:13 66:13 191:17	128:19 142:2	rigorous 277:9
136:13 162:16	246:8,9,13	308:7	143:22 145:14	ring 192:17
175:18 176:16	restrictive 22:7 72:12 73:13	revelation 31:10	145:21,22	ripens 65:8
182:16 212:2	77:19	revelations 36:2 141:11 142:22	146:4,11,15,16	rise 29:19 46:1
213:9,17,21	result 11:15 103:16 104:3	150:16 276:14	147:21 155:15	risk 117:21
216:4 218:18	198:3 254:14	reverse 12:22 115:17 117:4	158:20 159:3,9	141:2 150:5
219:16 236:3,5	resulted 43:21	reversed 90:12	160:13 164:9	187:5,19
236:8 238:20	resulting 31:11	review 3:15 4:13	164:20 165:4,8	205:14 234:14
240:3 278:16	results 180:11	36:13 38:12	165:17 166:2,8	235:10 306:4
287:17 305:13	resume 31:21 123:12 312:13	39:3 41:14	168:5 171:22	risking 203:12
305:20	ret 2:15	46:15 87:8,18	172:9 173:2	risks 132:1
respected 277:6	retain 17:12 69:15,17 112:2	90:12 92:14,18	175:18 178:6	164:1 199:20
respectfully 35:8	112:7 127:20	109:19 119:2,4	178:13 179:7	199:20 203:7
respecting 29:6	283:21	221:6,8,13	188:21 189:7	207:13,15
respects 22:17 242:9	retained 10:10	256:4 305:15	191:10,12,15	293:11
respond 44:6 86:15 188:22	retention 127:19 127:21 128:10	reviewable 36:1 306:1	192:1,13,14,19	road 28:3 79:7
189:8 211:9	140:20 278:22	reviewed 11:6 17:4 19:10	193:22 194:7	168:10
responded 292:7	282:20 283:6	63:10 90:12	195:3 201:20	robertson 2:15
responding 44:10 51:22	283:13,20	263:7	202:1,13,17	16:10 33:1,2
response 61:8 117:2 125:12	287:15	reviews 246:20	207:5 208:15	45:22 51:1
211:10 226:8	retrospectively 189:22 190:6	revise 125:22	209:12 210:7	62:10 63:7
305:19	return 18:13 23:16 118:10	richard 307:19	212:6 213:11	77:18 86:22
responses 6:20 54:16 256:19	118:14 193:12	rico 64:11 255:6	217:6,7 230:16	89:18,21 92:9
294:6		255:7	251:1 257:4	93:5 94:15
responsibilities		ricos 255:8	261:16 262:1,8	99:7 102:1
		rid 234:1 283:22	262:9,17	104:19 115:1
			263:19 264:9	121:17 193:16
			266:14,20	201:6 229:19
			271:2 274:8	249:15 259:14
			277:1 279:19	269:21 270:8
			281:5 283:18	robertsons 119:14
			283:20 284:5,9	robust 6:4
			284:11,14	257:14 311:15
			297:9 298:14	rogue 208:8

role 3:2 4:22 36:5 37:9 42:7 46:2 87:13 97:19 100:11 100:13 101:21 120:21 121:11 131:19 135:15 180:15 193:10 193:16 201:15 220:21 224:6,9 225:11,16,21 226:4 236:5 237:13 256:5,6 269:8,9 271:22 278:16	125:9 134:19 134:20 151:9 152:21 153:2,3 154:4,9,10,11 154:15,15,16 154:17 155:11 156:9 158:10 159:11 171:15 174:3,18 181:2 181:13 200:2,2 205:1 207:22 227:15 263:7 295:13	172:10,18 178:2 197:16 198:18 208:3 229:9 230:1,6 238:2,4,15 261:13 278:4 288:10,13,18 289:1,12,17,17 294:21,22 295:10 300:19 304:11,19 305:6,17,17,22	saw 64:7 207:16 213:1 234:4 247:4 saying 7:15 63:20 64:17 86:4 126:6 132:12 143:4 143:13 161:16 180:8 181:19 191:4 195:11 198:5 199:14 231:1 259:5,15 270:6 272:2 278:20 297:5 298:21 301:21 302:11 303:18 305:5 310:18 says 56:10 75:15 107:10 115:16 121:5 176:17 249:20 279:1 315:22 316:10 316:13	science 3:4,9 124:10 125:4,5 139:14 149:7 153:16 166:16 186:16 197:19 scientific 137:18 scientist 126:16 127:1,2 132:13 132:14 scientists 133:2 scoop 165:10 285:10 scope 9:6 48:8 58:10 77:13 176:14 200:21 270:17 276:11 276:16,18 299:8
roles 132:6 rolled 178:21 room 174:9 rotenberg 3:5 124:15 132:11 156:3 166:14 174:22 182:9 185:18 200:18 206:18 roughly 176:18 round 72:9 148:16 155:18 155:19 162:11 223:15 294:4 router 166:22 routine 246:4 roving 118:6 row 15:13 rubber 33:17 rudimentary 242:22 ruined 231:13 rule 53:8 150:3 151:9 206:4 231:17,17 232:3 242:10 243:22 274:13 283:20 288:7 rules 5:20 36:10	ruling 250:4 rulings 248:19 run 302:2 running 78:1 79:19 130:22 214:9 263:17 S s 11:17 12:14 13:1,3,4,12,16 14:1 16:10,17 18:8 19:1,4,16 39:11 41:10,21 42:9,10 45:12 45:13 52:2,20 53:4 66:6 94:22 107:17 107:19 108:1 108:13,15 109:1,7 110:2 110:5,6 115:14 116:13 128:3 136:12 139:16 145:7 156:13 161:8 162:14 163:15,16 164:8 165:13 165:15 167:7 167:13 168:10 168:11,21 169:1 171:4	sabotage 289:21 safe 151:18 safeguard 32:3 138:18,20 168:21 177:4 safeguarding 135:15 safeguards 48:9 74:8,9 80:15 139:11,11 140:3,9,10,21 175:6 177:2 224:8 225:12 244:16 277:21 299:7,16 saic 315:4 sales 3:20 211:2 240:19 261:16 273:19 278:12 280:21 307:20 308:19 salt 126:14 sam 28:16 sample 301:17 sanitized 107:1 satellite 108:10 satellites 297:18 satisfied 21:3 satisfies 74:7 satisfying 167:17 save 68:6 72:9	saw 64:7 207:16 213:1 234:4 247:4 saying 7:15 63:20 64:17 86:4 126:6 132:12 143:4 143:13 161:16 180:8 181:19 191:4 195:11 198:5 199:14 231:1 259:5,15 270:6 272:2 278:20 297:5 298:21 301:21 302:11 303:18 305:5 310:18 says 56:10 75:15 107:10 115:16 121:5 176:17 249:20 279:1 315:22 316:10 316:13 scale 38:11 47:10 58:17 155:6,8 178:21 184:22 188:16 189:21 205:4 scales 203:4 299:1 scaling 80:12 scanners 135:4 scans 315:19 scenario 159:19 160:8,9 280:9 scenarios 280:12 scent 276:16 scheduled 107:10 scheme 274:12 scholar 127:5 school 3:20 132:14 210:10	science 3:4,9 124:10 125:4,5 139:14 149:7 153:16 166:16 186:16 197:19 scientific 137:18 scientist 126:16 127:1,2 132:13 132:14 scientists 133:2 scoop 165:10 285:10 scope 9:6 48:8 58:10 77:13 176:14 200:21 270:17 276:11 276:16,18 299:8 score 187:21 scrambling 93:12 scratched 177:8 182:2,3 screen 9:7 screening 135:5 242:3 scrupulous 33:14 scrutinize 105:15 seal 319:12 search 21:6,9 24:22 25:22 26:2 35:16,21 51:3 66:15 76:14,19 104:16,19 120:11,11,11 126:9 128:13 130:17 131:14 156:15 193:11 193:12,14,20 254:7,10,11 268:19 270:1

272:19,21	section 1:6,7	105:8 124:13	seen 64:8 77:8	96:22 106:10
273:2,8,16	5:11,12 8:16	124:21 129:8	106:22 129:7	140:19 193:2,3
278:3	11:20 12:1,6	132:1,8 134:13	129:14 202:4	250:21
searched 57:3	12:22 17:3	135:3,7,14	203:21 228:11	sensitivity 106:8
76:11 105:2	20:2,8,21 22:6	159:15 174:5	232:9	sent 33:20
searches 76:5,8	24:7 25:13	177:19 186:21	segments 66:5	separate 19:3
157:3 194:2	26:6,13,16,17	205:14 207:12	219:1	20:22 69:18
232:15	28:15 37:19	208:22 210:20	segregate 70:11	72:2,2 181:10
searching 11:10	38:3 40:17	210:22 211:4	segregated	268:6
second 6:13	47:12 54:21	225:13 226:22	19:11	september 33:6
11:19 35:12	55:5,15 60:9	230:16 231:9	seize 67:4,5 75:8	sequence 65:17
44:4 53:19	61:1 62:11	232:14 243:19	seizure 76:19	series 15:18
64:21 78:4,11	80:22 81:1,8	243:20 244:7	113:16,17	103:11 125:1
87:1 120:10	81:13 85:7	245:9 265:22	seizures 75:14	135:17 230:2
123:16 125:18	86:11 100:13	270:9 280:2	76:2	244:3 280:11
128:12 134:10	122:7 123:17	299:4 304:8	select 210:13	serious 14:6
136:8 137:14	133:14 135:12	306:5 308:3	selector 198:2	29:17 75:17
151:10 166:20	136:5 149:18	309:9 310:16	selectors 145:21	113:15 129:8
170:4 199:12	166:4,5,8	317:9	selfpolicing	235:10 264:1
218:14 225:15	219:18 220:18	see 33:12 47:15	233:18	seriously 225:10
227:10 237:3	228:7,16 229:1	48:3 65:5,16	selfreport 195:6	226:4 270:10
244:14 256:1,3	232:19 233:9	71:6 79:12	senate 3:16	serve 28:2 284:2
262:3 264:4	233:13 236:3	89:7,7 98:5	210:13 219:2	served 16:11,14
286:2 304:22	238:20 239:8	105:6 106:9,9	292:12	62:4 210:12
secondary 127:9	239:18 255:11	121:15 122:21	senator 28:15	232:3
211:10	258:22 259:2	123:1 126:19	66:21	server 131:17
secondly 30:22	264:5 268:13	149:1,8,14	senators 292:13	207:2 316:5,6
34:10 51:12	270:18,18	151:16 152:2	305:5	servers 69:20
62:8 122:6	271:2 272:2	152:11 153:7	send 135:22	165:7 208:21
124:15 156:19	289:17 296:13	161:19 162:17	165:4	service 11:22
249:13	sections 81:18	165:5 166:14	senior 210:16	62:4 143:8
secrecy 28:22	sector 281:19	173:1 179:1	267:8	146:13 166:19
29:4 36:19	282:2,13,18,18	182:17 197:4	sense 66:12	171:8,8 278:20
46:1	282:21 286:1,4	198:19 244:9	105:6 136:12	280:17 294:22
secret 29:14,15	secure 42:5	246:15 255:8	150:13 151:3	295:10
29:19,20,21	94:13 313:14	263:19 264:8	152:19 154:10	serving 240:5
31:14,16 46:1	316:6	296:9 316:10	158:18 226:9	278:19
49:18 50:12	security 2:14,17	316:11	241:19 289:8	session 123:16
53:22 76:3,5,8	2:18 16:9,15	seeing 43:7,8	304:5 317:13	212:18 312:13
88:15 89:3	16:16 33:4	179:3 249:17	sensenbrenner	312:19
98:19 102:7	36:19,20 43:12	seek 19:3 229:22	86:1	set 20:18 30:17
103:10 135:20	69:18 70:7	seeks 21:20	sensible 169:2	50:16,16 55:11
255:1 272:6	72:16,19 93:16	265:15 268:19	sensitive 27:18	59:10 114:17
secrets 28:19	94:7 96:1,5,17	269:4	74:19 96:16,17	120:18 124:3

136:6 149:16 177:15 185:2 187:22 198:17 206:22 207:22 218:15 244:10 244:14 264:11 265:2 sets 187:15 244:8 268:10 setting 7:11 257:17 269:17 seven 26:15 286:7 seventy 190:8 sexual 25:11 shaking 166:15 shallower 26:5 shape 149:10 share 5:4 140:1 274:4 sharing 139:12 146:21 154:16 233:21 sharon 3:17 210:15 223:17 239:8 254:17 258:21 270:4 275:11 sharons 258:11 sheer 227:18 shes 280:3 shift 117:1 186:3 shifting 122:15 shiny 127:3 shocking 31:10 shores 302:4 short 130:21,22 224:1 shortage 132:15 shouldnt 181:6 188:8 198:4 244:21 255:12 268:15 285:16	306:16 show 62:17 143:4 165:15 165:16 277:2 showing 17:13 20:22 61:16 105:15 114:22 228:17 229:5,7 232:22 233:4 262:4 271:7 276:22 277:9 277:13,14 278:6 285:2 shows 274:21 shut 147:6 side 34:22 35:10 37:10 104:10 104:18 105:1,8 105:10 131:17 131:18 169:2 174:1 195:1,17 265:18 317:10 sidebar 54:13 sided 34:8 sides 30:6 34:17 34:20,20 158:17 201:11 265:12 310:6 sifting 18:1 sight 317:13 signal 209:1 signature 93:8 signed 33:7 214:19 significant 39:18 42:12 45:19 74:12 76:2 94:16 201:1 213:7 215:3,4 216:5 226:5 230:4 234:21 253:17 260:2 272:14 signing 245:4	signs 93:1 similar 20:6 135:7 141:3 175:13 229:2 similarly 57:17 103:18 257:18 simple 186:2 simplicity 217:16,17 simplify 217:4 simply 18:13 27:11 45:15 134:1 153:10 155:20 175:4 177:22 206:21 245:18 251:10 simultaneously 203:11 sincere 102:11 single 27:2 185:1,2 sit 17:5 33:10 sites 161:19 sitting 153:12 212:14 282:2 situation 58:7 64:2 78:19 92:16 94:8 103:20 196:2 196:11 205:16 207:17 situations 56:14 75:12 195:9 203:21 253:22 six 54:5 69:1 184:4 196:20 197:3 210:5 217:13 size 295:21 skepticism 133:4 skiffs 257:6 skype 146:9,9 slight 70:16	slightly 184:22 257:21 275:5 slippery 284:20 slope 284:20 slow 267:19 273:10 302:19 slower 137:13 small 11:5 18:11 93:4 143:20 253:13 smaller 207:4 smith 26:17,20 45:14 137:1 167:10 smiths 167:10 smoothly 317:7 sneaked 89:20 snowden 8:14 51:14 205:13 207:13 socalled 174:10 233:14 social 133:5 185:6,8,14 231:10 242:18 243:15 society 51:17 221:3 227:21 235:7 solely 18:9 231:9 solid 265:5 soltani 3:7 124:20 140:16 158:16 159:21 164:4 171:19 177:11 179:5 191:2 193:22 201:17,19 206:8 solution 109:6 163:22 175:5 215:20 216:17 284:4	solutions 133:4 139:2,19 175:2 247:11 solve 158:14 279:19 281:16 solved 208:9,11 solves 168:3 279:18 282:22 solving 132:17 somebody 12:14 12:19,21 52:22 53:1 85:8 88:5 96:3 97:18 104:21 109:15 114:2 115:20 116:2 117:11 121:5 123:1 127:14 131:4,7 169:14 195:17 198:7 205:16 206:1 250:20 250:21 277:16 285:7 someones 174:8 206:5 someplace 162:20 somewhat 162:10 164:12 166:9,10,15 174:4 226:16 304:12 song 146:15 soon 284:1 291:18 sophisticated 10:16 77:4 soprano 241:12 sorry 38:1 90:2 159:8 192:22 238:15 258:3 289:17 297:12 303:20 sort 48:1 54:13
---	--	--	---	---

55:7 65:18	special 109:3	spent 40:11 52:4	155:8 171:4	253:20 265:13
70:19 81:22	110:21 113:11	79:18 151:7	192:8 211:7,17	268:19 290:8
85:10 89:6	149:22	247:16	230:22 243:2	290:17 294:21
90:18 97:8	specific 8:15	sphere 110:8	247:19 270:5	295:9 297:4
106:5 121:13	12:17 26:8,9	spied 231:8	275:11	298:4,8 300:19
124:5 146:19	28:13 56:9	spirit 297:21	started 39:17	301:1,1,4
146:20 157:4	61:18,18,19	298:1,10	54:14 120:7,16	statistical
157:15 170:20	115:16 117:7	spite 59:14	139:6 181:19	182:11
183:16 191:1	119:4 120:6	spoken 86:3	204:15 205:2	statistics 256:13
193:9 205:7	121:8,15	spotify 146:9,10	starts 98:11	stature 220:20
212:4,10 234:7	122:16 140:8	spring 40:8	277:4	status 167:13
246:3 266:19	176:12 202:7	squarely 232:19	state 33:3 50:3	statute 38:16
272:7 280:6,9	226:1 228:17	staff 40:12	155:2 216:1	39:9 43:4,7
286:19 294:17	230:1,2 239:10	267:7 317:5	319:4	47:20,21 57:22
297:15 301:2	247:13,20	stage 262:3	stated 9:20 17:2	60:22 64:4,6
302:4 304:9	250:15 258:15	stake 246:5	statement 32:20	64:18 80:18
310:15	258:20 263:4	stamp 33:17	44:15 132:2,18	82:8 83:1
sorts 153:21	270:7 278:4	stand 28:20 33:8	136:3,7 144:13	84:12,13,21
244:15 246:2	287:4 288:1	314:8	152:4,5 183:10	85:1,19 86:7
247:4 263:13	306:21 307:14	standard 20:20	191:22 223:20	87:10 91:3,22
276:12 310:3	specifically	20:21 21:3	296:8 303:16	92:2 96:21
sotomayor 25:6	39:22 67:3,13	54:21 58:3,17	statements 7:2	100:2 103:6
sought 39:8	88:21 110:9	59:13,16 61:9	63:18 191:14	107:7 111:7,19
62:16 122:10	116:19 228:15	62:21 81:21	205:20	112:14,19
122:15 158:4	309:7	82:12 156:16	states 12:16,20	122:9,10
228:19 239:12	specificity 59:22	156:17 172:7	12:21 13:5,13	133:21 149:19
sound 71:3	specifics 218:10	172:16 191:16	13:17 18:21	219:19 220:7,8
149:2	specified 10:22	228:16 260:5	23:19 39:21	220:10 223:5
sounds 34:21	specifies 279:3	260:11,12,21	41:7 42:1	224:16 225:15
source 164:13	specs 173:18	263:9,13,20	48:14,18 49:20	239:17,21
sources 36:21	speculate 266:8	279:13,15	52:17 53:2	253:4 274:6
southern 101:9	speculative	296:14	75:9 77:12	279:1 288:12
span 254:9	47:12 48:2	standards 20:8	95:1,5 107:18	288:21 289:5
speak 37:16	49:2 79:6	74:21 106:3,3	107:20 108:9	305:12 309:7
184:20 211:19	80:13	156:20 157:11	108:22 109:8	statutes 21:11
231:3 310:22	speed 162:12	227:8,14,20	109:10,16,20	59:14 64:9
speakers 6:5,9	267:14 294:3	228:22 275:22	110:3 112:11	84:9 216:19
125:18 175:9	spell 123:1	283:11	113:17,20	217:8 225:9
313:5	spelled 278:9	standing 37:4	114:2,8 115:22	227:5
speaking 211:22	spells 10:7	101:11	116:5 117:11	statutorily
speaks 67:11	spend 181:3	start 7:11 16:19	161:7,12 169:6	41:16
spearheaded	204:13	47:3 51:22	169:13 170:6	statutory 20:7
144:14	spending 94:21	56:3 75:6	175:22 187:17	36:15 41:2
spearss 146:15	200:13	140:17 144:4	201:4 248:12	109:6 118:15

200:21 220:3 223:6 238:16 245:19 284:15 stay 79:22 stayed 80:5 staying 174:2 stays 308:22,22 309:2 steady 232:10 steel 51:11 stems 27:14 step 178:18 241:1 283:12 steps 41:5,16 132:19 133:7 188:13 sterile 309:12 steve 15:22 16:19 22:19 40:10 44:8 46:18 52:5 56:3 63:18 65:21 68:16 87:2 104:13,17 107:14 113:2 116:6 120:13 124:9 126:1 152:9 153:20 157:22 160:15 161:12 163:10 165:8 171:22 181:17 199:1,1 259:4,14 285:5 steven 2:11 3:3 132:10 178:12 steves 49:10 106:6 132:12 164:4 170:17 181:13 196:19 stipulate 156:10 stop 78:16 218:7 stopped 31:19 60:19 storage 279:4	store 158:6 183:21 213:19 stored 138:2 stories 129:15 storm 209:1 story 90:1,3 95:7 233:20 stove 51:11 straight 185:9 294:4 straightforward 242:12 strategic 14:11 strayed 235:17 streams 191:1 street 102:13 124:22 strength 80:12 185:10 stress 22:6 155:1 strict 22:13 54:18 200:2 227:15 229:17 stricter 217:15 263:19 strictly 227:11 strike 173:2 230:15 striking 212:17 213:20 stroke 168:2 strong 79:3 80:9 174:8 225:3 251:5 262:21 269:18 317:8 strongly 61:22 313:18 struck 175:11 175:19 structural 99:11 99:17 205:15 205:19 216:14 structure 199:6	211:5 266:4 282:12 298:19 structured 189:13,18 196:7 structures 215:12 struggled 251:4 students 185:4 studied 175:20 studies 2:14 16:9 study 115:8 stuff 163:4,19 192:13,20 209:4 248:1 249:4,10,11 stunned 89:22 90:2 subconscious 234:9 subject 8:14 13:20 19:19 30:7,7 51:5 88:7 114:5 115:8 134:14 160:2 161:8 176:21 178:20 296:6 subjected 10:15 subjects 312:8 submissions 220:2 submit 7:7 32:19,21 34:12 37:6 123:7 141:9,12 158:5 182:6 183:5 249:19 submits 41:12 submitted 7:9 125:19 132:18 176:19 subordinate	70:17 subpoena 21:16 57:12 58:15,22 62:1,3,5,11 65:1,7,21 81:16,17 82:1 subpoenas 21:12,18 56:14 58:8 59:17 65:3,5,11,15 84:16,18 286:11 subquestions 55:8 subscriber 17:18 subsequently 305:18 subsidized 282:4 subsidy 279:7 substantial 134:16 221:19 substantially 260:9 substantive 203:3,9 substitute 246:8 246:12 300:6 succeeds 41:18 successful 14:14 135:6 256:9 suddenly 108:13 108:16,20 sue 5:6 123:8 317:5 sufficient 67:15 99:10 108:3 227:16 285:14 287:21 sufficiently 54:3 suggest 18:22 149:21 151:5	158:2 170:9 175:1 196:4 208:11 237:10 269:22 290:20 suggested 66:10 85:12 88:1 91:2 93:5 105:21 149:14 208:12 suggesting 79:11 157:7,10 180:1 293:16 suggestion 24:11 35:3 51:22 119:14 suggestions 120:6 121:9,12 135:21 suggests 276:10 276:10,11 sum 308:4 summaries 254:12 260:2 summarize 136:2 summarized 17:2 136:7 summarizing 224:4 226:17 summary 7:16 111:5 250:12 250:18,22 251:10,21 253:12 260:5,7 260:14,18,21 261:5 summer 40:15 sunset 218:16 291:2,19,19 sunsets 291:5 superstar 206:11 supervision 12:1
---	--	--	---	---

supervisory 205:9	surface 177:8 182:3	228:4 229:4 234:4 235:20	233:11 234:2 241:17 262:4	149:17 151:14 154:22 155:2,4
supplied 32:8	surprise 38:10 255:3	236:13,18,19 237:2,15,17	262:14 263:2 277:1,3,14	174:10 181:4 189:15 192:7
support 86:7 105:17 183:2 188:9 226:13	surprised 186:20	238:10,14,18 238:21 239:18	279:14 285:3 suspicious 18:14	203:10,15 205:2,7 206:12
supported 17:3 19:5 92:17 110:11 139:7	surprising 59:12 129:22 138:4 253:18	240:3 241:2,5 241:7,12,17,19 241:22 242:2,7	45:9 108:20 sustainable 259:22	<hr/> T <hr/>
supporting 95:18	surprisingly 43:8 138:3	242:13 243:17 244:12,22 245:5,13	swath 64:16 swept 26:14 switches 83:8	t 143:4 table 167:6 294:12
suppose 85:10	surveil 39:12	246:19,21 248:13 252:14	switching 145:4 syllabus 250:13	taft 16:14 tagged 306:20
supposed 51:9 60:2 78:20 99:5 208:13 276:4 313:14	surveillance 1:5 1:8 2:16 8:5 9:1 11:17 12:2 15:3,5 16:12 19:3,4 23:4,11 24:21 25:4,21 26:1,3,5 27:2 27:14 29:9,14 31:2 34:3,12 35:15,18 36:6 36:18 38:21 39:4,5 40:6,19 40:20 41:3,7 41:20 42:4 43:11 44:13 46:6,10,14 47:11 48:8 50:4 53:16 58:17,20 66:11 83:18,19,20 84:3,4,6 93:21 94:9,9 95:16 95:21 96:16 100:1,12,20 103:7 108:14 109:3 110:10 111:2 117:6 118:7 133:13 134:9 135:9 148:4 175:21 213:18 217:19	252:21 258:3 261:7,11,15,18 263:10 264:7 264:10 270:16 274:1,2,20 275:1 276:21 277:4 288:22 289:5 290:13 299:5,8,18 300:1,4 301:18 302:18 315:3 317:17	system 29:18,19 30:1,17,22 32:1 102:17 103:17 114:17 126:17,19 131:19,21 132:3,6,9 146:18 148:1 149:1,3,10 154:1,2,12 161:5 173:17 174:5 181:7 193:9 198:8 199:11 203:19 205:22 207:2 220:6 221:16 221:21 240:12 244:12,16 245:15 265:11 266:21 267:11 267:13 268:11 268:17 269:9 269:10 274:18 291:9 292:4,16 292:21 293:10 300:7 systems 140:12 142:4 145:19 146:8,22 147:15 149:16	take 28:11 35:8 37:10 38:17 48:15 54:4 73:18 79:9 84:16 89:17,21 92:11,13 102:10 104:10 121:14 123:12 126:14 141:17 155:13 163:1 170:17 174:4 209:14 212:4 222:4 225:10 226:4 236:14 241:1 245:10 255:12 261:3 269:19 270:10 301:17 312:6 317:14 318:1 taken 41:16 132:19 133:8 246:21 270:7 306:17 takes 9:14 41:6 58:18 97:20 111:3 159:17 261:2
supposedly 131:15		266:10 270:16 274:1,2,20 275:1 276:21 277:4 288:22 289:5 290:13 299:5,8,18 300:1,4 301:18 302:18 315:3 317:17	103:17 114:17 126:17,19 131:19,21 132:3,6,9 146:18 148:1 149:1,3,10 154:1,2,12 161:5 173:17 174:5 181:7 193:9 198:8 199:11 203:19 205:22 207:2 220:6 221:16 221:21 240:12 244:12,16 245:15 265:11 266:21 267:11 267:13 268:11 268:17 269:9 269:10 274:18 291:9 292:4,16 292:21 293:10 300:7 systems 140:12 142:4 145:19 146:8,22 147:15 149:16	
suppression 65:12		surveillances 39:10,20,21 115:13		
supreme 24:19 36:22 37:5 47:6 66:8,10 75:5 76:13 99:15 133:10 134:3 253:21 254:7,8		surveilling 289:10		
sure 46:20 58:13 78:22 80:4,14 91:20 92:13 95:14 102:4 105:16 106:1 116:20 126:12 140:2 157:6 181:5,9 189:9 212:5 215:6,8 216:20 223:16 225:12,18 227:22 229:14 251:20,20 264:19 266:6 277:9 285:21 298:20 299:9 311:3		susceptible 129:20		
		suspect 27:3 53:9 61:5,18 109:15 167:15		
		suspected 160:2 228:19 258:9 313:12		
		suspects 243:14		
		suspicion 10:20 18:5,9 95:20 100:17 231:20 232:1,8,10,16		

talk 33:9 45:21 134:7 141:6 151:15 159:18 162:4 193:8 206:19 215:19 242:8 248:2 257:22 306:11 313:10	13:4 31:2 41:1 41:7 46:11 48:1,13 107:17 115:19 116:2 117:9 130:4 146:5,16,17,20 146:21 170:14 171:2 176:3 236:22 241:21 276:3 277:2	teaming 178:5 technical 6:14 126:18 130:15 131:2,5,6,8,16 132:5 133:2,4 140:3 142:12 144:20 147:14 147:17 148:7 149:2,4 151:16 158:19 160:10 160:12 163:13 173:21 175:1 177:12 178:10 181:15 197:11 197:18,21 198:7,10,21 201:9	139:21,22 142:17 149:10 159:8 162:3 173:10,13,16 174:20 177:10 178:22 179:21 194:17 210:22 211:1 235:13 298:14,16 303:5	279:8 312:6,10 tend 200:2 tenure 314:3 term 81:10 83:20 121:14 121:19 213:9 253:17 276:9 terminal 206:22 terms 8:15 17:22 22:11,13 44:16 54:9 70:15 83:2 84:10 92:14 93:18 106:7 120:6,16 121:18 122:22 162:1 169:8 213:13 215:18 215:19 216:13 220:8 234:15 248:6 251:21 254:22 256:7 282:10 310:7 311:9
talked 45:1 53:20 62:10 66:6 69:3 70:18 114:16 187:10 194:14 194:19,21 195:15 212:9 215:22 257:19 266:7 294:16 302:12 310:6	targeted 13:11 88:16 100:21 109:7 116:15 229:13 253:7 targeting 12:19 13:1,3 34:3 41:4,13,21,22 45:8,11 52:19 88:16 101:3 109:20 110:2 115:17 117:4 119:4 172:7 220:6 222:22 229:16 233:19 237:4 271:12 299:12 301:1 310:3	technically 88:10 177:15 technique 67:12 129:19 162:11 171:12 187:14 190:9 techniques 137:8 139:8 153:14,21 166:19 technological 23:6 29:8 139:1,19 195:2 297:16 technologically 170:2,3 technologies 14:14 139:4 161:14 technologist 127:5 technology 3:2 3:19 23:8 39:15 51:6 83:3 108:7 123:18 124:8 124:14 125:5,7	tecum 81:16 telecom 144:8 telecommunic... 133:16 186:9 telephone 8:21 9:10,10,11,16 10:4,14,21 11:17 17:1 20:11,18 44:16 60:11 61:12 67:21 69:6,12 70:5 71:17 83:12 105:3 128:7 133:18 135:16 136:20 157:2 196:15 228:9 238:22 284:6 308:15 telephony 31:15 98:2,9 tell 33:20 34:16 70:5 77:22 79:17 103:13 105:18 159:4 164:13,14 175:15 178:8 195:21 202:13 233:20	terrible 121:5 territory 294:22 terrorism 4:14 4:20 13:9 77:7 110:17 208:5 216:4 227:16 228:1,6 262:15 262:18 263:15 279:17 289:22 309:14 terrorismrelat... 9:8 11:8 terrorist 8:4 10:22 14:9,10 18:6 19:1 20:14 74:12 108:22 109:14 160:2 234:18 234:21 243:4 terrorists 8:3
talking 16:7 52:21 58:11 70:20 71:12 79:20 82:8 96:15 103:19 109:14 114:1 114:11 117:11 118:4 149:10 151:8 162:7 167:1,2 193:15 214:3,7 216:3 232:18 247:17 249:16 254:22 256:3 258:9,21 263:17 271:15 277:16 285:4 289:9 301:3 302:13 305:4 309:13,14 310:5 315:11	targets 39:13 40:19 41:3 42:4 43:12 52:14 94:4,20 95:4,5 100:20 146:2 175:15 190:4 199:10 199:10 202:8 233:11 305:21 task 203:11 212:21 230:13 268:9 tasking 88:17 tasks 42:11 taught 133:3 tax 246:2 263:18 team 178:17		telling 144:14 tells 305:12,13 temporary 292:1 tempting 139:1 ten 183:18,19	

188:7 242:15 243:10,12 258:4,9 test 178:22 181:8 273:1,2 311:3 tested 65:10,12 272:21,21 testified 19:7 testify 139:16 testifying 40:11 testiment 317:18 testimony 85:3 testing 178:20 183:18 text 38:12 249:10 thank 5:2,6 14:20,21 22:18 22:19 28:4,7,8 32:16 33:2 37:12,13,15 44:3,9 46:21 47:2 51:21 54:10,11 80:17 92:7 104:7 107:8,9 119:8 123:3,3,4,9 132:10,11 140:14 148:10 202:19 209:13 209:16,21 211:18,18 217:21 223:18 230:8,10,11 240:18,19 247:5,6 254:17 278:10 285:19 293:21 312:4 312:10,12 315:7,8 316:20 317:2,3,5 318:6	thankfully 51:18 thanks 16:20 22:20 56:4 65:21 68:17 84:4 123:11 124:1 126:2 140:16 148:12 148:12 156:3 183:4 313:7,8 313:9 thats 7:13 9:9 11:5 18:16 20:19 23:2 27:6 33:8 34:8 36:12 45:2 49:5 50:8,20 51:14 53:3,5 54:2 55:3,12 57:4,21 64:1,2 64:18 65:6,14 65:18 67:21 68:13 70:6 75:1 77:9,16 78:20,21 79:8 79:11 82:13,22 83:3,3 87:10 89:18 90:3 92:2 94:14 95:14 96:7 97:1 101:4 105:4,11 111:14 112:11 113:10 114:12 120:8,12 126:22 127:1,2 127:6,10 128:21 129:16 130:7,18 133:17 134:5 142:2 143:16 145:12 148:18 149:6 150:5,12 150:18 151:22	152:20 156:11 158:21 159:3 159:22 160:13 161:5 163:19 167:4 169:6 174:16 175:5 178:7,14 181:20 187:4 188:5 189:13 197:12 201:10 202:17 204:5 204:13 205:11 206:6 207:3 209:9,9,10 213:5 214:18 215:17 218:19 219:4,18 220:17 222:2 223:13 228:14 234:19 237:7 237:18 239:2 240:2 241:8 245:18 248:20 248:22 249:16 250:5 251:18 252:4 255:4,5 255:15,21 260:11 261:12 261:13 263:13 264:14 265:10 267:16,22 268:18 271:1 275:2,8 280:12 284:4,4 287:21 290:17 292:21 298:9 301:10 302:16 303:17 303:19 304:14 306:17 307:7 307:18 308:19 309:8 310:10 310:18 312:3 314:10 315:2 theme 105:7	theoretical 31:6 theories 106:20 theory 167:21 thered 180:16 theres 18:1 22:4 44:20 45:8 47:22 48:3 58:15 63:14,14 65:10 67:18 81:13,19 86:6 89:11 95:21 105:16 108:5 113:14 115:15 120:21 122:1,6 131:11,19 141:10 142:20 144:16 148:19 150:10 154:8 154:20 156:7 159:16,22 163:19 164:5 164:22 165:14 165:16 170:18 172:5,16 174:13 179:13 180:15 182:4 184:10,15 188:20 189:3 190:21 191:16 191:17 196:14 196:14 200:3,9 204:9 205:7 218:19 219:11 222:19 226:2 228:1 233:3 235:20 242:21 244:8 246:16 248:1 249:2 250:6 254:4 261:21 262:13 262:17 265:17 266:22 269:16 271:6,8 272:10 272:12,17,19	273:2,19 274:6 274:15 277:16 279:12 280:1 280:19 282:1,6 283:5 286:15 293:4,19 298:6 301:6 309:8 311:7,12 313:20 314:4,5 314:7 thereve 192:15 theyll 145:16 147:22 206:11 293:19 theyre 23:12 50:15 75:19 82:17,21 83:22 88:6,17,18 91:22 93:12,16 107:5 110:12 126:8 145:14 145:14,15 147:11,19 162:13 163:12 163:14 175:2 176:21 178:9 178:21 181:5 192:6 202:13 202:15 204:2,2 204:12 266:21 282:3 283:8 291:13 theyve 147:6 200:7 282:2 314:21 thin 314:14 thing 34:9 53:9 54:2 59:12 71:2 74:2 81:15,15 83:17 111:14 113:4 116:21 120:13 130:6 132:7 133:3 134:10
--	--	---	---	---

145:18 155:1	46:4 48:11	151:1,1,3,5,10	238:20 239:7	313:10,17,20
164:16 174:14	49:4,8,12 50:5	151:18,20	239:15,16	313:22 314:10
188:3 194:22	50:8,17 51:4	152:11 153:1,7	240:5,13,15	314:13 315:1
202:22 206:10	51:16 54:2,14	154:7 155:3,6	241:12 242:7	317:18
213:20 247:9	56:5,11 57:18	155:12,12	244:4 245:13	thinking 118:5
248:2,6 251:8	57:20 58:5,12	156:15,17,20	245:20 246:1,7	122:13 149:9
271:8 272:3	59:9,20 60:2,7	157:13,21	248:21 249:2,3	150:2 173:15
283:18 287:2	60:14,20 61:13	158:12,13,17	249:11,15,21	187:11 193:10
288:2 300:15	63:5,7 64:17	160:10 168:9	250:8 251:4,5	212:2,5,15,15
308:16 312:19	66:20 67:19	170:16,18,22	251:18 252:5	214:12 275:12
things 8:1,3,20	69:8,9 71:4,6	171:10,15	254:15 257:2	286:3 287:16
55:6,14 66:4	71:21 72:12,20	172:18 175:4,5	258:5 259:2,13	287:22
70:19 71:22	73:9,12 75:4	177:2,5,11	259:21 260:21	thinks 261:17
80:4 81:9 84:9	75:15 76:1,20	178:13,17	261:1,13,16	279:9
85:14 97:5	77:9,10,11,18	179:17,22	262:18,20	third 4:3 6:14
101:6 123:21	78:6 79:5,8,9	180:1,6,9,18	263:9,12 265:3	87:22 129:9
124:22 127:6	79:11,14 82:4	181:3,8 182:2	266:11,17,18	131:3 137:19
129:21 130:1	82:7,8,11,22	182:9,22 183:1	267:13,16	164:5 166:21
131:11 135:21	84:5,12,17	184:10,12,15	268:3,5 269:12	209:15,18,22
144:9,10 145:3	85:5,18,19	186:18 187:2,6	270:21,22	210:4 218:16
145:11,13,19	86:6,15 89:4	188:13 189:1,4	271:1,17,19,21	227:12
146:8 153:20	89:19 90:11,21	190:15,19	272:4 273:12	thirty 269:4
159:10 164:9	91:19 92:3	195:15 196:7	273:19 274:6	301:2
172:14 173:19	93:10,16,19	196:12,17	274:18 275:7	thorough 40:13
175:9,22	95:6 97:16	197:10,20	275:16 280:15	thoroughly
177:22 178:11	98:11,12 99:10	198:9,14	280:22 281:13	264:5
186:21 198:3	101:16,19,22	199:14,15	282:19 283:16	thought 44:12
205:14,17	102:16 103:4	200:20 201:10	283:17 284:4,4	64:12 85:21
212:9,10	105:4 106:6,14	203:14,19	284:13 285:18	86:2 167:16
214:15 215:14	109:21 112:20	204:8,11 207:6	286:5,17,19	175:8,9 201:5
216:3,18 217:3	113:7,14 114:7	208:15,16	287:7,21	210:3 246:16
227:3 232:21	115:7,17,22	209:11 212:18	288:14,17,20	251:17 255:4
248:16 251:4	117:3 119:18	212:21 213:1,3	289:8,15,19	272:16 287:9
252:5 258:6	120:4,14,20	213:4,12,12,16	290:10,14,18	300:11 306:4
275:10 276:12	121:6,9,11,22	213:22 215:4,5	291:4,4,18	315:13
286:12 298:17	122:6,13	215:15 216:14	292:4 293:7	thoughts 81:17
302:19 304:19	129:10,13	216:16,18,22	294:15 295:11	118:19 179:20
306:13 310:4	134:6 135:6	217:4,18	295:17 297:9	247:7 270:4
think 22:15 23:2	136:4 137:17	220:19 223:10	297:14 298:12	281:15
23:7 28:22	138:12 147:10	225:21 226:13	298:22 300:17	thousand 191:6
30:15 31:22	147:10 148:7	235:17 236:2,4	301:5,10,11,18	194:1
32:4,12 34:21	148:15,18	236:9 237:6,9	301:20 303:17	thousands
35:12 44:14,17	149:13,16,19	237:12,14,17	307:8,12,12,15	108:21
44:19,21 45:19	150:1,7,14,21	238:3,5,7,12	308:8,19 309:4	thread 314:14

threat 14:5 46:11 187:17 216:1 230:17 264:1	83:8 93:6 94:21 108:12 111:10 115:6 117:13 123:4 124:2,15 125:7 130:22 132:16 138:8,17,20 140:7 142:1,1 151:7 152:11 161:5 162:11 167:3,8 171:9 171:16 174:16 182:14 194:5 197:2 201:1 204:1,7,17 220:1 223:10 246:15 247:16 248:15 250:1 267:10,18 269:6 274:5 276:17 279:3,9 287:17 292:9 293:20 294:2 303:11,19 308:12 309:16 309:17 312:15 314:18 315:21	today 5:10 6:12 16:7,21 23:10 28:10 31:12 33:9 37:18 38:2 44:1,14 80:1 88:2 123:16 126:4 141:6 146:8 163:19 182:18 201:7 211:22 212:10,21 213:3,4 214:3 214:18 215:22 216:4,17 221:2 223:19 225:17 232:18 247:17 259:11 272:5 283:13 302:1 303:19 315:12 317:3 318:2	66:19 148:22 touched 54:2 107:15 tough 46:19 217:1 317:8 tower 9:22 town 126:4 trace 35:17 83:2 track 118:2 tracked 26:21 tracking 25:6,12 26:7 45:2,4,6,8 tracks 181:10 tradeoff 147:11 282:10 traditional 64:14 102:17 141:14 175:13 176:1,15 270:12,14 289:11 299:14 traditionally 158:3 193:11 traffic 38:9 141:22,22 186:9 trail 159:5 205:10 trails 141:18 trained 23:3 training 126:22 transactional 17:11 21:21 137:5,10 transcribed 312:20 transcript 7:4 319:6 transcription 319:5 transform 186:7 201:13 transformed 186:10	translate 141:15 transmitted 83:22 165:7 transparency 106:18 150:13 150:15 151:4,6 151:8,11,12,17 158:19,20 180:13 202:9 225:21 227:13 230:3 236:4 238:8 240:3 245:6 248:3,8 254:19 256:1 transparent 106:20 transparently 163:2 245:17 trap 35:17 81:19 83:2 86:20 239:21 281:1 traps 81:21 travelers 163:13 187:16 traveling 163:14 travels 243:6 treating 171:5 302:10 trend 201:4 202:8 trends 152:1 182:17 trial 65:9,13 triangulation 166:20 tried 49:17 tries 261:3 trigger 242:20 triggered 27:10 trip 162:11 tripped 209:7 trouble 48:4 251:19 troubled 156:5
threats 14:15 77:12,13,14 96:16 244:7 245:22		today's 5:20 told 155:10 234:16 tolerate 233:13 tomorrow 283:14 ton 194:2 tony 241:12 tool 79:4 242:13 315:17 tools 80:5,10,13 164:11 177:18 183:2 245:21 246:2,3 263:14 top 182:5,7 209:12 topic 48:11 275:5 torture 84:8 total 27:21 168:6 307:16 totally 298:5,18 314:9 touch 6:2 56:5		
three 6:12 43:16 54:17 74:10 87:4 118:20,21 127:18 148:21 166:18 183:22 214:5 215:10 257:1 294:11 314:19				
threshold 138:13 171:7				
throw 55:1				
thrown 308:16				
thwarted 234:20 310:14				
thwarting 310:8				
tick 182:6,8 217:10				
tie 239:9				
ties 213:11				
tight 295:17,19				
tighten 296:14				
tightened 296:12				
tightening 227:8 227:14 228:15 295:13				
tighter 148:9				
till 248:14				
time 7:1 9:12 17:14 35:18 42:6 43:3 54:14 57:15 58:9 61:2 66:13 74:1,22 77:6,6 78:19 81:22 82:17	timekeeper 223:13 312:17 timely 266:12 times 31:7 52:13 102:13 130:3 140:19 143:6 196:20 197:3 207:9 313:8 tiny 19:9 27:9 152:21 tireless 5:9 title 53:7,10 104:20 116:22 175:13 176:1 201:3 217:11 268:13 277:17 308:8,12,13,20			

true 27:12 51:2 51:14,16 62:9 65:6 74:3,6 78:22 80:5,6 137:17 156:12 176:3 189:9 204:14 213:9 239:2	193:13 283:4 turning 11:19 291:17 turns 73:5 131:7 170:5,7 235:4 235:5 243:8,10 274:22 276:19 310:13	239:3 246:17 248:19 252:1 256:2 279:2 types 15:3,5 54:5 94:9 213:13 216:7 286:9 typical 84:17 166:17 typically 93:2 136:10 166:21 178:22	304:11,19 305:6,17,17,22 uk 164:8 ultimate 175:5 ultimately 40:14 65:5 101:11 109:5 133:5 135:5 152:18 157:14 176:22 198:15 253:1 283:18 unable 40:5 unanimous 24:20 unauthorized 31:13 104:4 140:3 unbelievably 310:14 unbounded 186:13 uncertain 170:16 uncertainty 118:7 unclassified 5:22 7:17 190:16 250:12 253:11,14 257:16 260:2 uncommon 73:21 unconstitutio... 23:12 26:4 uncovering 186:21 undeniable 36:19 underline 304:21 underlying 50:9 136:11 137:11 137:20 147:18 186:1 187:7	197:8,8 205:18 228:11 252:9 undermine 277:5 underneath 215:15 underscore 23:10 understand 14:3 17:7 20:3 46:4 56:19 60:6 73:3 90:6 93:20 94:21 131:9 132:8 134:21 142:4,5 143:18,18,19 144:18 147:1 147:13,17 158:1 165:14 182:17 186:2 213:19 249:13 253:21 272:13 288:7 298:9 307:2 understandable 23:2 307:5 understandably 222:16 226:12 understanding 56:1 75:7 76:18 130:19 142:7,11 144:2 147:20 148:8 172:13 255:18 261:20 298:13 understandings 142:17 understands 81:11 understood 55:14,21 57:19 196:8 undertake 46:9 undertaking
truly 274:15,19 296:5,5 298:18 trust 105:14,14 179:15 199:6 248:7 251:15 307:13 truth 75:4 191:17 try 54:17 102:10 116:10,12 166:10 192:2 202:5 215:5 216:19 217:4 226:16 229:12 248:1 258:3 273:13 277:20 294:5 316:9 trying 101:13 154:7 163:9 168:6 173:19 175:16 177:1 191:5 197:9 216:13 226:7 266:10,15 276:15 293:2 293:17 tune 192:7 turn 10:4 14:16 41:4 55:2 123:20 209:19 210:4 238:4 275:5 277:13 290:21 turned 36:8 65:11 73:5 82:17 135:13	tweaking 91:3 twelve 29:16 twenty 300:16 twice 79:5 twitter 163:21 two 5:10,18 6:16 7:2,13,21 8:2 10:2 14:18 15:3,15 27:3 30:6,16 32:3 44:5 51:1 62:2 63:17 81:18 103:21 106:4 120:19,19 125:12 126:19 127:22 141:16 142:3 149:8,21 150:7 151:6 155:19 172:14 181:9 183:13 185:4 208:16 211:6,10 215:2 224:3 236:1 243:3,10,13 244:8 247:8 248:16 249:2,7 253:19 254:15 254:18 256:19 263:18 280:22 304:19,22 310:5 312:16 315:20 318:5 type 10:3,18 20:15 38:10 83:9 88:11 94:8 137:19	U u 11:17 13:1,3,4 13:12,16 14:1 16:10,17 18:8 19:1,4,16 39:11 41:10,21 42:10 45:13 52:2 53:4 66:6 107:19 108:1 108:13,15 109:1 110:5,6 115:14 116:13 128:3 136:12 139:16 145:7 156:13 161:8 162:14 163:15 163:16 164:8 165:13,15 167:7,13 168:10,21 169:1 171:4 172:10,18 178:2 197:16 198:18 208:3 229:9 230:1,6 238:2,4,15 261:13 278:4 288:18 289:1 289:12,17,17 294:21,22 295:10 300:19	uk 164:8 ultimate 175:5 ultimately 40:14 65:5 101:11 109:5 133:5 135:5 152:18 157:14 176:22 198:15 253:1 283:18 unable 40:5 unanimous 24:20 unauthorized 31:13 104:4 140:3 unbelievably 310:14 unbounded 186:13 uncertain 170:16 uncertainty 118:7 unclassified 5:22 7:17 190:16 250:12 253:11,14 257:16 260:2 uncommon 73:21 unconstitutio... 23:12 26:4 uncovering 186:21 undeniable 36:19 underline 304:21 underlying 50:9 136:11 137:11 137:20 147:18 186:1 187:7	197:8,8 205:18 228:11 252:9 undermine 277:5 underneath 215:15 underscore 23:10 understand 14:3 17:7 20:3 46:4 56:19 60:6 73:3 90:6 93:20 94:21 131:9 132:8 134:21 142:4,5 143:18,18,19 144:18 147:1 147:13,17 158:1 165:14 182:17 186:2 213:19 249:13 253:21 272:13 288:7 298:9 307:2 understandable 23:2 307:5 understandably 222:16 226:12 understanding 56:1 75:7 76:18 130:19 142:7,11 144:2 147:20 148:8 172:13 255:18 261:20 298:13 understandings 142:17 understands 81:11 understood 55:14,21 57:19 196:8 undertake 46:9 undertaking

168:15	235:10 242:14	64:8 65:3 77:4	V	versus 37:1
undertook	276:5	81:10 84:4	v 26:17 47:7	45:14 77:20
38:20	unlawful 238:21	102:15 110:15	49:2 66:7	120:10 137:1
undue 39:13	unnamed	111:15 118:16	100:9 111:2	177:9 183:8
150:5	271:11	121:19 139:6	268:13	258:18
uneasy 150:20	unnecessarily	144:22 146:8	vacuum 309:11	vett 53:17
150:22 151:1,2	273:11	146:10 159:7	valid 121:21	view 25:4 36:8
unfortunately	unnecessary	159:10 163:14	validity 6:10	62:22 70:19
123:4 217:14	19:15	173:6 176:14	100:2 222:17	77:19 84:11
291:5	unproven	204:3 206:2	valuable 116:7	98:15,16
unilateral 94:1	235:11	208:5 213:15	185:22 189:20	103:14 111:7
unique 64:2	unquote 162:18	241:15 242:20	190:9 282:7	112:21 137:17
134:20 167:7	unregulated	246:9 252:20	value 54:3 79:16	191:7 265:21
uniquely 168:1	298:5,7,18	255:21 263:9	187:3 264:8	viewed 122:19
234:13	unrelated 137:2	263:21 275:15	273:20 295:19	205:13
united 12:16,20	unreliable 145:1	282:4 284:12	values 242:10	views 5:4 6:21
12:21 13:5,13	184:9 191:13	305:2 311:5,11	242:11 244:1,6	15:8 54:22
13:17 18:21	unstructured	useful 57:1,4	317:21	80:20 224:15
23:19 39:20	189:16,17	77:6,19 137:10	variant 218:8	violate 30:10
41:7 42:1	unusual 94:14	149:19 163:18	253:2	205:18 206:4
48:14,18 49:20	unwise 23:12	182:16,17	variety 127:22	violated 103:11
52:17 53:2	unworkable	185:21 208:18	213:14 216:7	135:12
75:9 77:12	259:12 301:22	227:18 235:5	various 42:11	violating 200:12
95:1,5 107:17	update 187:6	237:19 260:1	68:2 79:20	206:3
107:19 108:9	upheld 26:18	260:11,16	219:1 242:4	violations
108:22 109:8	upside 136:13	301:11 309:20	243:6 245:19	154:14 224:15
109:10,16,20	urge 114:15	310:1,14,19,22	315:12	virtual 163:14
110:3 112:10	224:22 225:10	usefulness	vast 11:6 27:17	virtually 176:22
113:17,19	226:4 228:11	227:22	185:13 189:21	visions 213:2
114:2,8 115:21	236:14 294:3	user 167:8,11	231:2	visited 25:18
116:5 117:11	urged 6:9,19	168:3	vehicle 264:6,20	visits 23:22
161:7,12 169:6	urgent 43:2	users 145:3,4	velocity 216:9	vladeck 285:5
169:13 170:6	usa 1:6 5:12	uses 50:11 127:7	vendors 77:21	voice 186:9
175:22 187:17	8:16	127:9 137:21	verbatim 319:5	189:14,16
201:4 248:12	usage 84:10	138:3,5 145:4	verge 219:5	190:18,22
253:20 268:19	151:13 153:3,9	154:3 159:20	verify 174:2	voices 32:13
290:8,17	154:9 155:11	162:11 227:11	verizon 133:12	225:2
294:21 295:9	157:4 158:10	usual 97:16	133:19 135:12	voicing 64:4
297:4 298:4,7	158:18 159:2	usually 35:22	143:13 156:22	volume 196:14
300:19,22	usages 307:15	49:19 63:12,12	279:7	216:6
301:1,4	use 20:12 21:3	83:22 92:21	version 107:2	volumes 190:18
university 3:3	35:9 49:14,18	257:22	253:11 257:21	voluntarily 22:1
124:11	50:13,19 53:21	utilities 265:14	versions 213:1	voted 56:9 63:21
unknown	60:7 62:6,6	utility 265:15		voting 255:5

vpn 164:10	29:13 32:10	295:2 297:10	101:10 143:2,3	279:10 283:12
vpns 145:3	33:9 45:21	303:10 317:2,3	200:12 209:4	286:10 291:10
vulnerability	49:7 55:3,3	317:5	275:1 300:7	296:12 305:3
159:16	56:3 64:22	wants 88:12	waste 181:6	311:7,20 314:5
<hr/>				
W	66:19 78:13	92:11 128:20	194:5	314:15 317:18
wagging 315:2	80:19 97:15	247:5 250:19	wasted 314:21	319:10
wainstein 2:17	102:21 109:13	war 231:7	watching	ways 29:5 77:14
16:13 37:14	113:2 117:3	warehouse	212:14 261:10	141:3 145:2
38:1 47:5,17	129:6 132:12	261:22 262:22	way 52:1 55:20	177:3,6,12
51:21 63:16	132:22 140:17	279:7	62:9 63:22	286:7,15
73:19 78:10	141:13 143:11	warehouses	64:4,18 76:6	weak 208:21,21
87:1 103:18	144:18 146:21	162:20	78:20 80:2	208:22,22
104:7 115:10	147:2,12	warrant 12:17	84:7,19 85:5	weakened
150:10 255:1	148:20,22	21:6,20 35:21	85:19,22 86:5	232:20
259:3	149:21 152:7	76:7 90:9	86:12 89:1	wealth 25:10
wainsteins	157:1 159:7	92:17,20 93:1	92:7,9 95:22	weapons 14:13
51:12 175:12	160:15 162:20	94:8 104:19,21	99:4 102:1	wear 126:3
waiting 179:2	164:4,16 170:9	105:16,17	103:2,16	wearing 126:4
293:18	172:21 178:17	109:22 113:8	120:18 121:19	web 126:8 157:3
wald 2:5 4:6	182:8 187:10	113:16 114:1,5	126:20 138:7	171:8
14:19 15:1	190:2 193:6	114:10,11,22	140:5 146:22	website 7:5
44:3,9 46:18	197:3 198:19	116:10,12	151:12 154:8	23:22
46:22 49:6	199:5,19 200:6	185:15 193:12	154:19 157:7	websites 25:17
50:22 51:20	204:17 214:4	193:14 270:1	158:13 161:21	wed 69:19
65:22 68:19,22	214:11 215:20	270:13,14	167:9 169:22	week 133:11
69:4 70:16	224:3 226:19	271:8 272:19	170:11 171:5,6	183:22
72:6,10 87:3	228:3 244:3	273:8 277:17	171:8 172:2,16	weeks 49:4 86:4
89:20 92:7,10	245:12 246:3	277:17 304:18	174:17 176:10	98:18 115:9
96:1 97:14	247:9 249:20	warrantless	179:18 180:11	220:14
104:5 107:8	257:2 258:5	60:18	180:20 186:2,8	weigh 273:14
194:11,14	277:8 278:3,11	warrants 24:4,8	188:1,17	278:11 286:21
196:5 197:14	279:21 280:2	33:19 35:15,16	193:15,17	287:4
198:12,16	283:7,8,9	35:18 102:1,2	202:9 205:21	weighing 235:9
300:13 304:9	284:3 286:17	105:11 110:11	206:1 212:6	309:19
308:11,22	286:20 293:22	110:13 201:3	213:8 221:20	weighs 273:7
walk 174:9	299:2 300:12	229:20 271:10	223:3 235:17	weitzner 3:9
207:3	304:21 313:5	272:1	242:9 243:22	125:3 148:12
walking 79:10	wanted 5:2,6	wartime 303:16	244:18 248:11	155:16 157:6
wall 102:13	32:17 98:10	304:1	249:7 250:18	170:9 179:22
124:22 221:7	139:12 144:1	washington	255:17 257:7	184:20 188:12
walled 235:15	156:4 202:22	1:16 16:18	257:20 258:8	190:14 196:4
want 4:5 7:11	203:5 205:17	132:15 237:3	259:5 265:10	198:9,14,17
11:13 28:11	206:18 232:3	wasnt 62:19	266:22 274:6,6	203:14 207:11
	281:14 287:4	91:2 100:19	278:14,18	welcome 4:2 7:8

32:21 123:7 209:18 312:6 wellformed 206:6 went 198:2 306:9 weve 49:16 63:19 77:8 118:3 135:17 136:19 139:7 143:1 149:4,11 154:13 159:14 165:2 168:9 169:20 173:4 182:1,2 189:4 192:13 202:4 203:21 205:1 215:22 216:3 229:10 233:1 233:12 235:17 235:21 251:4 257:19 275:22 276:15 277:20 318:2 whack 92:11,13 whats 49:5 57:18 95:16 96:9 102:20 122:3 136:17 151:14 156:14 186:8 189:9 193:18 199:10 200:13 208:4 214:13,13 259:1 271:1 282:10 283:14 316:14 whistle 200:9,10 white 2:18 93:14 125:5 252:14 252:16 253:6 wholeheartedly 140:18 whos 104:10	115:20 116:2 116:15 145:11 167:9 174:6 189:14 198:7 201:13 208:13 263:18 269:17 312:7 317:15 whove 292:13 wickersham 16:14 wide 51:16 127:22 213:3,6 280:18 widely 137:17 wiesner 139:13 wife 308:15 wifi 166:22 wikileaks 207:16 208:21 william 314:13 willing 194:9 234:14 wilson 60:22 wire 84:1 108:14 144:3 wiretap 35:16 35:21 53:10 104:20 175:14 182:16 190:2 241:14 308:7 wiretapped 114:5 wiretapping 182:19 wiretaps 53:8 176:1,6,15 308:8 wish 7:7 33:22 102:11 withdrawn 176:19 witness 319:12 witnesses 119:9 119:15 183:6	294:16 witnessing 29:17 witting 95:17 wonder 305:11 wondered 97:12 306:9 307:3 wont 148:1 155:9 163:1 164:14 269:18 woodward 51:9 wool 51:11 word 35:5,9 56:11,13 60:7 63:1 83:18 84:4 104:6 130:8 137:3,4 229:14 261:6 286:13 311:2 words 11:3 12:22 28:21 67:2 111:16 156:14,22 167:6 191:14 225:8 work 29:4 33:14 33:20 57:2 60:3 79:22 88:8 91:1 102:12 103:17 107:4 116:19 133:1 142:8 230:20 235:15 240:2 251:21 257:7 258:11 266:22 268:7 268:15,16 283:10 291:14 311:14 workable 95:6 108:18 259:3 worked 32:11 76:4 137:1 259:16 303:16	303:22 304:4 314:22 working 154:22 179:3,16 195:22 199:18 200:11,12 202:11 293:10 works 35:14 179:1 201:7 250:1 253:10 265:11 workshop 1:5 1:15 5:4,14,20 7:3 167:20 workshops 128:4 world 79:13 116:17 149:7 150:22 152:1 154:21 186:3,4 235:18 290:10 297:2 300:15 300:17 worlds 153:20 worrisome 96:14 worry 204:9 235:19 304:14 worrying 94:22 worse 40:3 128:8 worst 161:11 worth 27:20 122:13 147:11 303:17 wouldnt 110:12 113:9 141:1 176:4 237:19 253:18 285:7 309:13 311:17 woven 255:16 write 248:22 274:6 writes 279:1	writing 126:13 250:18,22 written 7:7 12:9 32:19 60:22 123:8 131:1 136:3 141:7 148:20 154:18 205:20 226:18 251:1 wrong 24:13 52:3 115:12 130:14 145:15 185:20 192:6 195:6 198:3 wrongdoing 231:21 313:13 wrote 33:5 251:18 <hr/> X <hr/> x 198:2,3 249:20 250:2 <hr/> Y <hr/> y 249:22 250:2 yall 118:21 203:12 yalls 118:16 yeah 107:13 172:21 179:15 200:6 209:5 254:16 272:17 285:8,19 308:22 year 42:16 47:7 48:2 129:16 219:20,22 220:15 271:9 283:6 308:6 years 18:18 26:15 29:16 32:5 33:11 39:16 65:16 74:10,10 90:7
--	---	---	--	--

98:19 100:5 112:5 124:11 127:22 130:3 132:4,22 137:1 140:5 154:6 167:20 184:3,4 185:4 190:8 220:3 263:18 266:7 268:17 279:8 292:1 300:16 301:2 yellow 15:13 294:5 yield 169:19 194:9 243:18 300:13 york 101:10 102:13 130:3 youd 32:21 69:11 96:22 148:3 youll 52:20,22 78:5 146:7 191:12,21 251:19 288:4,5 youre 32:21 52:19 70:4,6 83:4,15 91:5 108:13 109:14 110:2,5,6 112:20 114:7 114:11 116:3 118:12 121:4 161:20 162:19 165:18,19 166:6 167:1,2 168:6 188:19 208:15 215:6 225:18 235:21 249:17 262:9 266:10,15 268:2 270:12 270:15 271:15 276:22 277:16	281:3 286:3 289:9 297:5 301:21 314:13 316:2 youve 46:19 121:6 129:14 138:8,15 149:11 165:20 166:2 214:5,7 214:7,8,8 <hr/> Z zazi 73:4,4 122:20 258:14 zealand 164:6 zero 232:17 295:7,8 <hr/> 0 000 185:8 209:6 <hr/> 1 1 125:17,21 141:21 176:18 176:19 289:18 1040s 263:19 10th 319:19 11 4:10 40:4 79:10 107:10 107:10 108:19 109:11 167:22 232:5,9 243:2 243:16 1127 1:16 12 123:13 12333 67:9 116:17 14 318:8 15 15:19 209:14 289:17 17 107:10 18 238:14 1801 289:18 1890s 300:21	19 243:2,16 1902 90:13 1970s 231:15 1974 28:16 1978 38:20 40:2 46:6 93:21 103:2 108:7 259:6 296:18 1994 76:4,12 1998 248:14 1st 7:10 141:9 <hr/> 2 2000 294:18 2000s 314:15 2001 31:11 61:16 64:8 122:9 294:18 2002 141:21 142:2 221:5 242:21 2003 201:2 20036 1:17 2004 85:5,6 252:11 254:2 2005 16:3 36:3 122:9,12 2006 17:9 118:6 252:10,12 2007 40:8 248:14 259:7 2008 36:5 38:16 40:16 42:16 218:20 219:4 221:13,16 2009 16:3 2011 8:17 20:2 254:3 2012 11:9 12:7 19:7 33:6 176:18 2013 1:10 293:17 319:13 2014 293:18	319:19 2015 291:3,16 293:18 20th 180:3 194:16 215 1:6 5:11 8:16,18,21 17:3 19:18 20:2,8,21 22:6 22:10 23:15,17 24:7 25:13 26:6,13,16,17 28:15 44:16 54:21 55:5,15 60:9 61:1,6,10 61:14 62:11,13 62:14 63:1,21 65:21 67:3,14 67:21,22 71:11 71:17 81:1,5,8 82:4,5 83:19 85:7 86:11 89:15,15 118:17 120:3,5 122:8 133:14 136:6 149:12 228:7,14,17 232:19 236:6,8 238:20 239:8 239:18 255:11 258:22 261:20 262:13 264:5 264:19 268:13 270:18 278:13 278:18,20 281:2 309:21 21st 180:2 194:17 206:20 222 135:12 25 185:8 250 209:6 290 141:21 <hr/> 3	30 1:17 107:10 123:13 300 11:9 19:8 74:5 196:16 <hr/> 4 4 318:8 40s 234:4 <hr/> 5 5 166:5,8 50 289:17 5000 172:22 50s 234:4 51 237:4,13 <hr/> 6 60s 182:20 234:4 <hr/> 7 702 1:7 5:12 11:20 12:1,6 12:22 23:16 28:15 37:20 38:3 40:17 45:11 47:12 48:13 94:17,18 95:2 100:13 107:14 109:6 109:18 110:17 110:18 111:3 113:22 114:12 115:13,16,22 116:11 117:5,6 117:12 118:15 119:2,6 120:4 149:12 161:1,9 165:19 167:14 167:18 219:18 220:18 229:1 229:21 233:9 233:13 236:3 236:12 237:16
---	---	--	--	--

238:7 259:2 270:18 271:2 272:2 294:9,15 295:12 296:10 296:13 305:4 305:11,14 70s 182:20 234:5 247:4 783 176:19 784 176:18				
<hr/> 8 <hr/>				
85 162:3 170:17				
<hr/> 9 <hr/>				
9 1:10,17 4:10 40:4 79:10 108:19 109:11 167:22 232:5,9 243:2,16 90 10:11 17:5 184:3 197:5 219:9 268:12				