

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Defining Privacy Forum

November 12, 2014

The public forum was held at the Georgetown
Marriott Hotel, 1221 22nd Ave, N.W., Washington,
D.C. commencing at 8:30 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

SESSION 1

Defining Privacy Interests

- Ed Felten, Princeton University
- Liza Goitein, Brennan Center for Justice
- Paul Rosenzweig, Red Branch Consulting, PLLC
- Dan Solove, George Washington University School of Law

Privacy Interests in the Counterterrorism Context and the Impact of Technology

Alvaro Bedoya, Georgetown Center on Privacy & Technology

Hadi Nahari, Chief Security Architect, NVIDIA

Privacy Interests Identified and Addressed by Government Privacy Officials

Erika Brown Lee, U.S. Department of Justice

Rebecca Richards, National Security Agency

Applying Lessons Learned from the Private Sector

Harley Geiger, Center of Democracy and Technology

Chris Inglis, Paladin Capital Group and former Deputy Director of NSA

1 PROCEEDINGS

2 MR. MEDINE: Good morning, and welcome
3 to the Privacy and Civil Liberties Oversight
4 Board's public meeting on defining privacy.

5 It's 8:30 a.m. on November 12th, 2014,
6 and we're meeting in the west-end ballroom in the
7 Washington Marriott Georgetown Hotel in
8 Washington, D.C.

9 This hearing was announced in the
10 Federal Register on October 21st, 2014. As
11 chairman, I will be the presiding officer.

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

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

19 (Vote taken.)

20 MR. MEDINE: We will proceed.

21 So what is privacy? The right to be
22 left alone? A desire for independence of

1 personal activity? The right to make decisions
2 regarding one's private matters? Space for
3 intellectual development, anonymity or obscurity?
4 Freedom from public attention? Freedom from
5 being observed or disturbed by others? Freedom
6 from intrusion into one's solitude? Avoiding
7 public disclosure of private facts about
8 yourself? Freedom from publicity which places
9 you in a false light? Freedom from appropriation
10 of your name or likeness? Control of how one's
11 personal information is collected and used?
12 Freedom from surveillance.

13 These are just a few definitions that
14 have been given to privacy in the past. I expect
15 during the course of today's discussion that
16 we'll hear others.

17 The meeting today and the comments we
18 receive will inform the Board's approach to
19 privacy issues within its statutory mandate.

20 There will be four panels today. The
21 first will focus on defining privacy interests.
22 The second will consider privacy interests in the

1 counterterrorism context and the impact of
2 technology.

3 Next we will hear from government
4 privacy officials regarding privacy interests
5 that have been identified and addressed. The
6 final panel will see how lessons learned from the
7 private sector can be applied in the
8 counterterrorism context.

9 Each panel will be moderated by a
10 different Board member, and after the Board
11 member poses questions other Board members will
12 have the opportunity to pose questions.

13 And afterwards, members of the audience
14 are invited to submit written questions. Peter
15 Winn has cards and people can get a card from him
16 and submit the questions, time permitting, for
17 the moderator to pose to the panelists.

18 I want to thank the panelists who have
19 agreed to appear here today on this panel and
20 others.

21 I also want to note that we have a
22 strict timekeeper, Joe Kelly, sitting in front,

1 and so panelists are encouraged to keep their
2 remarks brief so we can have a more extensive
3 discussion.

4 We will be taking a lunch break between
5 noon and 1:15.

6 Today's program is being recorded and a
7 transcript will be prepared and put on our
8 website at plcob.gov in a week or so.

9 Written comments from members of the
10 public are also welcome and may be submitted
11 through regulations.gov through the end of the
12 year.

13 Finally, I want to thank the Board's
14 staff, Sharon Bradford-Franklin, Shannon Wilson,
15 Simone Awang, Lynn Parker Dupree, Renee
16 Gewercman, Peter Winn, Joe Kelly for their
17 efforts in making today's event possible.

18 And so we'll now turn to the first panel
19 moderated by Judge Wald.

20 MS. WALD: Thank you. Panel 1 will
21 attempt to explore, I think it would be too
22 ambitious to say define privacy, and the many

1 separate individual and societal interests that
2 the notion of privacy encompasses.

3 The novelist Jonathan Franzen
4 perceptively remarked, "Privacy is like the
5 Cheshire cat of values, not much substance but a
6 very winning smile. Legally, the concept is a
7 mess." That's a quote.

8 That may be unduly pessimistic. Most
9 commentators do agree that there are aspects of
10 privacy that go way back to the most ancient
11 civilizations, and that our own Founding Fathers
12 enshrined several of them in the Bill of Rights.

13 But the concept of privacy has become a
14 receptacle for a conglomerate of interests or
15 values that individuals and society care about,
16 but which to varying degrees they're willing to
17 balance with competing values, such as national
18 security.

19 Thus, the law of privacy consists mainly
20 of a series of situations in which courts,
21 legislators or government officials have decided
22 to recognize a privacy interest, or not to, and

1 to protect, or not to, that interest against a
2 competing value.

3 So our panelists today will identify the
4 varied individual and societal interests that
5 travel under the rubric of privacy and discuss
6 how far and under what conditions our laws do or
7 should legitimate claims that are based upon
8 those particular interests.

9 Now our format will be for each panelist
10 to talk initially for seven minutes. And the
11 gentleman in the front row will give you a yellow
12 card two minutes before, and a green card will
13 mean it's time to wrap up.

14 And then at the end of their initial
15 speeches, then I will question them as the
16 moderator for about 20 minutes. Then that will
17 be followed by another 20 minutes of questions by
18 my fellow Board members.

19 After that, and I hope there will be
20 some time left for the written questions which
21 members of the audience are invited to send to
22 the people who circulate to collect them, and

1 then I will question them. I will discuss some
2 of those questions with the people on the panel.

3 You already, I think, have bios of our
4 illustrious panelists, but I'm going to identify
5 them very briefly before they speak.

6 So we'll start off, Liza Goitein is a
7 Co-Director of the Brennan Center's Liberty and
8 National Security Program.

9 MS. GOITEIN: Thanks very much, Judge
10 Wald. And I apologize in advance, I have a cold
11 so my voice kind of comes and goes, but thank you
12 to all of the Board members for inviting me to
13 participate in today's discussion.

14 If there's one thing I've learned from
15 my own involvement in privacy issues over the
16 past few years is that privacy is different
17 things to different people.

18 David gave a very comprehensive list of
19 some of the things that privacy is. I'm not sure
20 what I would add to that, except to say that I
21 think that for those who are outside the
22 ideological mainstream in this country, privacy

1 vis-a-vis the government can be critical to
2 effectuate other rights, such as the freedom to
3 religion, speech and association.

4 So collectively as a society we value
5 all of those aspects of privacy, even if some of
6 us value only some of them, or none of them.

7 So what does that mean for our analysis?
8 I think it's interesting for us to think about
9 different definitions of privacy, and it's
10 helpful insofar as it shows the range of
11 definitions that are out there.

12 But I'm not at all convinced that
13 Congress, or the courts, or this Board should be
14 in the business of attempting a granular
15 definition of privacy or its importance.

16 Look at the freedom of religion, by way
17 of comparison. Courts don't probe what religion
18 is or why it's important. And that's not because
19 the definition of religion is obvious, by any
20 means. It's at least in part because of the
21 opposite, because religion is different things to
22 different people.

1 So what the court does is it adopts a
2 concept of religion that's broad enough to
3 encompass the many different roles that religion
4 plays in people's lives, and then the court
5 protects it, except in the rare circumstance
6 where there's an overriding governmental
7 interest. And Congress has followed the same
8 approach.

9 When it comes to information privacy,
10 which is what I focus on in my job, the best
11 working concept of privacy, the concept that best
12 encompasses all of the important interests that
13 privacy serves, is control of information.

14 This concept avoids to some extent the
15 what and the why of privacy, and focuses instead
16 on the how, how privacy is realized as a
17 practical matter.

18 And it also has the additional advantage
19 of matching up quite well with the text of the
20 Fourth Amendment. If a person controls her
21 papers, she is secure in them. If a person does
22 not control her papers, she is not secure in

1 them.

2 What are some of the ramifications of
3 this concept of privacy? Well first, controlling
4 one's information means controlling not only what
5 one shares, but with whom and under what
6 circumstances.

7 I may share certain information with my
8 mother or with a close childhood friend, but that
9 doesn't mean that I've chosen to share that
10 information with the entire world, including the
11 NSA.

12 Sure, there's a chance my mother might
13 rat me out. There's a chance that my childhood
14 friend has a tax problem I didn't know about and
15 could be pressured by the government into
16 becoming an informant.

17 But to equate this outside risk that my
18 confidences may be misplaced, with a willing
19 disclosure to everyone in the world is a legal
20 fiction of the worst kind, and that's really what
21 the third-party doctrine is, in my view.

22 Second, you don't, in fact, relinquish

1 all control over information about your public
2 activities by virtue of walking out your front
3 door. There is such a thing, functionally
4 speaking, as privacy in public.

5 And this is something that's
6 well-understood in the FOIA context, the Freedom
7 of Information Act context. There's a privacy
8 exception under FOIA which allows the government
9 to withhold information if releasing it would
10 unduly compromise personal privacy. Think of
11 Social Security records.

12 The Supreme Court held in 1989, that a
13 rap sheet would be covered by this exemption,
14 despite the fact that all of the information in a
15 rap sheet is available by virtue of a diligent
16 door-to-door combing of court records.

17 So why was the rap sheet still private?
18 Because the court held while the information in
19 it was publicly available, it was practically
20 obscure.

21 This is such a commonsense concept and
22 it deserves a home in Fourth Amendment

1 jurisprudence. The sum total of a person's
2 movements in public over extended periods of time
3 may be publicly available information, but using
4 normal powers of human observation it is
5 practically obscure.

6 So when the government uses drones, or
7 stingrays, or GPS technology to pierce that
8 obscurity, it has compromised the control that
9 the person would otherwise exercise over this
10 information, and that's a privacy violation.

11 Third, privacy violations happen at the
12 point that the information is collected. We've
13 heard intelligence officials recently telling us
14 that we don't have to worry about the NSA's
15 collection of bulk collection of telephone
16 records because nobody looks at the records
17 unless they have reason to suspect some kind of
18 terrorist link. That is the government telling
19 you what aspects of privacy you should value.

20 Many people won't care if the government
21 collects but doesn't look. Other people won't
22 care if the government looks but doesn't

1 prosecute.

2 But the point at which the government
3 collects the information is the point at which
4 you've lost control. And for plenty of people
5 that loss of control itself produces harm. It
6 produces a feeling of vulnerability. It causes
7 people to change their behavior.

8 In 2014, there was a poll after the
9 Snowden disclosures showing that 47 percent of
10 respondents had changed their online behavior
11 after those disclosures.

12 There was another survey of 520 American
13 writers showing that one out of six authors,
14 after the Snowden disclosures, refrained from
15 writing about certain topics because they feared
16 surveillance.

17 After news stories broke about the
18 NYPD's infiltrations of Muslim student
19 associations, attendance in those associations
20 dropped.

21 In some ways these are some of the worst
22 harms that come from privacy violations because

1 they're society-wide. They impact the way we
2 function as a society. They impoverish our
3 social discourse by causing people to censor
4 themselves and not put ideas out there.

5 One last ramification of this concept of
6 privacy -- if I have time, I can't believe I have
7 time -- is young people. So I hear it said quite
8 often that young people don't care about privacy.
9 And it's certainly true that many young people go
10 on Facebook and share incredibly personal
11 information with 622 friends. But they don't
12 share that information with 623 friends.

13 What they share and the number of people
14 that they share it with may very well have
15 changed, it certainly appears so, but they still
16 control the sharing, or at least they think they
17 do.

18 And my impression, based on a totally
19 unscientific survey of all the young people in my
20 life, is that they still value that control.

21 So, the red card, I knew it was coming.
22 All right, I'll stop there.

1 MS. WALD: Okay, thank you. Professor
2 Daniel Solove is the John Marshall Harlan
3 Research Professor of Law at the George
4 Washington Law School.

5 MR. SOLOVE: Good morning. I would like
6 to make five brief points this morning.

7 The first point is that privacy is much
8 more than hiding bad secrets. One of the common
9 arguments that people often make about privacy is
10 that people shouldn't worry if they have nothing
11 to hide. And I hear this argument all the time.

12 This argument, and many other arguments
13 about privacy, are based on a conception of
14 privacy, a conception of privacy that's very
15 narrow, that sees privacy as hiding bad or
16 discreditable things.

17 Well, privacy is much more than that.
18 Privacy isn't just one thing, it's many different
19 things. Privacy involves keeping people's data
20 secure. It involves the responsible use of data.

21 It involves making sure that when data
22 is kept, it's kept accurately. It's making sure

1 that people who keep the data are responsible
2 stewards of that data, that people have rights in
3 that data and some participation in the way that
4 data is used.

5 All these things have nothing to do with
6 nothing to hide. They have nothing to do with
7 secrets and everything to do with how their
8 information is kept, collected, stored, etcetera.

9 I think that if we see privacy broadly
10 we can move away and abandon these very narrow,
11 cramped views of privacy.

12 The second point I'd like to make is
13 that privacy is a societal interest, not just an
14 individual one.

15 When balancing privacy and security,
16 privacy is often seen as an individual right and
17 then security is often seen as a social right.
18 And when they're balanced, society generally wins
19 out over the individual. And I think this
20 actually skews the balance to the society side,
21 to the security side.

22 But, in fact, privacy isn't just an

1 individual interest. It doesn't just affect the
2 individual, it's a societal interest. We protect
3 privacy because we want to protect society. We
4 want to shape the kind of society we want to live
5 in.

6 Privacy doesn't just protect the
7 individual for the individual's sake, it protects
8 the individual for the society's sake, because we
9 want a free society where people are free to
10 think and speak without worrying about negative
11 consequences from that.

12 The third point I'd like to make is that
13 the collection of personal data through
14 surveillance and other means of government
15 information gathering can cause significant
16 problems.

17 Data collection and surveillance aren't
18 inherently bad, but just as industrial activity
19 causes pollution, government surveillance and
20 data gathering can cause problems. And these
21 problems must be mitigated. They must be
22 addressed when they clash with important

1 interests.

2 Some of the problems include, one, that
3 this activity can chill people's expression. It
4 can chill people's exploration of ideas. It can
5 chill people in many different ways. Either they
6 might not say something, or they might say
7 something slightly differently, or they might act
8 differently, or do things differently. We don't
9 want that chilling when it comes to legal
10 activity.

11 The other thing, the other problem, is
12 that surveillance gives a lot of power to the
13 watchers. There's a lot of things that can be
14 done with a vast repository of data beyond a
15 particular aim that it might have been collected
16 for. Data has a way of often being used in other
17 manners, in other ways.

18 I think that another issue too is the
19 level of accountability and oversight that goes
20 into this, because it's about the structure of
21 our government and the relation of the government
22 to the people that we're talking about here.

1 What kind of accountability will the
2 government have when it gathers all this
3 information? What limits will there be on the
4 information gathered and used? How long will the
5 information be kept?

6 In a free society people are free to act
7 as they want to act, as long as it's within the
8 bounds of the law without having to justify
9 themselves.

10 They don't have to go and explain their
11 actions to a bureaucrat sitting in a room full of
12 television monitors about what they're doing.
13 They don't have to go and explain themselves when
14 a computer's lights are blinking red because of
15 something that they said and it can be
16 misinterpreted.

17 People don't have to worry about that.
18 They can act freely without having to worry about
19 how suspicious their actions might look. That is
20 a key component to freedom.

21 The fourth point I'd like to make is
22 that we can't adequately balance privacy and

1 security without a reasonable amount of
2 transparency.

3 There's an overarching principle that
4 this nation was founded upon, it is that we the
5 people are the boss. The government is our
6 agent. We can't evaluate what government
7 officials are doing if we don't know what's going
8 on.

9 Now this doesn't mean there should be
10 absolute transparency, but it does mean that we
11 need to know something, enough to be able to
12 evaluate government surveillance.

13 Because ultimately the choice about the
14 proper level of surveillance isn't the NSA's to
15 make, it's not the President's to make, it's the
16 people's choice. We can't forget that. It's the
17 people's choice, and the people must be given
18 sufficient information to make that choice.

19 My last point is that the government
20 must get buy-in from the people for its
21 surveillance measures. Without buy-in, people
22 are going to start to take self-help measures,

1 which is something that we see happening now.

2 We see that companies are providing
3 people with ways to encrypt their data to protect
4 it from snooping government entities. This is
5 the market speaking. This is something that
6 people want. This is something being sold to
7 people that people are going to buy. This is
8 something in demand.

9 Why? Why are people demanding this?
10 Because they've lost trust, because the laws
11 regulating government surveillance are weak and
12 do not provide adequate oversight or
13 accountability.

14 This is why strong privacy protections
15 aren't necessarily bad for security. In fact,
16 they ensure that the people are comfortable that
17 there is adequate oversight and accountability
18 for that surveillance and that they're
19 comfortable and know that they have the
20 information that they need to continually
21 evaluate what's going on.

22 And if they can evaluate what's going on

1 and buy into what's going on, things will be a
2 lot better when it comes to balancing privacy and
3 security. Thank you.

4 MS. WALD: Paul Rosenzweig is the
5 founder of the Red Branch Consulting Program, and
6 a senior advisor to the Chertoff Group, and he
7 was formerly Deputy Assistant Secretary for
8 Policy at the Department of Homeland Security.

9 MR. ROSENZWEIG: Thank you, Judge Wald,
10 and thank you, Mr. Chairman and members of the
11 Board. I appreciate the opportunity to speak
12 with you today.

13 It's really entirely appropriate for the
14 Board to begin a discussion of privacy in this
15 new technological age. In fact, in my judgement
16 it's essential.

17 And the reason for that is essentially
18 one that puts me in some disagreement with my
19 fellow panelists. I think that our conceptions
20 of privacy, founded as they were back in the
21 1970s with the FIPPs, are somewhat outdated and
22 antiques that don't survive the technological

1 challenges that we face.

2 The 1973 Thunderbird was a marvelous car
3 but we don't think of holding it out today as the
4 state of automotive engineering. Nor would I
5 think we should address the FIPPs as the state of
6 privacy thinking. We need, in effect, a Tesla
7 for privacy today.

8 What would that look like? Well, there
9 are many ways to answer that question, and I
10 think to answer it you have to begin by thinking
11 about what sort of value privacy is.

12 And here, again, I think I find myself
13 in some disagreement with other members on the
14 panel and perhaps with members of the Board. I
15 do not think that privacy is an ontological
16 value. I don't think it's akin to religion.
17 It's not an inherent human right or the product
18 of some natural law.

19 Rather in my judgment privacy is an
20 inherently instrumental value, one that acts in
21 the service of other societal values. It's a
22 utilitarian value that derives its worth only

1 insofar, in my judgment, as it fosters other
2 positive social gains.

3 Privacy for its own sake is just an
4 assertion of autonomy from society. It is
5 valuable insofar as it advances other objectives.

6 Now let me kind of put some salt on
7 that. The problem is that buried in the word
8 privacy are many different social values that
9 we're fostering, too many really to catalogue,
10 though the chairman did a good job of trying to
11 start.

12 For example, we often see in the
13 discussion here privacy is enhancing our freedom
14 from government observation. That's probably the
15 use that's most salient to what the Board does.

16 But it also enables democracy. That's
17 why we keep the ballot private. It fosters
18 personal morality. That's why we keep the
19 confessional private.

20 Privacy is also about restraining
21 government misbehavior, which is why we see
22 privacy values in the Fourth Amendment and other

1 procedural limitations on government action,
2 another way in which privacy is obviously
3 relevant to this Board.

4 And it's also, as Dan said, sometimes
5 about transparency in the sense that we have
6 privacy rules so that I know what you know about
7 me.

8 It can be about control, about control
9 of my own image.

10 And it's sometimes also about simply
11 shame, since one ground of privacy is enabling me
12 to keep from the world things that I'm not proud
13 I did, of which there are far too many, I fear.

14 What's important to note is that in all
15 of these instances the value that we're
16 protecting that underlies privacy is different
17 from the privacy itself.

18 And that in turn suggests to me that the
19 way to think about privacy is to think about what
20 operational activities would protect the
21 underlying value most.

22 It means we need to go to a micro level

1 to understand in general the nuance that arises
2 from the particular interest that is at the core
3 of the privacy that we're talking about.

4 For example, we protect the
5 confidentiality of attorney client
6 communications. Why? Because we think we need
7 to foster candor in the discussion between a
8 client and an attorney. That's something that we
9 feel so strongly about that the instances in
10 which we permit that privacy to be violated are
11 few and far between, and they come only with the
12 highest level of judicial scrutiny.

13 The Fourth Amendment itself reflects a
14 similar utilitarian value of the security of our
15 persons, places and things against intrusion.
16 Once again, we impose a high bar, a probable
17 cause requirement and a strong independent
18 outside adjudicator, a judge issuing a warrant.

19 But those aren't the only mechanisms by
20 which we can protect privacy. We have a series
21 of administrative processes that are often
22 adequate to protect and restrain government

1 observation.

2 They're embedded in many of the internal
3 reviews that are very common in the IC, in the
4 intelligence community that you spend your time
5 reviewing.

6 They're common in virtually every
7 institution of government that we have, at least
8 at the federal level that I'm familiar with,
9 where we think that administrative review,
10 internal oversights, inspectors general,
11 intelligence committee oversight are adequate
12 alternate administrative mechanisms.

13 So what does that mean for some of the
14 things that you think about? Let me look at the
15 two programs that you've written about and just
16 kind of express something there.

17 The 215 program is one that directly
18 impacts issues of government abuse or potential
19 abuse because of the pervasiveness of the
20 collection that underwent, that was there.

21 It strikes me that that sort of
22 pervasive collection is one that would require a

1 strong, independent review mechanism because of
2 the comprehensiveness of its activity.

3 By contrast, the 702 program, which
4 seems from what I've read from the outside from
5 your reports, more narrowly focused, is one in
6 which less error correction mechanisms are
7 necessary, less likelihood of inadvertent abuse
8 is there.

9 So if you press on what is being
10 protected, you get a sense of a better way to
11 protect it.

12 Let me say one brief word more about
13 transparency. I completely agree with others on
14 the panel that transparency is essential to
15 control conduct and misconduct.

16 But the critical question is, what type
17 of transparency? And for me, again, this
18 requires us to ask what transparency is for.
19 It's the ground of oversight and audit.
20 Transparency without that ground is just
21 voyeurism.

22 But absolute transparency, as Dan said,

1 can't be squared with the need for secrecy in
2 operational programs.

3 I sometimes think that some calls for
4 transparency, though I hasten to say not by any
5 other members of the panel or on the Board, are
6 really just coded efforts to discontinue
7 surveillance programs altogether.

8 The truth is that if we believe in
9 absolute transparency, we've gone a long way to
10 the view that democracies can't have secrets, a
11 view which I think is untenable in the modern
12 world.

13 And with my last thirty seconds let me
14 offer one last thought about the role of the
15 Board and the multi-varied nature of privacy.

16 Because I think that privacy is many
17 things and has many applications in many
18 different contexts, I also think that the most
19 appropriate ground for making judgements about
20 privacy is not in boards or judiciaries, but in
21 the most representative bodies that we have
22 available to us, in this instance Congress.

1 I realize that's perhaps leaning rather
2 heavily on a body that is not held in the highest
3 regard at this time, but nonetheless, that is the
4 mechanism in a democracy for accumulating diverse
5 preferences, weighing them in the balance and
6 reaching a judgment for a broader societal
7 interest.

8 MS. WALD: Okay.

9 MR. ROSENZWEIG: Thank you. My
10 apologies.

11 MS. WALD: Ed Felten is a Professor of
12 Computer Science and Public Affairs at Princeton
13 and founder of the Princeton Center for
14 Information Technology Policy. So he'll give us
15 a somewhat different lens through which to view
16 privacy.

17 MR. FELTEN: Thanks for the opportunity
18 to testify. Today I'd like to offer a
19 perspective as a computer scientist on changing
20 data practices and how they've affected how we
21 think about privacy.

22 We can think of today's data practices

1 in terms of a three stage pipeline. First,
2 collect data, second, merge data items, and
3 third, analyze the data to infer facts about
4 people.

5 The first stage is collection. In our
6 daily lives we disclose information directly to
7 people and organizations. But even when we're
8 not disclosing information explicitly, more and
9 more of what we do online and off is recorded.

10 And online services often attach unique
11 identifiers to these recordings which are used to
12 link them up again later.

13 The second stage of the pipeline merges
14 the data. If two data files can be determined to
15 correspond to the same person, for example,
16 because they both contain the same unique
17 identifier, then those files can be merged.

18 And merging can create an avalanche
19 effect because merged files convey more precise
20 information about identity and behavior, and that
21 precision in turn allows further merging.

22 One file might contain detailed

1 information about behavior and another might
2 contain precise identity information. Merging
3 those files links behavior and identity together.

4 The third stage of the pipeline uses big
5 data methods such as predictive analytics to
6 infer facts about people.

7 One famous example is when the retailer
8 Target used purchases of a product such as skin
9 lotion to infer pregnancy.

10 Today's machine learning methods often
11 enables sensitive information to be inferred from
12 seemingly less sensitive data.

13 Inferences also can have an avalanche
14 effect because each inference becomes another
15 data point to be used in making further
16 inferences.

17 Predictive analytics are most effective
18 in inferring status when many positive and
19 negative examples are available. For example,
20 Target used many examples of both pregnant and
21 non-pregnant women to build its predictive model.

22 By contrast, a predictive model that

1 tried to identify terrorists from everyday
2 behavioral data would expect much less success
3 because there are very few examples of known
4 terrorists in the U.S. population.

5 With that technical background let me
6 discuss a few implications for privacy. First,
7 the consequences of collecting a data item can be
8 very difficult to predict. Even if an item on
9 its face doesn't seem to convey identifying
10 information, and even if the contents seem
11 harmless in isolation, the collection could have
12 substantial downstream effects.

13 We have to account for the mosaic
14 effect, in which isolated, seemingly unremarkable
15 data items combine to paint a vivid and specific
16 picture. Indeed, one of the main lessons of
17 recent technical scholarship on privacy is the
18 power of the mosaic effect.

19 To understand what follows from
20 collecting an item we have to think about how
21 that item can be merged with other available
22 data, and how the merged data can in turn be used

1 to infer information about people. We have to
2 take into account the avalanche effects that can
3 occur both in merging and inference.

4 For example, the information that the
5 holder of a certain loyalty card account number
6 purchased skin lotion on a certain date might
7 turn out to be the key fact that unlocks an
8 inference that a particular identifiable woman is
9 pregnant.

10 Similarly, phone call metadata, when
11 collected and analyzed in large volume has been
12 shown to enable predictions about social status,
13 affiliation, employment, health and personality.

14 The second implication is that data
15 handling systems have gotten much more
16 complicated, especially in the merging and
17 analysis phases, that is the phases after
18 collection.

19 The sheer complexity of these systems
20 makes it very difficult to understand, to predict
21 and to control how they behave. Even the people
22 who build and run these systems often fail to

1 understand fully how they work in practice, and
2 this lead to unpleasant surprises, such as
3 compliance failures or data breaches.

4 Complexity frustrates oversight, it
5 frustrates compliance and it makes failure more
6 likely. Despite all best intentions
7 organizations will often find themselves out of
8 compliance with their own policies and their own
9 obligations. Complex systems will often fail to
10 perform as desired.

11 Complex rules also make compliance more
12 difficult. It's sometimes argued that we should
13 abandon controls on collection and focus only on
14 regulating use. Limits on use do offer more
15 flexibility and precision in theory, and
16 sometimes in practice.

17 But collection limits have important
18 advantages, too. For example, it's easier to
19 comply with a rule that limits collection than
20 one that allows collection and then puts
21 elaborate limits on usage afterward. And
22 collection limits make oversight and enforcement

1 easier.

2 Limiting collection can also nudge
3 agencies to develop innovative approaches that
4 meet their analytic needs, while collecting less
5 information.

6 The third implication is the synergy
7 between commercial and government data practices.

8 As an example, commercial entities put
9 unique identifiers into most website accesses.
10 An eavesdropper collecting traffic can use these
11 identifiers to link a user's activity across
12 different times and different online sites, and
13 an eavesdropper can connect those activities to
14 identifying information.

15 Our research shows that even if the user
16 switches locations and devices, as many users do,
17 an eavesdropper exploiting commercially placed
18 identifiers can reconstruct 60 to 75 percent of
19 what a user does online and can usually link that
20 data to a user's identity.

21 My final point is that technology offers
22 many options beyond the most obvious

1 technological approach of collecting all of the
2 data, aggregating it in a single large data
3 center and then analyzing it later.

4 And here I think Paul's analogy to the
5 1973 Thunderbird is a good one. We would no
6 longer accept the safety technologies that were
7 available on that vehicle. Nowadays we expect
8 airbags, we expect anti-lock brakes, we expect
9 crumple zones. We expect the latest technology
10 to be used to make the technology safer and to
11 reduce risk.

12 And we should ask for the same when it
13 comes to privacy. We should ask agencies to use
14 advanced technologies to limit how much
15 information they collect, to use cryptography to
16 limit undesirable flows of information.

17 There's a large and growing literature
18 on privacy-preserving data analysis and methods.
19 Determining whether collection of particular data
20 is truly necessary, whether data retention is
21 truly needed and what can be inferred from a
22 particular analysis, these are deeply technical

1 questions.

2 In the same way that the Board asks
3 probing legal and policy questions of the
4 agencies you oversee, I hope you'll build a
5 capacity to ask equally probing technical
6 questions.

7 Legal and policy oversight are most
8 effective when they're combined with
9 sophisticated and accurate technical analysis,
10 and many independent technical experts and groups
11 are able and willing to help you build this
12 capacity.

13 Thank you for your time and I look
14 forward to your questions.

15 MS. WALD: Thank you. Okay, for the
16 next 20 minutes or so I'm going to pose some
17 questions to the members of the panel, and I'll
18 pose them to a particular member, but then if one
19 of the other members has something very cogent,
20 as I'm sure everything you say is cogent, feel
21 free to contribute.

22 Liza, I'm going to start with you. Our

1 Constitution defines certain aspects of privacy
2 in the Fourth Amendment, security of one's home
3 and papers from unreasonable search and seizure
4 and protection from general warrants.

5 But are there other aspects of privacy
6 that the advocacy community believes deserve
7 legal recognition and judicial oversight, or can
8 they all be encompassed within the bounds of the
9 constitutional guarantees?

10 And if so, what are the ones you think
11 ought to be specifically recognized, protected in
12 our law?

13 MS. GOITEIN: Sure. Okay, so to start
14 with I suppose the obvious, the Fourth Amendment
15 applies only to the government. It's a
16 restriction on the government. It's not a
17 restriction on private parties.

18 And I think there's absolutely a place
19 for regulation of private entities and how they
20 control, acquire and control people's
21 information. Because the market doesn't always
22 do a great job of many things, although it does a

1 great job of other things.

2 But we certainly know that people are
3 not a hundred percent satisfied with the privacy
4 protections that have been provided in the
5 private sector, and that obviously falls outside
6 of the Fourth Amendment, but is deserving of
7 regulation.

8 MS. WALD: While I've got you there
9 before you go on, there was another question that
10 follows directly from this.

11 We hear an awful lot about the
12 commercial acquisition of so much personal
13 information and what they do with it. And in
14 fact, the argument is sometimes made, look, don't
15 worry so much about the government, but some of
16 the private, Google, some of the communications,
17 the Internet, have great masses of data.

18 Do you think that there's any
19 significant difference in the risks to privacy
20 that are displayed by the holdings of so much
21 personal information by the government, as
22 opposed to private entities, or is it like two

1 big behemoths?

2 MS. GOITEIN: I do think there's a
3 difference. I think that difference may be
4 getting smaller, but I think there is a
5 difference. There remains a difference, which is
6 that private companies do not have the same
7 coercive power over the individual that the
8 government has, and private companies and private
9 entities don't have the same motivations to
10 persecute people based on ideology or religion.

11 I mean these are things that we have
12 seen in the history of this country,
13 unfortunately. We have seen people targeted for
14 surveillance because they were political enemies
15 of the reigning administration.

16 So what I would say is that private
17 entities have neither the ability nor the motive
18 to throw people in jail on pretext because they
19 are politically opposed to the current
20 administration.

21 That said, I think companies, the line
22 between big companies in this country and

1 governments is getting thinner and thinner. And,
2 you know, certainly companies might have some
3 political axes to grind with respect to the
4 workforce, and they certainly have access to
5 people's information.

6 I am not in the least bit unconcerned
7 with the private accumulation of information, but
8 I remain more concerned with privacy vis-a-vis
9 the government.

10 MS. WALD: Okay. Let me try Professor
11 Solove.

12 Now you wrote something in an article
13 called, Conceptualizing Privacy, and you went
14 into it a little bit in your prior remarks, there
15 are sixteen kinds of activities that represent
16 privacy risks. Privacy itself has six aspects.
17 They're all defined too broadly and they're all
18 defined too narrowly.

19 And so you concluded, I think, if I read
20 it correctly, that we should concentrate on
21 specific types of disruptions to those interests
22 and what should be done about that.

1 Can you apply that kind of framework to
2 the kinds of protection that we need in national
3 security data and surveillance programs, in
4 collection processing, identification, secondary
5 use, all of the other things that you talked
6 about in your article?

7 MR. SOLOVE: Yes, actually in what I
8 wrote I talked about privacy not being just one
9 thing and having a common denominator, but being
10 a pool of common characteristics and actually
11 applying to what I laid out was a taxonomy of
12 privacy about various types of problems.

13 And I wanted to focus on the problems or
14 areas where certain activities cause disruption,
15 they cause problems. And we want to mitigate
16 those problems.

17 And what are those problems? Because
18 that's where we want to step in and say, hey, we
19 should regulate this, we should do something
20 about this, we should address these problems.

21 It doesn't mean that the activities that
22 cause them are bad, but it does mean that they do

1 cause the problems we need to address.

2 Some of these problems that relate to
3 government data gathering include, one is
4 aggregation, that you can take a lot of different
5 pieces of data, each one being particularly
6 innocuous, not really saying a whole lot about
7 somebody, but when you combine them together, you
8 can learn new facts about somebody. This is what
9 data mining is all about, and data analytics.

10 The whole becomes greater than the
11 parts. It starts to create a mosaic, a portrait
12 of somebody.

13 This then leads to the revelation of
14 information that someone might not have expected
15 or wanted when they gave out little pieces of
16 information here and there.

17 And I think this causes a problem. It
18 disrupts people's privacy expectations. It can
19 lead to knowledge of information that people
20 don't want exposed or that society might not want
21 exposed. And so I think we need to address that
22 problem.

1 And oftentimes conceptions of privacy
2 will ignore aggregation because they'll say,
3 well, if the information all were different facts
4 that were gathered from public information
5 there's no privacy.

6 But I don't think that's true. I think
7 we really want to look at what the problems are
8 and if we look at the problems, there's a problem
9 here.

10 Another aspect is a problem I call
11 exclusion, which is the fact people lack an
12 ability in a lot of cases to have any say in how
13 that information might be used against them, any
14 right to correct that information, or to make
15 sure that it's accurate.

16 And I think that's a key component of a
17 lot of privacy laws is there's a right for people
18 to make sure that proper decisions are being made
19 about them based on their information.

20 I can't go through all sixteen. I can
21 hit some others.

22 One is identification, the fact that

1 this involves linking a body of data, what I call
2 a digital dossier to a particular individual. By
3 identifying them you actually are connecting them
4 to data that then can be used to make decisions
5 about their lives. Some of the decisions could
6 be good, but some decisions could in fact be
7 harmful to an individual.

8 Security is another issue that I see as
9 related and part of my taxonomy of privacy, and
10 that's keeping data secure. When data isn't kept
11 secure, it creates risks and vulnerabilities to
12 people that could expose them to a lot of harm
13 if, in fact, the data is leaked improperly.

14 And that happens all the time. We're
15 all at risk when all this data is gathered
16 together in a big repository.

17 There are a lot of other things, but
18 I'll stop here in the interests of time.

19 But these are just some of the ways that
20 the taxonomy addresses this problem. I think
21 it's important to think of the overarching point
22 is don't start with some platonic concept of

1 privacy and see, you know, what fits in it and
2 what doesn't.

3 I think it's better to look at things
4 from the bottom up and say, where are the
5 problems here? What are the problems and harms
6 that are caused by these activities and how do we
7 address those harms?

8 MR. ROSENZWEIG: Could I just make a
9 brief comment?

10 MS. WALD: Yes, sure.

11 MR. ROSENZWEIG: I would agree with
12 everything that Dan said but I would also say
13 also look at what the benefits are.

14 You know, the President's report on big
15 data looked at the increase in the volume,
16 velocity and variety of data, and championed the
17 idea that large scale data aggregation creates
18 ubiquitous new knowledge -- serendipitous new
19 knowledge that is of value to society as well.

20 So it brings with it harm, but it also
21 brings with it benefits, and that is why I see it
22 as a kind of cost benefit utilitarian analysis.

1 MS. GOITEIN: Sorry.

2 MS. WALD: Yes, go ahead.

3 MS. GOITEIN: I just want to say one
4 thing quickly. I thought this it's a utilitarian
5 value, not a human right, it is a human right.
6 It's listed in the Universal Declaration of Human
7 Rights, it's listed in the ICCPR, and other
8 treaties and protocols that the United States has
9 signed and that have the force of customary
10 international law.

11 So whatever one's personal feelings
12 about that, I don't think this Board has the
13 latitude to decide that all these treaties we've
14 signed declaring it as a human right are void.

15 MS. WALD: Of course defining what's
16 included in that human right has been one of our
17 problems, it's been one of your problems, it's
18 been everybody else's problem.

19 MS. GOITEIN: Of course, but it's a
20 human right.

21 MR. SOLOVE: May I make one small point?

22 MS. WALD: Yes.

1 MR. SOLOVE: And that is I think I
2 totally agree about the benefits of big data and
3 the use of these things, but I think often the
4 balance is wrongly cast between, okay, here,
5 let's take the benefits and let's weigh it against
6 the harms.

7 Because protecting privacy doesn't mean
8 getting rid of big data, or not engaging in
9 surveillance, or not doing a search. The Fourth
10 Amendment allows searches and allows
11 surveillance, for example, it just requires
12 certain oversight.

13 So what we need to look at when we're
14 balancing is not all the benefits of big data
15 against privacy, we need to look at to what
16 extent do oversight, accountability and these
17 protections on it, to what extent do they
18 diminish some of those benefits.

19 And that difference, that diminishment
20 is what gets put on the scale against privacy,
21 not all of big data's benefits. And I think if
22 we weigh that appropriately, then I think we get

1 a better balance.

2 MS. WALD: All right.

3 MS. GOITEIN: Very quickly.

4 MS. WALD: Briefly.

5 MS. GOITEIN: Yes. We don't get to
6 weigh these things de novo when it comes to the
7 Fourth Amendment. The balance has been struck.
8 The government can't say we want to do searches
9 in people's houses, we have a really good reason,
10 we don't have a warrant, but we have a really
11 good reason, let's everybody do this balance
12 anew.

13 That balance was struck by the drafters
14 of the Fourth Amendment. You need, in the vast
15 majority of cases, there are some narrow,
16 delineated exceptions, but you need a warrant
17 based on probable cause of criminal activity to
18 do those searches. This is not starting from
19 scratch.

20 MS. WALD: Mr. Rosenzweig, your
21 approach, and you talked a little bit about this,
22 your approach for balancing privacy and national

1 security has I think been termed, whether you
2 call it instrumental or consequential, but in one
3 of your articles you talked about you thought
4 limiting the right of somebody to complain or to
5 go to court, etcetera, to intervening on the
6 basis of when they are suffering a tangible harm,
7 like a warrant or being called before the grand
8 jury, as opposed to Professor Solove's views of
9 privacy as a kind of foundational value,
10 recognizable in its own right.

11 Yet you also recognize in some of your
12 other works the significance of some aspects of
13 privacy to a democratic society.

14 Now all of you have talked about it
15 isn't just an individual right, it's a right that
16 an open society needs, starting with even the
17 necessity for people developing their
18 personalities in an atmosphere in which they feel
19 free to experiment a little bit, to have
20 relationships, to talk without feeling that
21 they're constantly being judged by the government
22 or society.

1 I'm wondering how you reconcile your
2 recognition of the aspects of privacy that are
3 necessary to a democratic open society with this
4 notion that we really shouldn't start intervening
5 until somebody is suffering some tangible harm.

6 MR. ROSENZWEIG: Well, thank you for the
7 question. I think that I don't see them as
8 irreconcilable because I see the question about
9 the adversity of consequence and the error
10 correction mechanisms as critical to the first
11 part of your question, the inherency of the
12 value.

13 To say that, I sort of sometimes use a
14 thought experiment, which is, what if in some
15 hypothetical world, which I assure you does not
16 exist, the government never abused anybody, never
17 actually misused the data it was collecting,
18 never, had no lists of enemies, no persecution,
19 and never made a mistake.

20 Now granted, that's an impossible
21 standard, but if that were the instance then in
22 the long run the values that underlie, the

1 democratic values, would be supported and people
2 would no longer fear the collection because the
3 lack of adverse consequence, or by hypothesis, a
4 hundred percent would have gone away.

5 So to my mind, the way to support the
6 values that we see in the underlying democratic
7 sphere is to build the error correction
8 mechanisms, the audits, the oversights, this
9 Board, into the process in a way that reassures
10 society, as much as possible, that we're driving
11 down the errors, and frankly both types, the
12 false positives and the false negatives, but this
13 Board is principally concerned with the false
14 positives, driving down the errors as much as we
15 humanly can.

16 We don't eliminate government programs
17 because of the possibility of error because every
18 government program, every human endeavor has the
19 possibility of error.

20 We arm police officers, even though we
21 know that they will sometimes misuse their
22 weapons. We don't eliminate that. We try and

1 drive down the error rate as much as possible so
2 that we engender people's confidence in the
3 police.

4 And we see sadly these days exactly what
5 happens when people's confidence in the police is
6 not maintained, that our error correction
7 mechanisms are deemed by society inadequate.

8 And I think we're sort of seeing some of
9 the same thing in response to the Snowden
10 disclosures as well. But that suggests to me
11 that the right way to support the underlying
12 values is to go back and think about how to fix
13 the error correction mechanisms.

14 MS. WALD: So let me just pursue one
15 thing that you brought up earlier, which has come
16 up in some of our past reports and is bound to
17 come up in future ones, I think, and that is at
18 what stages, if you would go into a little bit
19 more into the point at which you think an
20 independent review of decisions outside of the
21 government's internal auditing and processes are
22 necessary to ensure that you have this kind of

1 trust by the people that the government is not
2 taking risks to its privacy, and in terms of what
3 you yourself suggested that history has got some
4 lessons for us on the "trust us" aspect.

5 MR. ROSENZWEIG: Well, I certainly don't
6 dispute that we've had failures in the past.
7 Anybody who would dispute that hasn't read
8 history.

9 I would say that there's no one size fit
10 all answer, that it really depends upon the harms
11 involved and the nature of what you anticipate
12 the failure mode would be.

13 I'll give you two examples. On the one
14 side we have the current TSA inspections programs
15 at the airport. Probably a fairly significant
16 error rate of false positives, pulling people
17 aside for secondary inspection.

18 On the other hand, a comparatively
19 modest intrusion. And I say that knowing that
20 many people think it's a very large intrusion,
21 but nonetheless comparatively modest compared to
22 the coercive nature of being put in jail, for

1 example.

2 So in that instance we seem reasonably
3 happy with a principally administrative
4 methodology that doesn't require any outside
5 check because individual liberty is not at issue,
6 long-term confinement is not at issue. The
7 degree of harm is small.

8 By contrast you will infer that I
9 certainly think that independent review is
10 essential whenever people's liberty is at stake,
11 when significant aspects of livelihood are at
12 stake.

13 I think that one of the strangest things
14 that I see in the privacy debates today is that
15 we seem to get all wrapped up about things like
16 the TSA screening and we don't look at how
17 government databases are used to deny employment
18 to people.

19 You can't get a job in the
20 transportation industry with a record, even if
21 the record is itself ripe with error, because of
22 the transportation worker identity card.

1 So we, I think, have it backwards a
2 little. And that would be an instance where an
3 independent review of some sort for somebody
4 who's denied employment in the nuclear industry
5 or in the transportation industry would be right.

6 So putting that in this context I
7 certainly think that any time there is an adverse
8 consequence to an individual that we get to the
9 point where there is room for a judicial
10 intervention, an independent intervention.

11 That's why I sort of like what the
12 President has done in adding the reasonable
13 articulable suspicion trigger to the querying of
14 the 215 database because that's the point at
15 which some individual becomes, you know, out of
16 the mass pulled out for individuated scrutiny,
17 and that's the point at which he begins to at
18 least suffer the risk of inaccurate adverse
19 consequences. And so I sort of like that as a
20 transition point.

21 MS. WALD: Good.

22 Mr. Felten, you talked about the

1 tendency for institutions, including the
2 government, to build ever larger databases and
3 then to aggregate them. And I think you've said
4 either today or in some of your writings that
5 there are inherent risks to privacy interests
6 when the databases get larger and larger, and
7 especially when they aggregate them.

8 So I guess my basic question to you is,
9 what are the principles, and we'll all take notes
10 on this, what are the principles that you
11 recommend as a computer expert for protecting
12 privacy in the increasing use of technology in
13 this field?

14 I mean all along the way from
15 collection, aggregation, whatever you think, if
16 somebody wanted to design a system in broad
17 concepts that maximize privacy but took adequate
18 concern for security, what would they look to?

19 MR. FELTEN: Sure. Well, I think the
20 first principle would be to try to look beyond
21 the most brute force technological approach,
22 which is collect all the data that might turn out

1 to be useful and retain it all in a single large
2 data center for as long as you can.

3 The more data you have, the more you
4 collect, the greater the adverse consequences
5 could be, the greater the risk and the more of a
6 target it is, either for abuse or for breach.

7 So the first principle is to try to fit
8 the practices to the specific, to think in terms
9 of what kind of analysis it is that you know you
10 need to do and figure out which data you can
11 collect and how you can structure a system in a
12 way that can do that analysis, while collecting
13 less data, holding the data more separately and
14 pre-processing or minimizing the data first.

15 And there's a growing array of technical
16 methods that can do this. And unfortunately,
17 this becomes a technical problem.

18 So the key principle here is simply to
19 insist that that technical work be done to try to
20 architect a system to collect and hold a minimum
21 of data.

22 MS. WALD: Who should do that, the

1 government or private industry?

2 MR. FELTEN: In my view if, say, a
3 government agency wants to argue that they have a
4 need to collect and use certain data, there
5 should be some onus on them to justify the
6 technical practices they're using to justify the
7 amount of data collected, the way they're
8 organizing it and so on.

9 That those who would argue for a
10 collection and use of data should be prepared to
11 discuss these issues and offer a technical
12 justification.

13 When it comes to private parties that's
14 a more complicated discussion. I think that the
15 best practice in industry ought to be to do that
16 as well, although obviously the legal and market
17 mechanisms that drive that relationship are very
18 different.

19 MS. WALD: My last question I'm going to
20 throw out, and you can all take a whack of it if
21 you want to, but several of you, and I think you
22 especially, Ms. Goitein, have talked about the

1 element of control of information as being
2 essential, but then some other people have
3 written in the field said, well, that certainly
4 can't be an absolute value. There's got to be
5 balance. I mean we wouldn't be able to have the
6 kind of national security programs if indeed
7 everybody said, well, I'm keeping control over
8 that piece of information because I don't want
9 anybody to have it, etcetera.

10 So what kinds of principles do you
11 apply? Because I assume you recognize that some
12 balancing, even as Paul pointed out that even in
13 the Fourth Amendment there's an unreasonable
14 clause which gives you a kind of a balancing to
15 talk about, so how would you handle that?

16 And then everybody can take a whack at
17 it, and then my panelists will take some more
18 whacks.

19 MS. GOITEIN: So as I said before, I
20 think in the vast majority of circumstances, and
21 that's the way it should be anyway, the drafters
22 of the Fourth Amendment did that balancing for us

1 and gave us what the government had to do to
2 override the privacy right, and that is to show
3 probable cause of criminal activity.

4 There are some very narrow exceptions
5 that the Supreme Court has recognized, some of
6 which are controversial, some of which are not.

7 And again, so we're not starting from
8 scratch. We have to follow the Supreme Court
9 case law here. We can't just say, well, I think
10 this particular search was reasonable, even
11 though there wasn't a warrant. If it doesn't
12 fall within one of the delineated exceptions for
13 the court, you have to get a warrant based on
14 probable cause.

15 Within those exceptions there is for
16 balancing, and that's part of the reasonableness
17 analysis. What I would say about that is, first
18 of all, the courts do their balancing when they
19 do a review.

20 But Congress has a role as well. And
21 when Congress does the balancing on behalf of the
22 people, I would agree with what I believe Dan

1 said, which is that this is a choice for the
2 public to make. This needs to be a public choice
3 and it needs to be an informed choice, not a
4 choice that's made in secret by a small number of
5 officials, but by the public, because this is a
6 democracy.

7 So we need to have the information about
8 what the security is, how that threat could be
9 mitigated by the collection of this information,
10 and what exactly is going to be the effect on
11 either side.

12 The other quick point I would make is
13 that in balancing tests national security is too
14 often a trump card. The words are uttered and
15 we're done.

16 And Julian Sanchez from the Cato
17 Institute made an excellent point, which is when
18 you look at how courts weigh national security
19 against the individual interests in question,
20 they tend to weigh national security writ large
21 over that person's particular interest in that
22 information. And that's not the right

1 comparison. You either need to weigh that
2 person's particular interest in that particular
3 information against the incremental threat to
4 national security in that case, or you need to
5 address national security writ large, weigh
6 national security writ large against the values
7 that privacy serves in our society.

8 And when you think of it that way,
9 national security really shouldn't be a trump
10 card.

11 You know, we talk about these values as
12 being in competition. I think the evidence for
13 the most part shows that targeted surveillance is
14 more effective than dragnet surveillance. But
15 when they are in conflict there needs to be a
16 fair and public balancing.

17 MS. WALD: Okay, thank you. Some other
18 comments? I'll let everybody have a shot at this
19 so we can go down the line. We'll start at that
20 end with you.

21 MR. FELTEN: Okay, thanks. I think in
22 thinking about these issues of control, it's

1 important to recognize the ways in which people
2 try to reassert control, even if they don't have
3 it legally.

4 And I'm referring specifically to
5 technical self-help measures that people use to
6 try to limit the flows of information, to try to
7 obfuscate identify and behavior, as well as
8 strategic behavior in which people avoid doing
9 certain things or deliberately do certain things
10 in order to present a different kind of image to
11 whoever it is that they worry is looking at their
12 data.

13 And these things have substantial costs.
14 And I think if you're trying to do a kind of
15 utilitarian balancing like Paul was talking
16 about, you need to take into account the ways in
17 which resources are spent and sometimes are
18 really wasted in a kind of arms race between
19 self-help and strategic behavior on the one hand,
20 and attempts to overcome that on the other side.

21 And those costs can often be
22 substantial. Just ask any teenager about their

1 online use and what you'll hear, and privacy, and
2 what you'll hear is an elaborate story about
3 technical countermeasures and strategic behavior.

4 MS. WALD: Paul?

5 MR. ROSENZWEIG: I think your point is
6 generally well taken, which is to say that
7 fundamentally the notion of control is at odds
8 with government collection of information,
9 whether it's for the purpose of imposing a tax
10 under the IRS, or law enforcement, or national
11 security.

12 That doesn't mean that it's not an
13 important value. It is one that many would
14 advance, and I see no reason to discount that at
15 all.

16 But in some ways if you advance that as
17 the touchstone of what you mean by privacy,
18 you're setting privacy ineluctably in opposition
19 to effective government action in a host of areas
20 where people might reasonably want to control.

21 You know, I'm sitting here as a
22 Republican on the panel thinking of all the

1 friends I have who are Second Amendment people
2 who think that the government should not collect
3 any information about their gun ownership. And,
4 you know, that's a perfectly reasonable position
5 for them to have. It's not one that we currently
6 accept as society.

7 And then the last point I would make,
8 which is just in response to Liza, because she's
9 mentioned it twice, but when I was last in
10 government the percentage of searches that were
11 conducted without warrants was actually quite
12 high, on the order of 50 percent.

13 Now I don't know if that's changed much
14 because it's been a while since I've been a
15 prosecutor, but many, if not most of our typical
16 interactions with law enforcement are adjudicated
17 on an ex-post reasonableness standard rather than
18 an ex-ante warrant standard.

19 I don't actually have the data so I
20 can't say more about it than that, but I
21 certainly seem to recall that it's not always a
22 pre, as opposed to a post activity, judicial

1 review.

2 MS. WALD: Dan, you have the last word.

3 MR. SOLOVE: Sure. A few really quick
4 points. First of all, even if you can't always
5 give people a total control, there are certain
6 partial things that we can give people for
7 control.

8 And the other thing is that it's not
9 just people being in control, it's that the uses
10 and gathering of the information is under
11 control. And that's another important thing
12 about it, that there's appropriate oversight and
13 accountability and controls on that gathering
14 too.

15 On the Fourth Amendment, I think that it
16 would be wrong just to track existing Supreme
17 Court interpretations of the Fourth Amendment,
18 which I think are a lot of times flawed in a lot
19 of cases.

20 In fact, I think there are a lot of
21 exceptions to the warrant requirement, a lot of
22 instances where the Fourth Amendment doesn't even

1 get applied at all because the court has this
2 platonic conception of privacy that is incredibly
3 narrow.

4 And that's how we get the third-party
5 doctrine and how we get a lot of bodies of Fourth
6 Amendment law that often take the Fourth
7 Amendment away from any kind of approach.

8 Now the Fourth Amendment, I think, is a
9 utilitarian balancing. It says basically the
10 right to be secure against unreasonable searches
11 and seizures. It actually doesn't say privacy,
12 it says actually a right to be secure against
13 unreasonable searches and seizures.

14 And I think that means that any time the
15 government is engaging in searches, and
16 surveillance, and gathering information that it
17 is unreasonable if it's creating problems that
18 are not adequately dealt with the right amount of
19 oversight and accountability.

20 And that's really what the Fourth
21 Amendment is trying to impose there, either
22 justification to gather information, such as a

1 warrant and probable cause, or appropriate
2 oversight to make sure that an independent
3 judicial body looks at what the government wants
4 to do and evaluates it.

5 I think it's very important that we
6 conduct the balance between privacy and security
7 appropriately.

8 I'm not a privacy absolutist, I think
9 that there should be a balance. But I think it's
10 very important that when we balance, we balance
11 it correctly and not incorrectly, and that we
12 don't skew the balance too much to the security
13 side by overweighing the security interests,
14 because it's not the entire security interests on
15 the scale.

16 It's the marginal difference between a
17 security interest without certain kinds of
18 oversight and accountability, and the security
19 interests with oversight and accountability.

20 And I think all branches should be
21 playing a role and have a role to play in this.
22 Congress in the 1970s at the Church Committee,

1 which did an extensive review of intelligence
2 agencies, produced a very illuminative public
3 report about that.

4 Congress hasn't done anything quite like
5 that since. I think it should.

6 I think the judiciary has a role to
7 play. I think this body has a role to play. I
8 think the people ultimately also are the key to
9 all this. They have a role to play.

10 MS. WALD: Thank you. We're now going
11 to have 20 minutes of questioning from my fellow
12 Board members, and I think I'll start with the
13 Chair.

14 MR. MEDINE: Great, thank you.

15 Liza raised a question about the proper
16 standard for privacy and referenced the Katz
17 decision essentially, on expectation of privacy
18 and how in some ways people rely on practical
19 obscurity because the government is too complex
20 or burdensome to gather information.

21 In some ways in the computer age we're
22 beyond that, which is that the court file that

1 was gathering dust now is easily accessible and
2 public.

3 The question is, how should we look at
4 privacy issues when public databases are so
5 readily available?

6 And there's also a reference to the fact
7 that the line between government and commercial
8 databases isn't always great and the government
9 can access commercial databases.

10 So how do we look at privacy when the
11 information is out there, it is publicly
12 available, but yet, as Ed pointed out, you
13 combine it into a mosaic and it can create a very
14 detailed profile, and should the government be
15 collecting that information?

16 So what standard should we apply in this
17 context? What's the Katz 2014 version as far as
18 how the government ought to recognize privacy
19 issues?

20 And I'm happy just to go down the line.

21 MS. WALD: Well, whoever wants to take
22 it. I might note that time-wise, we're going to

1 have about five minutes per, so if you can keep
2 your answers or your comments relatively brief,
3 we can make sure that everybody gets their full
4 component of time.

5 MR. SOLOVE: I'll be super-brief. I
6 think that right now what's been known as the
7 mosaic theory that we see in the concurrences to
8 the Jones case in the Supreme Court are starting
9 to look at this very question.

10 I can't really answer it in a few
11 seconds, but I think it's to look at when we
12 combine various pieces of data, what are the
13 implications of that and when does the combining
14 of that data reveal new information that can
15 create certain problems and harms to people, and
16 that's where we want to step in.

17 MR. ROSENZWEIG: I'd make two quick
18 points. The first is of course that practical
19 obscurity is itself a sort of a post-industrial
20 concept.

21 If you were in a medieval village back
22 in the 1200s there was no practical obscurity.

1 You were limited to who you knew and they knew
2 everything about you, pretty much. The data
3 aggregation system was the coffee klatch where
4 everybody talked to each other.

5 So in advancing practical obscurity
6 we're advancing a value that has come to be
7 something that we value more now, one that I
8 agree with.

9 I think Dan's exactly right, the mosaic
10 is real. To deny that is to deny the reality of
11 the science that Ed knows.

12 So it strikes me that the most likely
13 points of intervention are either at the
14 collection, or at the aggregation, or at the use
15 of the aggregated data.

16 I tend to think you can't do it at
17 collection because the databases are there.
18 They're so big it's impossible to stop. Unless
19 you're going to stop Google from collecting,
20 we're going to have big data collection.

21 So it's got to be when the government
22 chooses to aggregate it or perhaps chooses to act

1 upon the aggregation. And as between those, I
2 don't have too much choice.

3 MS. GOITEIN: Just a quick note, I agree
4 with most of what's been said in terms of the
5 mosaic theory.

6 I mean another way to look at it is just
7 that the information that's being gathered by the
8 government is, in fact, information that using
9 normal powers of human observation would be in a
10 person's control and would not be something the
11 government would have access to.

12 The one thing I would say is that I
13 don't agree that the point of collection is a
14 moot point because the mere fact that Google has
15 all of this information and Facebook has all of
16 this information does not mean that the
17 government has all of this information.

18 And there are burgeoning new
19 technologies that their use has not been decided,
20 such as UAVs and how the government will be
21 allowed to deploy UAVs. So there's still plenty
22 of room to regulate at the collection phase.

1 And for all the reasons we discussed
2 earlier about chilling effect and about what
3 privacy means to different people, I think that
4 is the point at which the privacy interests
5 arise.

6 MR. FELTEN: And I'll be very brief as
7 well. Along with what the other panelists have
8 said, I'd also point out that much of the
9 information that is in corporate databases is
10 information that was observed rather than
11 disclosed, and there's not always consent, or at
12 least often consent is very thin from the person
13 who the data is about.

14 And so I don't think you can always
15 infer that there was an awareness. You can't
16 infer from the fact that information is in, say,
17 a corporate database that a user was aware that
18 it was collected or that they were aware that it
19 might go to the government and be used for
20 government purposes.

21 MR. MEDINE: And therefore should the
22 government not collect the information under

1 those circumstances?

2 MR. FELTEN: Well, I hesitate to make a
3 legal opinion here, not being a lawyer.

4 MR. MEDINE: As a policy matter.

5 MR. FELTEN: As a policy matter?

6 MR. MEDINE: Yes.

7 MR. FELTEN: But I should say that as a
8 policy matter I get very nervous when it appears
9 that there is a legal fiction that something has
10 happened when it's clearly not happening. So a
11 fiction of consent or a fiction that the mosaic
12 effect doesn't exist are troubling.

13 MR. MEDINE: My time has expired.

14 MS. WALD: Rachel Brand.

15 MS. BRAND: Thank you. Thank you all
16 for being here, first of all.

17 Going back to this notion of control
18 that Judge Wald was asking about, Ms. Goitein,
19 you went to the Fourth Amendment concept. I'm
20 interested in whether the notion of control
21 that's embodied in the FIPPs, which is more of an
22 individual participation concept, can apply in

1 the national security surveillance context.

2 So I think one of you noted that maybe
3 no individual would say, yes, I consent to being
4 surveilled by the NSA, or the FBI, or anybody
5 else, and if that were the standard then you
6 couldn't have surveillance programs.

7 And the FIPPs is on top obviously of
8 whatever the Fourth Amendment baseline is. FIPPs
9 would impose on government agencies additional
10 restrictions.

11 Can that kind of notion apply at all in
12 the national security context? What's your view
13 on that?

14 MS. GOITEIN: I think it can apply but
15 I'm just sort of pausing because I'm thinking
16 about some of the premises of the questions.

17 It's not the case that you couldn't have
18 surveillance programs if people didn't consent to
19 the disclosure of their information. The
20 government can obtain your information with a
21 warrant based on probable cause.

22 MS. BRAND: No, no, my point is that

1 we're beyond the Fourth Amendment now. We're
2 layering on top of the Fourth Amendment the FIPPs
3 individual participation notion.

4 And the reason I ask is because, for
5 example, when the NSA published their report on
6 targeted data collection under 12333, they said
7 that they were applying the FIPPs, but then they
8 turned right around and said, but the individual
9 participation concept doesn't apply so we're not
10 applying that part of it.

11 So what I'm wondering is whether the
12 FIPPs is just not the right, I don't know,
13 framework to apply in this context. That's what
14 I'm trying to get at.

15 Is it, does this individual
16 participation thing just not apply and should we
17 look for some other framework or standard to use?
18 That's what I'm getting at.

19 MS. GOITEIN: Actually if you wouldn't
20 mind I'd like to think about the question.

21 MS. BRAND: Okay.

22 MS. GOITEIN: I have some thoughts but I

1 want to think about it a little more and maybe I
2 can put it in writing along with my testimony.

3 MS. BRAND: Okay.

4 MR. SOLOVE: I have a thought on it. I
5 think the FIPPs model has some flaws to it. You
6 know, a lot of times people don't read the
7 privacy policies, in most cases, of companies.
8 And I'm not sure just providing a notice is
9 effective.

10 So we do need to think about what works
11 in this context. I think that the key is in
12 certain cases we might want individuals to play a
13 greater role. I think the TSA, if you're on the
14 no-fly list, I think you should have a right to
15 be heard. There should be rights of redress
16 there and to challenge your being on that list.

17 So I think there some of the FIPPs make
18 a lot of sense. Some of the FIPPs like security
19 I think make sense. Other ones might not.

20 But I think the larger component of all
21 this is that there's adequate control and
22 accountability, which is also part of the FIPPs.

1 So while everything in the FIPPs, such
2 as an individualized notice of every time
3 information is collected is not really feasible,
4 there are certain things.

5 There's a greater transparency right in
6 the FIPPs too, not that individuals get notified
7 about every collection about them, but that
8 there's a public accountability and a generalized
9 disclosure about what's going on.

10 MR. ROSENZWEIG: I thought that the
11 acknowledgement in the NSA report that some of
12 the FIPPs principles simply could not be fully
13 implemented in the context of a national security
14 surveillance program was an absolutely accurate
15 acknowledgement of reality.

16 You can't provide error collection
17 notice in all circumstances. I certainly agree.
18 I mean was talking more about the secondary
19 screening than the no-fly list where we do have
20 more robust rights.

21 But the challenge for you is going to be
22 trying to figure out what the underlying values

1 are and how to get at those.

2 So in this context I think the
3 underlying value is prevention of governmental
4 abuse, that's what animates everybody in this
5 sphere, and government surveillance modifying
6 behavior.

7 And the types of accountability and
8 transparency that you have to help build are ones
9 that match the operational needs of the national
10 security system, while providing protections
11 against that.

12 We tried that with the intelligence
13 committees and the post-Church Commission
14 modifications, something that we might call kind
15 of delegated transparency where we all trust the
16 Congress to do it right.

17 It seems as though we're less willing to
18 do that now. Personally I'm not so certain that
19 that's a good impulse, but it seems like that.

20 So maybe it's this Board. Maybe it's a
21 judicial panel with a cleared advocate in front
22 of it.

1 There are lots of mechanisms, short of
2 the complete transparency and accountability and
3 individual participation that are part of FIPPs
4 that could be imagined that would achieve the
5 objective of controlling against governmental
6 abuse and misuse, while not completely
7 frustrating the operational necessities that I
8 think most of us see as remaining regnant.

9 So I think a lot of it would be things
10 that are more in Ed's bailiwick, which are
11 thinking about what the use case scenarios that
12 are legitimate are in advance and building in
13 enhanced privacy protections on a technological
14 level. And then you can have as much of your
15 cake as you want and still get to eat some of it.

16 MR. FELTEN: To the extent that
17 particular principles from the FIPPs might be
18 difficult or impossible to apply in this kind of
19 setting, it seems there should be a greater
20 obligation to further the goals of that
21 principle.

22 So, for example, if you can't offer the

1 right to control or correct errors in the data,
2 you could imagine asking for greater effort to
3 ensure the correctness of the data as it is, or
4 extra safeguards ex-post regarding the
5 possibility of error.

6 MS. BRAND: Thank you.

7 MS. WALD: Okay. Did you collect any
8 thoughts that you, very briefly --

9 MS. GOITEIN: Yes, and I think I would
10 agree with Ed. I mean part of what I was
11 struggling with is how much are we giving up on
12 this sort of collection, which I'm not quite
13 willing to do, in talking about sort of, you
14 know, post-collection? And that's why I wanted
15 to go back to that issue of surveillance and
16 control over the information.

17 I still want to go back and look more.
18 This is honestly something I just haven't thought
19 about enough and so I do want to go back and, you
20 know, look at FIPPs, which I used to use all the
21 time when I was on the Hill to craft our privacy
22 amendments, but I want to go back and look more

1 carefully.

2 But, you know, it sounds to me like the
3 best approach is a modified version of the FIPPs,
4 but I want to look more closely.

5 MS. WALD: That's fine. We'll be glad
6 to receive any later submissions from any of the
7 panelists.

8 Before we go on to Beth Cook's questions
9 I want to remind the audience that if you have
10 any questions, write them down and they'll bring
11 them up to me and then I will -- okay, they're
12 coming, that's good to know.

13 Okay, Ms. Cook.

14 MS. COLLINS COOK: So thank you all for
15 what I've found to be a very, very interesting
16 panel. I hope it bodes well for the rest of the
17 day.

18 And in fact, a lot of, I think panel 3
19 will be dealing exactly with how you translate
20 the FIPPs, is that the right transition, does
21 that really work in the government context.

22 But I was also struck by the numerous

1 mentions of mosaic theory because there are
2 obviously other implications of the mosaic
3 theory.

4 One bears on transparency, which is to
5 the extent that we are transparent in seemingly
6 discreet ways, our adversaries are also looking
7 to aggregate information about sources and
8 methods.

9 The other is that the national security
10 establishment I think would argue that the mosaic
11 theory is critical. You need to understand
12 mosaic theory to understand collection, to
13 understand exactly how the national security
14 apparatus works, that they have to be able to
15 aggregate information.

16 You can agree or disagree, but I think I
17 was struck by the different implications of the
18 mosaic theory.

19 So I wanted to start with you, Professor
20 Felten, and I was really interested in your
21 notion of moving away from the brute force
22 collection mechanism.

1 And I think the Section 215 program is
2 one that the government had made the argument
3 essentially that they need the brute force
4 collection, they need to have the retention in
5 order to identify previously unknown links and
6 information.

7 Have you given thought as to whether or
8 not there are technological options available to
9 limit collection for a program like Section 215?

10 If you haven't, then more generally if
11 could you be more specific about collection
12 options.

13 MR. FELTEN: Yes. Well, with respect to
14 Section 215, the data of course is collected
15 initially by the phone companies, right? And
16 there's the question of whether the information
17 needs to be transferred in bulk to the
18 intelligence community in order for them to be
19 able to do their analysis.

20 And I think it's pretty clear that as a
21 technical matter the kinds of linking, looking
22 for, say, multi-hop links that the intelligence

1 agencies want to do, can be done technically
2 while the information is still held by third
3 parties such as the phone companies.

4 This requires a modest amount of
5 technical coordination between the companies, the
6 entities holding the data and the entities that
7 are doing the analysis.

8 So there are opportunities to match, to
9 look for whether there are paths of two hops or
10 three hops from point A or point B, etcetera, and
11 then to reach in and extract just the data items
12 of those individuals or phone numbers that are
13 highlighted by that kind of analysis. That's the
14 kind of thing that can be done.

15 There's further work that is more
16 technical that goes to questions of whether you
17 can use, say, advanced cryptography to allow that
18 same analysis, while not disclosing to the phone
19 company information about which numbers are being
20 searched or linked.

21 And those sorts of methods are, I'd say
22 developing, and there's been some interest in the

1 technical problem of how to do this in the
2 independent research community in light of what
3 we've learned publicly about the Section 215
4 program.

5 And one of the lessons of that is that
6 methods are often available or developable when
7 you have a specific technical problem like this.

8 MS. COLLINS COOK: I think our biggest
9 challenge is taking the concepts that we're
10 talking about today and developing practical,
11 feasible recommendations that can actually be
12 implemented.

13 So the more concrete and the more
14 specific that we can be in terms of
15 recommendation, the more likely they are to be
16 implemented.

17 Briefly, both to the professors in the
18 middle I would ask, you both talk a little bit
19 about risk mitigation, and assuming that there
20 are going to be harms, how do you mitigate those
21 harms past the collection stage?

22 What have you found to be the most

1 effective mechanisms for mitigating risk? Is it
2 retention periods? Is it access controls? Is it
3 audit trails? So what can the government do
4 concretely to start mitigating risks?

5 MR. SOLOVE: Well, I think it's not
6 really just one thing that I can sort of point to
7 like, that is it. It's all of those things are
8 very valuable to do, everything from mechanisms
9 to ensure that this information is accurate when
10 information is grabbed from one context to
11 another.

12 You know, what's accurate enough for the
13 purposes of Amazon.com to recommend books for you
14 is not the same level of accuracy we might want
15 from the government. So if Amazon makes a
16 mistake and recommends the wrong book to you, big
17 deal. It doesn't need a hundred percent accuracy
18 for that.

19 But the level of accuracy differs as we
20 differ in context. So we need to have mechanisms
21 to make sure that when information might be taken
22 from one context and put into the other that it's

1 appropriately accurate for that particular
2 context.

3 We need an analysis of how long we keep
4 the data, audit trails to make sure that it's not
5 being improperly accessed, appropriate
6 accountability to make sure it's being kept
7 adequately secure, and also how it's being used,
8 controls on its use so it can't be used for any
9 purpose ten years from now.

10 So we need all these different things,
11 and oversight from a lot of different bodies, I
12 think. So it's actually a complex thing with
13 many, many parts.

14 MR. ROSENZWEIG: There are certainly
15 many moving parts, but from my perspective both
16 from outside and when I was inside, since the
17 threat that we're talking about is governmental
18 abuse or misuse is the primary one, the principal
19 factors that I would focus on that seem to have
20 been effective were ones that focus on the
21 individual government actors.

22 Training in the first instance so that

1 they know the rules, inculcating a culture of
2 compliance that is pre-error mechanisms, then
3 obviously a lot of audit compliance work from
4 outside inspectors general and/or Congress.

5 And then finally, and this is perhaps
6 where we fall down the most, the willingness to
7 impose at least administrative sanctions on
8 people who vary from the accepted rules, at least
9 in a willful context, and even perhaps in a
10 negligent context.

11 You know, nothing attracts the attention
12 of a government employee so much as the prospect
13 of losing his job or being suspended for a term
14 of months. So that would be where I would focus.

15 MR. FELTEN: If we look at the failures
16 of compliance that have been acknowledged, we see
17 some of them that are individual employees doing
18 things they shouldn't, but we've also seen some
19 that are failures of the technical systems to
20 behave consistently with the internal policies.

21 And this is a case where oversight can
22 operate without needing to get deeply into the

1 nuts and bolts of the technology, just the
2 question of what processes are in place to make
3 sure that your technology does what your general
4 counsel says it should do. And I think there's
5 an opportunity to push on oversight in that area.

6 MS. WALD: I think we'll move to Jim
7 Dempsey now.

8 MR. DEMPSEY: Thank you, and thank you
9 to all the witnesses. I think it's very
10 important as we wrap up this panel to highlight
11 what I at least heard is an awful lot of
12 commonality.

13 Because I think that it's important to
14 the Board and important for the public debate
15 moving forward not to end up with the proposition
16 that this is all so confusing, or this is all
17 disparate, there are so many different views.

18 I heard actually a lot of commonality
19 among the witnesses, starting with the point that
20 I think you all agree, whether you start from the
21 premise that privacy is a human right or whether
22 you start from the premise that it's an

1 instrumental right, I think all of you agree that
2 it's an umbrella term which covers many different
3 values, many different interests.

4 And I also heard agreement that the
5 mosaic theory, even if it hasn't been accepted by
6 courts, is real. It's real, both from a privacy
7 perspective and it's real from the governmental
8 perspective.

9 MS. GOITEIN: Let the record reflect
10 nodding.

11 MR. DEMPSEY: And thirdly, I think I
12 heard unanimity that what the law refers to at
13 least as the third-party doctrine, the doctrine
14 that by giving information to one person you lose
15 all interest, all privacy interest in that
16 information, that disclosure to one surrenders
17 your right with respect to disclosure for any
18 other purpose, again, am I right there was
19 agreement that that concept of disclosure to one
20 is disclosure to all is not valid,
21 constitutionality aside, for modern day reality,
22 that doctrine just doesn't fit with the way we

1 view information and the way we view privacy?

2 And Dan is nodding. Paul, would you
3 agree that disclosure to one is not a surrender
4 of all interest in the information?

5 MR. ROSENZWEIG: I would say that the
6 way that people interact today it would be
7 inappropriate to imply consent to universal
8 disclosure from explicit consent to disclosure to
9 a single person, yes.

10 I'm not sure that I would agree with
11 what's implicit in your question, which is that
12 it necessarily follows that that is a matter of
13 either constitutional significance or one of
14 legal cognizable significance that should animate
15 this Board. I want to think about that.

16 But I would certainly accept the premise
17 that human experience is that if I tell Dan a
18 secret, I'm not expecting him to tell everybody.

19 MR. DEMPSEY: In fact, there's an
20 instrumental approach, there's an instrumental
21 value that the disclosure of your medical records
22 to the doctor is specifically premised on the

1 notion that they are, thereby you have not
2 surrendered your privacy rights. And in fact, we
3 want people to accurately disclose information to
4 their doctors, therefore we promise them that
5 their medical records, disclosure to the doctor
6 is not disclosure to all.

7 MR. ROSENZWEIG: That's true, though of
8 course that's a wonderful example because we
9 accept statements made to a doctor as an
10 exception from the hearsay rule precisely because
11 we think that when you talk to a doctor in an
12 emergency situation you're motivated to actually
13 be telling him the truth. I was shot, doc. And
14 so the doctor can in some circumstances be
15 compelled to. So those realities work both ways.

16 MR. DEMPSEY: Can be compelled but not
17 obviously --

18 MR. ROSENZWEIG: Not obviously
19 collected. Not collected under, yes, HIPAA.

20 MR. DEMPSEY: Right, yes.

21 Also there were several witnesses
22 mentioned the FIPPs. And I think it's, first of

1 all, important to say we're talking about the
2 Fair Information Practice Principles, which
3 actually there's no definitive version of them.

4 But there is a version that was adopted
5 by the Department of Homeland Security in 2008,
6 which is as good as any, I think.

7 And it seemed to me also that there was
8 agreement that they are, the FIPPs framework
9 provides the framework, the questions.

10 They're nowhere perfectly implemented,
11 they're nowhere fully implemented, but they are
12 relevant as a framework for asking about how you
13 deal with information.

14 And then you decide, do you adjust it,
15 does it work? If it doesn't work, do you
16 compensate for it with more emphasis on other
17 issues? Is that again a fair --

18 Paul, you're making a somewhat skeptical
19 face, but you at least can say that it is a
20 framework for asking the questions.

21 MR. ROSENZWEIG: It's a framework for a
22 starting point for asking the questions, but I

1 think that many of those questions don't
2 withstand the technological transitions we're
3 going through.

4 And so I accept it as a leaping off
5 point, but I think I'm probably more willing than
6 some of the other members of the board to discard
7 some of them as inoperable under current
8 circumstances.

9 MR. DEMPSEY: And what would you replace
10 them with?

11 MR. ROSENZWEIG: Well, as Ed said,
12 emphasis on the remaining aspects and then, to my
13 mind, I think kind of a more granular analysis of
14 the underlying interests at stake and thinking
15 about what the mechanisms are, the privacy
16 interests that we're talking about is that we
17 have to protect.

18 Because, you know, FIPPs is kind of one
19 size fits all, and I just don't think it kind of
20 covers the range of the privacy interests that
21 the chairman outlined so ably, so ably, earlier
22 in the day.

1 MR. DEMPSEY: Okay, thank you.

2 MS. WALD: Okay. We have a couple of
3 questions from the audience. I'm not sure we're
4 going to get to all of them, so what I'm going to
5 do is direct them. I'll just be arbitrary and
6 direct them to a particular panel member, and
7 then if you can keep it as brief as you possibly
8 can.

9 The first one, actually the writer
10 wanted it directed toward you, Ms. Goitein. When
11 a government draws data from private databases,
12 such as telephone metadata, at which point of
13 collection is more regulation required, the
14 private entity's collection or the government
15 collection from the private entity?

16 That's a yes or no.

17 MS. GOITEIN: I was going to say, I
18 don't think I can answer that question. It just
19 depends what you mean by more regulation.

20 I think obviously when you disclose
21 certain information to your telephone company,
22 you are in a contract with that company and that

1 contract regulates your dealings with the
2 company.

3 I think one of the problems with the
4 metadata program is that there was no reading of
5 either the contract or Section 215 of the PATRIOT
6 Act that would have enabled any person to know
7 what they were consenting to and to know that
8 their information would then go to the NSA.

9 MS. WALD: Your answer is both?

10 MS. GOITEIN: It's both. There's just
11 different types of regulation. There's the
12 contractual regulation.

13 There is some degree, I mean the Stored
14 Communications Act is government regulation, when
15 you get certain kinds of information from the
16 telephone company.

17 And then for the government there's the
18 Fourth Amendment. And there's all manner of
19 laws, so lots of regulation everywhere. I know
20 that's --

21 MS. WALD: Okay, for you, Dan. I think
22 it was Liza Goitein that said that private

1 companies have no incentive to coerce or imprison
2 people, that's why perhaps the risks of injury
3 might be greater from the government than from
4 private companies.

5 But the writer asks, does that take into
6 account the homeland security and prison
7 industries? NSA couldn't do what it does without
8 484 contractors providing IT technical support.
9 Are there risks inherent in the increasing
10 commercialization of national security?

11 MR. SOLOVE: Well, yes, I definitely
12 think problems can come from anywhere, and I
13 don't think there's sort of inherent things that
14 can be said about, you know, various things about
15 where problems could be caused.

16 I think we want to look at, you know,
17 when does the collection and the amassing of data
18 by the private sector cause problems? When does
19 that access by the government create problems?

20 And increasingly we see a cooperation or
21 an industry in the private sector that has grown
22 up to basically perform government functions and

1 help gather data, help analyze data and then
2 share data with the government.

3 I think all these things create various
4 problems that we need to address. And so I think
5 if we both keep our eye on the problems and stop
6 looking elsewhere and just look at the problems,
7 and we address those problems wherever they may
8 happen, I think that's the best approach.

9 MS. WALD: Okay. Here are two, I think
10 this must go to you, Ed Felten, could the
11 panelists discuss what they think their Tesla, I
12 had to ask what that was, of today should
13 provide, what technologies of data flow analysis
14 could or should be built in?

15 I know you've covered a great deal of
16 this before, so if you could just give us a one
17 or two sentence summary on it, that would be
18 fine.

19 MR. FELTEN: In a sense the question is
20 asking me to sum up sort of a whole area of
21 knowledge in a few seconds, which I won't try to
22 do.

1 I'd simply say that as with cars, as
2 with the Tesla, you know, some sort of high end
3 car, you should think in terms of which
4 technologies are available and reasonably
5 practical to use to minimize, or control, or
6 limit the risk of certain information practice,
7 and then ask that those be there.

8 You should ask that an entity that wants
9 to collect and use the information be willing to
10 justify the choices they've made and be willing
11 to justify why they did not use some accepted
12 technical, privacy-preserving technical method if
13 it seems to be available.

14 MS. WALD: Okay. The last one is, Paul,
15 I don't think this is in your natural bailiwick,
16 but I'll pick you anyway.

17 MR. ROSENZWEIG: Okay.

18 MS. WALD: What about the application of
19 privacy in quasi-federal organizations like the
20 Postal Service or the PBGC?

21 If I can remember back to my old
22 judicial background, that's something benefits

1 guarantee corporation.

2 MR. MEDINE: Pension benefits.

3 MS. WALD: Pension Benefits Guarantee
4 Corporation. How are they impacted by the Fourth
5 Amendment? Are there issues and concerns for
6 privacy in those organizations?

7 MR. ROSENZWEIG: I suppose the honest
8 answer would be I'm not sure. But my
9 understanding is that the Fourth Amendment
10 applies to those institutions insofar as they are
11 exercising governmental authority and acting as
12 agents for the government.

13 So I assume that Postal Service
14 employees can't open your mail willy-nilly just
15 because they're pseudo-private actors. I may be
16 wrong about that, but since they don't open my
17 mail.

18 Jim's nodding, no, I'm right. So
19 thanks, that's good.

20 I think that the implication of the
21 question, which is really the most interesting
22 part of it, so I'll transition into something I

1 do want to talk about, is that it emphasizes the
2 point that Liza made, with which I do agree,
3 which is that the line between commercial
4 collection and government collection is
5 increasingly blurring some, you know, and the
6 idea that regulation of the government but no
7 regulation of Google's collection kind of sits in
8 dissonance. And there are these places that are
9 halfway between.

10 For me, you know, that suggests one set
11 of answers, because I'm unwilling to think about
12 wholesale government regulation at an extreme
13 level of corporate business practices. I think
14 there's some there, but it certainly emphasizes
15 the confluence between them.

16 MS. WALD: Okay. Well, that ends my
17 part of the panel, unless the Chair has some
18 parting words.

19 MR. MEDINE: Thank you very much.

20 MS. WALD: You've been extremely
21 forthcoming.

22 MR. MEDINE: Thanks to the panel and for

1 the audience questions.

2 We'll take a 10 or 15 minute break and
3 we'll resume at 10:30 with the technology panel.

4 (Off the record.)

5 MR. MEDINE: Thank you very much. We
6 will resume and Jim Dempsey will be moderating
7 this panel.

8 MR. DEMPSEY: Thank you, Mr. Chairman.
9 Good morning again to members of the audience,
10 particularly good morning to our second panel.

11 The title of our panel is Privacy
12 Interests in the Counterterrorism Context and the
13 Impact of Technology.

14 I have no statement of my own, so we can
15 go straight to the opening statements by the
16 witnesses. I'll introduce each of them in turn.
17 We can go down the row, which happens also to be
18 alphabetical order.

19 I remind the witnesses that we would ask
20 them to keep their opening remarks to seven
21 minutes. There is a timekeeper, which you might
22 not have seen, but in the front row here, Renee,

1 who will be holding up a yellow card for your two
2 minute warning and then a red card for time's up.

3 Thereafter a round of questioning by the
4 Board members, and again the possibility of
5 questions submitted by members of the audience.

6 PCLOB staff members throughout the
7 audience have little index cards, and so if
8 during the course of the panel a question occurs
9 to you, raise your hand and someone will bring
10 you over a little 3 by 5.

11 Our first speaker or member of this
12 panel is Annie Anton. She is a professor in and
13 Chair of the School of Interactive Computing at
14 Georgia Tech University. She has a Ph.D. in
15 computer science, and is one of the country's
16 leading experts on issues at the intersection of
17 technology and policy.

18 So, Annie, please.

19 MS. ANTON: Good morning and thanks for
20 the opportunity to testify.

21 We're in an ever changing world where
22 terrorists and criminals are getting smarter and

1 more sophisticated. Their offensive techniques
2 are surpassing our ability to protect our nation.
3 Providing strong technical protections for
4 privacy and civil liberties is a counterterrorism
5 weapon.

6 Today I focus primarily on three
7 technology considerations. First, strong
8 encryption is an essential technology for
9 fighting terrorism.

10 Second, de-identification, while not
11 perfect, may be a reasonable approach given a
12 thorough risk analysis.

13 And third, improved privacy threat
14 modeling is critical for counterterrorism.

15 Our national cyber infrastructure must
16 be resilient to attacks from foreign powers,
17 terrorists and criminals.

18 Requiring government backdoors in
19 commercial products, stockpiling zero-day
20 exploits and weakening software security
21 standards are all practices that weaken our
22 nation's cyber security posture and make it

1 easier for attackers to infiltrate these systems
2 for nefarious purposes.

3 The latest Apple and Google phones build
4 in encryption by default. Both companies are
5 configuring this encryption such that they cannot
6 decrypt the information for anyone, including law
7 enforcement.

8 These measures have been sharply
9 criticized by the Director of the FBI and the
10 Attorney General.

11 As a technologist, I can assert that
12 applying security best practices such as
13 encryption by default will yield a system that
14 can better withstand intrusions and denial of
15 service attacks, as well as limit access to
16 authenticated and authorized users.

17 Requiring companies provide backdoors
18 for law enforcement or national security hurts
19 both individual privacy and our nation's overall
20 security.

21 Moreover, the security benefits are
22 questionable at best because sophisticated

1 terrorists and criminals will simply use
2 international products or more secure, less
3 convenient alternatives.

4 Technology and policy scholars are
5 actively debating the merits of de-identification
6 and anonymization techniques. The issue is
7 critical because privacy rules only apply to
8 identifiable data. Technology scholars emphasize
9 that there is no way to mathematically prove an
10 anonymized data set, that it cannot be
11 re-identified.

12 In contrast, policy scholars believe
13 that anonymization provides real practical
14 protection to most of the people most of the
15 time.

16 Consider that the locks on your door at
17 home are pretty good, but not good enough to keep
18 a determined intruder at bay. That's the idea
19 behind practical anonymization.

20 There are some cases where it is
21 critical to protect a person's identity. For
22 example, for victims of domestic abuse we need to

1 ensure that their location is protected and
2 cannot be re-identified by their abuser.

3 However, in many settings, if we apply
4 effective but not perfect de-identification
5 procedures, overall privacy protection may be
6 increased and data may be more useful. In such
7 cases the perfect should not be the enemy of the
8 good.

9 The PCLOB might consider how to
10 determine in practice when agencies should insist
11 on technically strict de-identification versus
12 when effective, but not perfect,
13 de-identification may address the bulk of the
14 risk.

15 Finally, threat modeling is critical for
16 counterterrorism, and we must improve it to
17 achieve two goals.

18 First, we must develop privacy oriented
19 models. Most threat modeling techniques have
20 been developed entirely in a security context
21 with little privacy consideration. The latter is
22 crucial given the rise the big data analytics and

1 the Internet of things.

2 Second, as a nation we do not want
3 insiders leaking state secrets to foreign
4 journalists to become a common way to influence
5 public policy decisions and debates.

6 Insiders with access to sensitive
7 information must be considered as potential
8 threats simply because of the extreme damage that
9 a leak could do, either in direct cost by
10 providing useful information to enemies, or
11 indirect cost with respect to public relations or
12 erosion of trust. A good threat model makes risk
13 analysis feasible for any organization.

14 In closing, as a technologist and
15 privacy scholar I believe we should encourage
16 strong encryption by default, use practical
17 de-identification technologies now rather than
18 wait for theoretically perfect solutions, and
19 expand threat modeling to include privacy and
20 security as well.

21 In addition, Ed Felten mentioned the
22 importance of having technologists in the room.

1 I can't help but note that the review group did
2 not have a technologist that the PCLOB, which I
3 really appreciate all that you are doing, but
4 again, there isn't a technologist in the room.

5 And having technologists on panels is
6 helpful, but really I would like to see us move
7 forward to having more technologists actually
8 involved in the decision-making.

9 And so I'd like to thank the Civil
10 Liberties and Privacy Board for its commitment to
11 finding ways for the government to protect
12 privacy, and also for meeting our critical
13 security needs as a nation as well. Thank you.

14 MR. MEDINE: Let me just thank you for
15 your testimony, but actually we have a
16 technologist in the second row.

17 MS. ANTON: Great.

18 MR. MEDINE: And we have a technologist
19 outside as well. And so we actually do value the
20 role of having technologists and have two full-
21 time on our staff.

22 MS. ANTON: Good, and I look forward to

1 meeting them. Thank you.

2 MR. DEMPSEY: Thank you. Our second
3 witness is Alvaro Bedoya. Alvaro is the
4 Executive Director of the Center on Privacy,
5 Technology and the Law at Georgetown University
6 Law School and was previously chief counsel to
7 the Senate Judiciary Subcommittee on Privacy,
8 Technology and the Law. Alvaro.

9 MR. BEDOYA: Thank you. Good morning
10 and thank you for the opportunity to speak with
11 you today.

12 We have a problem right now in privacy
13 and it's a problem for government and industry.
14 Government and industry have developed
15 extraordinarily powerful data analysis tools.

16 These tools let them analyze data sets
17 that have previously been too large or too messy,
18 they let them process that data faster, and they
19 let them find latent value in data sets that have
20 previously seemed old and worthless.

21 In short, these processes create
22 enormous value, and that value is driving both

1 government and industry to collect as much
2 information as possible and to retain it as long
3 as possible.

4 The problem is, is that's hitting up
5 against long-established privacy values ingrained
6 in the FIPPs. The FIPPs encourage limited
7 collection, they encourage data minimization, and
8 the destruction of data that's no longer useful
9 for the purpose for which it was collected.

10 And so right now both in the
11 intelligence community and in industry there's
12 effectively an effort to redefine privacy.

13 Privacy used to be about collecting only
14 what you needed to collect. Under the new model,
15 you collect as much as information as possible
16 and you protect privacy through after the fact
17 post-collection use restrictions.

18 I'm here to encourage you to resist this
19 new model. In my written testimony I argue four
20 points. The first is that collection still
21 matters. The collection of personal data impacts
22 a person's core right to privacy, regardless of

1 what happens to that data after the fact.

2 Second, this was discussed in the first
3 panel, but there's a misconception, I think, that
4 the FIPPs are primarily useful for commercial
5 privacy.

6 In my written testimony I talk about the
7 fact that the FIPPs remain a critical benchmark
8 against which to measure the privacy impacts of
9 counterterrorism policies.

10 And I'll just add given the previous the
11 discussion, that literally since their inception
12 in 1973, the committee that wrote the report
13 dedicated a section, it's just two pages, talking
14 about how of course not all of the FIPPs can
15 apply in the intelligence context, but clearly
16 some of them must because the risk is too high.

17 Third, in my testimony I talk about that
18 we need to remember that privacy is not about
19 taking but about -- pardon me -- it's about
20 taking and not about sharing.

21 And fourth and finally, I think that
22 Americans do expect a degree of privacy in

1 public.

2 Now given my limited time here I
3 actually want to focus my oral testimony on just
4 that first point, collection. I think it's the
5 most important.

6 After the Snowden disclosures on the
7 telephone records program last summer, the IC's
8 first line of argument was that, you know, we may
9 collect a lot of this information but we only
10 look at a tiny part of it.

11 The problem is that this is not how
12 people think about privacy. If a police officer
13 knocked on your door and said, hey, I want you to
14 give me a list of every person you've spoken with
15 in the last week and then said, you know, don't
16 worry, we're really probably never going to look
17 at this stuff, would that reassure you? I think
18 that most people would say no.

19 And I think that this highlights the
20 fact that the forcible collection of sensitive
21 data in and of itself invades what this Board has
22 called, "the core concept of information

1 privacy". And that's, "the ability of
2 individuals to control information about
3 themselves".

4 It's not just a concept. As you know,
5 it implicates First Amendment and Fourth
6 Amendment interests. I elaborate that in my
7 written testimony.

8 But in my mind the single biggest reason
9 to resist the privacy model that primarily relies
10 on post-collection use restrictions is the
11 disparate impact that that model might have on
12 vulnerable communities.

13 Now again, in a use restriction model
14 you collect everything and you protect privacy by
15 banning harmful uses of data after it's been
16 collected.

17 The problem is that there's basically
18 what I'll call a moral lag in the way we treat
19 data.

20 What I mean by that is that we as a
21 society are often very slow to realize that a
22 particular use of data is harmful, especially

1 when it involves data of racial and ethnic
2 minorities, LGBT people, and others who have
3 historically lacked political power.

4 In fact, the two most prominent examples
5 of this moral lag involve the Department of
6 Defense, or formerly the Department of War.

7 During World War II, Japanese Americans
8 volunteered information about themselves and
9 their families in the census. They volunteered
10 that information under a statutory promise from
11 the federal government that that data would
12 remain confidential. This was a use restriction.

13 What happened? As you know, in 1942,
14 Congress waived the confidentiality provisions
15 and the Department of War used detailed census
16 data to monitor and relocate Japanese Americans
17 to internment camps.

18 After World War II a similar story
19 unfolded for gay and lesbian service members.
20 They were prohibited from serving openly, and so
21 many of them turned to military chaplains,
22 psychologists, physicians.

1 Yet routinely and even after don't ask,
2 don't tell, the military would use that
3 confidentially collected data to out and
4 dishonorably discharge LGBT service members.

5 Now today with the benefit of hindsight
6 we recognize that these events are
7 discrimination, but at the time the picture was
8 less clear for a lot of people.

9 And that took a long time to change.
10 The census only acknowledged the full extent of
11 wartime sharing of census data in 2007, and
12 Congress only repealed the ban on openly serving
13 gay and lesbian service members in 2011. That
14 was three years ago.

15 So let me be clear, my point is not to
16 cast aspersions on the Department of Defense,
17 rather my point is that all of us as a society
18 are consistently slow to recognize what's a
19 harmful use of data when it comes to vulnerable
20 communities. It often takes us decades to figure
21 that out. Far too often today's discrimination
22 was yesterday's national security measure.

1 What this means for our data and what
2 this means for privacy is that we cannot solely
3 rely on use restrictions.

4 What this means is that collection
5 matters and the that simplest and most powerful
6 way to protect privacy is to limit data
7 collection, particularly for the government.

8 I urge you to continue to protect that
9 core right. Thank you.

10 MR. DEMPSEY: Thank you very much. Our
11 next witness is Mike Hintze, who is Chief Privacy
12 Counsel at Microsoft, where he's been for sixteen
13 and a half years at the epicenter of the
14 evolution of technology and privacy.

15 MR. HINTZE: Thank you. Thank you for
16 the opportunity to speak with you today and
17 participate in this important discussion.

18 I come to this discussion from the
19 perspective advising on and managing privacy and
20 related issues in the private sector.

21 I've done that for nearly two decades,
22 first as an associate here in a D.C. law firm,

1 and as you mentioned for the last sixteen-plus
2 years at Microsoft.

3 At Microsoft we approach the issue of
4 privacy from a core belief that privacy is an
5 essential value, both to us and to our customers.
6 We have a strong commitment to privacy because we
7 recognize that customer trust is critical to the
8 adoption of online and cloud services.

9 Our customers, from individual consumers
10 to large enterprises, will not use our products
11 and services unless they trust them, unless they
12 trust that their private data will remain
13 private.

14 We seek to build that trust with our
15 customers by adhering to a robust set of policies
16 and standards. These policies and standards
17 guide how we do business and how we design our
18 products and services in a way that protects
19 customer privacy.

20 These standards are based on the Fair
21 Information Practices, which we agree remain
22 relevant today, including transparency about the

1 data and how we use it, minimization with regard
2 to the data collected and how long it's retained,
3 choice about collection and use of data, strong
4 security to ensure that the data is protected,
5 and accountability to ensure that we are living
6 up to our commitments.

7 These standards are not just a rule that
8 we create it and hope that our employees follow.
9 Instead, we built them into the processes we use
10 to operate our business.

11 For example, they're built into the
12 tools that are used in our software development
13 life cycle, and there are checkpoints that
14 prevent a product or service from shipping
15 without a privacy sign off.

16 In sum, we've taken what's often
17 referred to as a privacy by design approach to
18 how we operate the company and how we develop and
19 run our services.

20 And this approach is supported by a
21 mature privacy program that includes dedicated
22 personnel with privacy expertise who sit in both

1 centralized roles and are embedded throughout the
2 business. The program includes incident
3 management, response and escalation processes.

4 Further, we've developed and deployed
5 comprehensive role-based training for engineers,
6 sales and marketing personnel, as well as those
7 in HR, customer service and other roles that
8 touch and handle personal data. And our program
9 includes executive level accountability for
10 privacy compliance.

11 But that investment in privacy and the
12 trust we've worked to build is undermined if
13 those customers believe the government can freely
14 access that data.

15 Concern about government access to data
16 collected by the private sector can foster a lack
17 of trust in those private sector services.

18 And when those concerns are focused on
19 the access to data by the U.S. government, that
20 lack of trust becomes focused on U.S. companies.

21 That's why we've been vocal for the need
22 for surveillance reform in the United States.

1 There have been positive steps in this regard in
2 the last year but there's more that needs to be
3 done.

4 We've laid out several things the U.S.
5 government should do to help restore the trust
6 that's been damaged by last year's revelations.

7 First, bulk data collection programs
8 should end. We have been clear that we have not
9 received any bulk orders, any orders for bulk
10 data collection, but we strongly feel that
11 surveillance should be focused on specific
12 targets rather than bulk collection of data
13 related to ordinary people's activities and
14 communications.

15 The recommendations of this Board on the
16 Section 215 program are encouraging, as are the
17 comments of the President, and we urge the
18 administration to end the existing program, and
19 we urge Congress to enact prohibitions on any
20 such orders in the future.

21 Second, we should do more to increase
22 transparency. Transparency is a key element to

1 any program for protecting privacy. It
2 facilitates accountability and enables public
3 debate around policies and programs.

4 Here too we've seen positive
5 developments. In particular, the government has
6 declassified more information about its
7 surveillance programs and the workings of the
8 FISA court.

9 Additionally, we and other companies
10 filed lawsuits last year against the U.S.
11 government arguing that we have a legal and a
12 constitutional right to disclose more detailed
13 information about the demands we've received
14 under U.S. national security laws.

15 And earlier this year we came to an
16 agreement with the government enabling us to
17 publish some aggregated data about the FISA
18 orders and the national security letters we've
19 received.

20 It was a good step that helped foster
21 better understanding of the type and volume of
22 such orders that service providers received, but

1 we believe there can and should be more detailed
2 reporting permitted.

3 Third, we support reforms of how the
4 FISA court operates. In order to foster a
5 greater confidence in surveillance programs and
6 government access to data that are appropriately
7 balanced against privacy and other individual
8 rights, surveillance activities must be subject
9 to judicial oversight.

10 We need a continued increase in the
11 transparency of the FISA court's proceedings and
12 rulings, but effective judicial review requires a
13 true adversarial process where more than one side
14 is heard. We urge Congress to act on FISA
15 reform.

16 Fourth, government should provide
17 assurances that it will not attempt to hack into
18 data centers and cables.

19 In the year since the Washington Post
20 reported an alleged hacking by the NSA of cables
21 running between data centers of some of our
22 competitors, there's not yet been any public

1 commitment by the government that it will not
2 seek to obtain data by hacking into Internet
3 companies.

4 We believe the Constitution requires
5 that the government seek information from
6 American companies within the rule of law and
7 through authorized government access, and we've
8 taken steps to prevent such attempts by
9 increasing and strengthening our use of
10 encryption across our networks and services.

11 Nevertheless, we and others in industry
12 will continue to press for clear government
13 assurances.

14 Fifth, although recent government
15 revelations have focused mainly on the U.S.
16 government and many of the subsequent debates
17 have focused on the privacy rights of U.S.
18 persons, we must recognize that this is a global
19 issue.

20 As we seek to sell our products and
21 services to customers around the world,
22 discussions that focus exclusively on the rights

1 of U.S. persons are not enough. Many people
2 around the world do view privacy as a fundamental
3 human right, and they have a very real concern
4 about whether and how governments can access that
5 data.

6 In that regard, we appreciate the steps
7 that President Obama announced in January which
8 acknowledged the need to address protections
9 about non-U.S. citizens.

10 Along those lines in the law enforcement
11 context, we've challenged a federal warrant in
12 the U.S. courts seeking customer email for
13 content that's held in our data center in
14 Ireland.

15 Further, we've called for governments to
16 come together to create a new international legal
17 framework that allows for new streamlined
18 processes for cross border data access that can
19 supplement existing rules.

20 None of this should be taken to suggest
21 that we don't value and appreciate the absolutely
22 critical work that our law enforcement security

1 agencies do every day to keep us all safe.

2 In fact, we work closely with the U.S.
3 and other governments to help fight cyber crime
4 and other threats. We want to ensure that those
5 agencies have the tools and information that they
6 need to protect us from terrorism and other
7 threats to our safety and security, but there
8 needs to be a balance between safety and the
9 personal freedoms that people around the world,
10 especially law-abiding citizens and institutions
11 enjoy.

12 This balance is rarely an easy one. As
13 Chief Justice Roberts recognized recently in the
14 case of Riley v. California, privacy comes at a
15 cost. But the court's unanimous decision makes
16 clear privacy is an inherent and enduring value
17 that must be protected.

18 While there's not always a perfect
19 analogy between protecting privacy in the private
20 sector, law enforcement, and national security
21 context, we also, we in the private sector
22 regularly deal with questions of striking the

1 right balance between privacy and other needs.

2 In each of these contexts as technology
3 evolves we need to continually reevaluate that
4 balance and many of the principles that have
5 proved useful in striking and retaining that
6 balance, the Fair Information Principles,
7 continue to be relevant today.

8 MR. DEMPSEY: Mike, could you wrap up?

9 MR. HINTZE: Thank you. I'll end my
10 comments there.

11 MR. DEMPSEY: Okay, super, thanks.
12 We'll come back to some of those issues with the
13 questions.

14 Our final member of this panel is Hadi
15 Nahari. He is Chief Security Architect at
16 NVIDIA, a company that designs and builds high
17 performance computer systems. Hadi is a
18 cryptographer and computer scientist. Welcome,
19 please proceed.

20 MR. NAHARI: Thanks for the opportunity
21 to testify today. I appreciate it.

22 I'm here as a technologist and not as a

1 lawyer. In Silicon Valley we say the "I'm not a
2 lawyer" rule applies.

3 Our concern is about building systems
4 that are buildable and creating rules that are
5 enforceable, so I wish to provide some technology
6 background to the panel and to the conversation.

7 From our perspective security is to a
8 system what harmony is to music. Providing
9 security as a foundation of establishing rules of
10 privacy is our model.

11 We build systems that are enabled and
12 are able to enforce rules, and that is the
13 context of security as we see it.

14 Security is one of the intersections
15 between technology and civil liberty, and we deal
16 with issues such as trust and active adversary in
17 a system. This is how we build and design our
18 systems.

19 Our world used to be simpler, and
20 sometimes I provide samples of that simpler
21 world. You all remember this as a mobile phone.
22 This is from the time that the phones were

1 actually doing just that, they were a phone.

2 And some of these devices were
3 statements of class. You all remember this,
4 right? This was a phone. This was a mobile
5 phone. I worked in this company.

6 One of my favorites in the collection,
7 text, this used to send and receive even text
8 messages.

9 Oh, yeah, CLIE, this was your personal
10 and digital assistant.

11 I have some others. Oh, yeah, Palm,
12 they used to be a company that existed, this was
13 one of the darlings of the valley.

14 So these, of course this was also a very
15 important device that everyone carried.

16 This is from the time that the world was
17 very simple and we built systems that did very
18 basic things.

19 And it was per Thomas Friedman, and I
20 quote here, "When I sat down to write, The World
21 is Flat, Facebook didn't exist, Twitter was still
22 a sound, the cloud was still in the sky, 4G was a

1 parking place, LinkedIn was a prison,
2 applications were what you sent to college, and
3 Skype was a typo."

4 So June 29th, 2007, iPhone was
5 introduced, the world changed. The world for us
6 technologists changed, probably for everybody
7 else in the room, non-technologist and
8 technologists alike also changed. And we are
9 dealing with devices that are not as simple as
10 what we used to carry.

11 So that's part of the problem from my
12 perspective. I'm interested in the ramifications
13 of the changes in this technology as the subject
14 that we are talking about. It's only seven and a
15 half years.

16 It's only seven and a half years ago.
17 So I don't believe there's any other event in
18 history that in this short amount of time has
19 ravaged and gone through everything and tried to
20 change everything, such as the foundation of our
21 society.

22 In the old and pre-2007 world we said

1 things like, you cannot enumerate all the attacks
2 in cryptography is a known statement. And state
3 space combinatorial explosion, meaning you cannot
4 define a secure state of a system. It was
5 difficult back then during these devices. It has
6 just become worse.

7 The guarantees, we do not know anything
8 about our future but a couple of things I could
9 guarantee, a couple of things I could guarantee
10 right here is that things will only get faster.
11 We're going to build things that are faster.
12 They're going to become smaller, a lot smaller.
13 They're going to become cheaper, and these
14 devices are going to become a lot more abundant.

15 Some of them, we no longer care about
16 building devices that are usable for a long
17 period of time. It's a lot more economic to
18 build these devices that are basically throwaway
19 devices. That's the concept that we are
20 following.

21 And they're becoming more connected.
22 Everything is becoming more connected. You have

1 heard things such as IOT, Internet of things, or
2 as I call them, thingsternet.

3 Everything is just becoming very
4 talkative. All of these devices are very chatty.
5 They talk a lot. So you guys all have phones,
6 smartphones in your pockets. From the time that
7 I started, which was about five minutes right
8 now, until now, each one of those devices,
9 without you even touching them, has transmitted,
10 sent and received, about half a meg data, without
11 you even touching them.

12 This abundance of information that is
13 happening that is, without you interacting, is
14 having a lot of ramifications on what we are
15 doing.

16 We heard a lot of things about data is
17 only, you know, accumulating. It's not going
18 away. We are generating more data than we can
19 manage or fathom.

20 A hundred hours of video, a hundred
21 hours of video is uploaded on YouTube, and
22 YouTube is not the only recipient of the service,

1 other companies also have these services, a
2 hundred hours of video are uploaded to YouTube
3 every single minute. Every single minute.

4 So we are building systems to manage,
5 and compartmentalize, and define, and create and
6 work with these data. And this data, as we have
7 heard in the two panels, are not going away.
8 They are not disappearing.

9 In the new world, maintaining security
10 is even harder. So as a citizen, I'm very
11 carefully following what is happening by this
12 esteemed Board as to what is the ramification of
13 the decisions that we are making and whether
14 that's enforceable, whether we can build systems
15 that are enforcing these rules.

16 Because right now being a security
17 professional and creating doable and enforceable
18 security is as unpopular as being an atheist in
19 Jerusalem. No one likes you. So I'm hoping that
20 we can come up with a system that is also
21 buildable.

22 And lastly, I close my remarks and I'm

1 looking forward to the questions.

2 One more thing that I could guarantee is
3 the attacks are going to increase only, and
4 they're going to become simpler and easier to
5 mount.

6 By one measure the number of attacks in
7 2013 were three trillion, only affecting private
8 information, on average 27.3 dollars per attack,
9 about a hundred billion dollars, the cost of
10 these attacks. This data is 2013. None of the
11 Target, Home Depot, LinkedIn, none of that
12 information, none of those attacks are included
13 here.

14 So with that, I close my remarks and I
15 look forward to answering questions. Thank you.

16 MR. DEMPSEY: Thank you. We'll now go
17 through a round of questioning, and Board members
18 as well will be subject to the time limits here.
19 I think I have 20 minutes and then each Board
20 member will have five minutes, and then still the
21 possibility of questions from members of the
22 audience.

1 I wanted to build my first question off
2 of the point that I think Hadi was making at the
3 end, which is that there seems to be this
4 inexorable trend towards more sophisticated
5 devices collecting, generating, sharing, emitting
6 autonomously, automatically disclosing more and
7 more information.

8 And I think I'll go to Professor Anton
9 first and then maybe come back to Hadi with this,
10 but looking at that phenomenon and the seeming
11 inexorability of it, the seeming inevitability of
12 it, first on the technology design side and then
13 on the policy side, on the technology design side
14 what do you see as any potential at all for
15 limiting that growth, controlling the flow of
16 that information?

17 You talked to some extent about the
18 possibility of technology protecting privacy.
19 How does that square with this tremendous ongoing
20 growth of information?

21 MS. ANTON: Thank you. So you know, as
22 was mentioned in the earlier panel, systems are

1 getting more and more complex, which makes
2 compliance more and more difficult as well.

3 I really hope that we don't limit growth
4 and limit the ingenuity of new technologies that
5 might have really great applications in the
6 future and solve wonderful, really important
7 problems.

8 By the same token, there is a lot of
9 work that's been done, especially with work
10 that's being done at Georgia Tech, in fact, on
11 how do we design the Internet of things or the
12 Internet of devices, such that we are taking
13 privacy and security into consideration, give all
14 of the outputs, all of the possible inputs.

15 And engineers just simply need better
16 tools and heuristics for how to do that. And,
17 you know, it's privacy by design, it's thinking
18 about these things early on and not thinking
19 about it after the fact.

20 And in terms of controlling information,
21 I think what we want is to secure the flow of
22 information, but not limit the flow of

1 information.

2 And these are all things that
3 researchers are actively working on in
4 universities and at research labs in industry as
5 well.

6 MR. DEMPSEY: You know, I've written
7 myself about the potential for privacy enhancing
8 technology, value of privacy by design. But at
9 the same time, I mean at some level I just don't
10 see it happening.

11 MS. ANTON: So --

12 MR. DEMPSEY: Or let me put it this way,
13 while I see it happening, and I think Mike
14 Hintze's point that Microsoft has incorporated
15 privacy by design as a corporate concept, but
16 there are these other hugely dominant trends that
17 almost seem to be overwhelming.

18 MS. ANTON: So within the context of
19 counterterrorism I think that there's a lot of
20 policies and a lot of laws that are in place.

21 When I mentioned earlier that I'd like
22 to see more technologists in the room, it's not

1 just to kind of study it after the fact, but
2 actually to be involved in forming the policy.
3 Because a lot of times the policy and the law are
4 written in such a way that we can't implement it.

5 And so what I'd like to see is more
6 technologists involved in the discussion up front
7 really informing the decisions about laws that
8 are going to be passed, about the policies that
9 we're going to adopt, because we could write them
10 in a way that makes it a lot easier to comply
11 with the law.

12 MR. DEMPSEY: Do you have an example in
13 mind?

14 MS. ANTON: Excuse me?

15 MR. DEMPSEY: Do you have an example in
16 mind?

17 MS. ANTON: So I work a lot in HIPAA,
18 for instance. We have the new change with
19 meaningful use. I had one Ph.D. student who was
20 really working actively on how do we predict what
21 the change is actually going to be? Because when
22 they finally make that decision we're going to

1 have very little time to implement that change in
2 systems to be able to be able to make sure that
3 we're compliant with it.

4 And had we had more technologists
5 involved in that process, we'd be able to more
6 quickly adapt our systems and we'd have a better
7 community of practice, if you will, about how to
8 establish those laws and how to then instrument
9 systems to make sure that only the right people
10 are having access to the right information at the
11 right time and in compliance with law.

12 MR. DEMPSEY: Just to round that out,
13 certainly you would agree that we need both
14 better, clearer laws, as well as more mindful
15 technology design?

16 MS. ANTON: Absolutely.

17 MR. DEMPSEY: That it's not that one or
18 the other will solve this problem.

19 MS. ANTON: Absolutely, we need both,
20 right.

21 MR. DEMPSEY: I want to go to Alvaro
22 Bedoya. There was one point in your written

1 testimony that you didn't mention and I want you
2 to talk about it now. I think it's very
3 important.

4 A lot of our constitutional law of
5 privacy is based upon the concept of reasonable
6 expectation of privacy. And there's a lot of
7 worry and a lot of, I think, legitimate concern
8 that with these changes in technology that our
9 expectations of privacy diminish.

10 You talked about the fact that, in fact,
11 with changes in technology our expectations of
12 privacy may actually be growing. Could you
13 explain that?

14 MR. BEDOYA: Yeah, that's exactly right.
15 And the point here is that the Katz test cuts
16 both ways. You know, usually when the court
17 talks about Katz in society, they say, well,
18 everyone's becoming inured to this idea. They're
19 surrendering to the ubiquitous collection of
20 their data.

21 But I actually think people are,
22 technology is helping people learn about what

1 they think privacy is.

2 And the best example of this I think is
3 location technology and facial recognition
4 technology.

5 Previously people had no occasion to
6 develop an opinion on whether or not they
7 expected, you know, the sum total of their
8 movements to be developed, to be compiled in a
9 profile, but suddenly it's becoming radically
10 cheaper to conduct that surveillance.

11 And so I think that in the same ways
12 that you only realize what you had when you start
13 losing it, for the first time a reasonable
14 expectation of privacy in public is crystallizing
15 in people's minds.

16 And so I would say that ubiquitous
17 surveillance is making people say, hey, you know
18 what, maybe when I go to the grocery store, or I
19 drive down the street, or I go to work I expect
20 my colleagues at work to see me, you know, the
21 people I know at the store to see me, my
22 neighbors to see me, but I really don't expect

1 anyone to know that I'm at all those places at
2 all times no matter where I go.

3 And so I do think that technology can
4 expand our expectation of privacy.

5 MR. DEMPSEY: And Mike Hintze, certainly
6 over the past fifteen or sixteen years that
7 you've been at Microsoft, do you think it's fair
8 to say that your customers have become less
9 interested and less concerned about privacy or
10 expect more of Microsoft and other companies when
11 it comes to privacy?

12 MR. HINTZE: I think they expect more.
13 I think, you know, I agree that expectations of
14 privacy in some ways have increased. They've
15 certainly changed.

16 As technology evolves people learn about
17 it, they adapt. There's certainly data sharing
18 going on that people wouldn't have contemplated
19 or accepted a number of years ago, but that
20 doesn't mean people don't care about privacy
21 anymore.

22 It's very clear to us that our customers

1 care about privacy now more than ever. And you
2 see that in the amount of resources and attention
3 and focus that we've put on privacy.

4 It really is one of the top legal issues
5 we're dealing with. It's one of the top customer
6 issues we're dealing with. We hear every day
7 from customers who have questions about how their
8 data is being treated, how it's being protected,
9 how it's used. People's expectations of privacy
10 are not fading away.

11 MR. DEMPSEY: And by the way, just to
12 put a sort of nail in the coffin here, I think
13 the government argues, and there's obviously
14 Supreme Court precedent to support it, that a
15 person surrenders his privacy rights when he
16 discloses information to a third party such as
17 Microsoft in the course of using the Microsoft
18 products or services.

19 But it seems to me from what you're
20 saying that Microsoft does not believe that its
21 customers have surrendered their privacy rights
22 when they use the Microsoft product or service,

1 and thereby Microsoft has acquired information,
2 Microsoft does not believe that that information
3 has zero privacy interests.

4 MR. HINTZE: Absolutely not. On the
5 contrary. I mean to the extent that the third-
6 party doctrine ever made any sense, it doesn't
7 make any sense today.

8 I mean people increasingly are putting
9 all of the information that they used to keep in
10 their homes, in their file cabinets, online in
11 cloud services.

12 And as recent court decisions have
13 recognized, particularly in Riley, it's even more
14 data. There's more data in the cloud. There's
15 more data being created that reveal the most
16 private and intimate details of people's lives
17 that's in cloud services in the hands of third
18 parties, more so than was ever in people's homes.

19 And the expectations around privacy
20 around that data are quite profound.

21 MR. DEMPSEY: And that's true, in your
22 view, both of content, so to speak, and

1 non-content, or metadata, or transactional data.

2 There's sensitivity there in both categories.

3 MR. HINTZE: Absolutely. You know I
4 don't like the term metadata because it
5 encompasses too much. I think we should talk
6 about what we're talking about.

7 And you know, there's a broad range of
8 data that's collected, or even created, or
9 inferred through the use of online service. And
10 some of it's fairly benign.

11 You know, we call things metadata, put
12 the metadata label on things like the amount of
13 storage you're using in your online storage thing
14 or the average file size, but even that has
15 privacy implications. And we embrace the ideas
16 of transparency, and consent, and all of the
17 FIPPs around that kind of data, too.

18 But as you go up the scale with maybe
19 content being the end as sort of the most
20 private, the stuff that people have the highest
21 expectation of privacy around.

22 But other things about who you're

1 communicating with are right up there, right up
2 against content in terms of what that can reveal
3 about people's relationships, associations,
4 thoughts, beliefs, etcetera. And there's very
5 important privacy implications around that data
6 as well.

7 MR. DEMPSEY: You mentioned the
8 trans-border issues and the fact that people
9 around the world recognize privacy as an
10 interest, and in many cases as a human right.

11 Just where do we stand and what are you
12 aware of, or what do you know about, is there any
13 progress being made multilaterally, or
14 bilaterally in terms of developing standards for
15 trans-border surveillance and trans-border
16 government access, anything in the works there
17 that we should be aware of?

18 MR. HINTZE: Not that I'm aware of
19 specifically. You know, there's certainly more
20 discussions happening in recent years than there
21 has been in the past around a number of
22 constituents and interested parties on privacy

1 around the globe.

2 Jim and I were recently at an
3 international data protection conference where
4 these issues were loudly and vigorously discussed
5 and debated.

6 And so that dialogue is happening, but
7 in terms of actual progress towards making
8 headway in terms of developing an international
9 framework for this stuff, there's certainly a lot
10 more work to be done.

11 MR. DEMPSEY: May I just ask you and
12 others, as well as members of the audience,
13 additional panelists, if and when you do become
14 aware of things that are making progress, please
15 let us know. Obviously we're remaining
16 interested in that trans-border question.

17 For Hadi Nahari, you know we've talked
18 about privacy by design. In your experience do
19 technologists give adequate consideration to
20 privacy as they design products? And what more
21 could be done to encourage or promote privacy by
22 design?

1 MR. NAHARI: In technology we build
2 things that are reasonably well-defined. So I
3 recognize in the previous panel there was a
4 discussion that you don't necessarily need to
5 define privacy to be able to enforce it.

6 On the technology side, if we are able
7 to build a model that represents a need, then we
8 are very good at building it.

9 I think part of the reason that mapping
10 a very human, a very societal concept such as
11 privacy into the devices that we build, the
12 services that we build and we use, sometimes it's
13 simpler, sometimes it's not.

14 To answer your question, I see a great
15 deal of attention, a great deal of interest in
16 the notion of privacy, privacy by design, secure
17 by design, trustworthy by design.

18 And especially in the field that we are
19 dealing with, our model, in security of the
20 device when we release it and goes to the field
21 is a mutually distrusting system. So you don't
22 really know.

1 Let me take a step back. It's one thing
2 to build a server that resides in someone's data
3 center where you have full control over the
4 actual device and you have to control the flow of
5 information, the software that is there and how
6 it's used.

7 It's another thing to build a device and
8 leave it in the hands of the users and guessing
9 what they want to do.

10 And then it's one thing to have a notion
11 of privacy, as we do, and build a system based on
12 that.

13 It's another thing when you take a look
14 at this, should I call it a generation gap as
15 to -- there's this company called Snapchat and
16 they had promised that whatever picture you take,
17 it's going to disappear.

18 Anyone who has worked in technology
19 knows things like this are not possible, you
20 could simply just take a picture of that device.
21 But we call it job security.

22 Then when they realize that this is not

1 really possible they announced it, and they are
2 under the oversight of the government for about
3 20, I think, years to make sure that they do
4 things right. And they are paying attention. I
5 know they are paying a lot of attention to make
6 sure they get things rights.

7 But then you take a look at the users.
8 I think the stat was released last week or the
9 week before that they asked college students, 50
10 percent, more than 50 percent of college students
11 said, yeah, we still will use Snapchat. They are
12 aware. They understand.

13 I don't know how to reconcile that.
14 There is a new generation that has, I don't know
15 whether it's a more or less, but certainly a
16 different expectation and definition of privacy.
17 And there is a vagueness of what does that mean
18 in terms of a system that could be built.

19 Once those are, you know, in a
20 reasonable state, we are really good at building
21 systems that satisfy those rules.

22 Hence my opening remarks as to our model

1 in the industry and in technology is we
2 understand the rules, we are very good at, you
3 know, creating those rules and building systems,
4 devices, services and everything that enforce
5 those rules, but it has to be buildable and it
6 has to be enforceable. The attention is
7 certainly there.

8 MR. DEMPSEY: But the first premise is
9 the rules have to be clear and if they're not
10 clear, then you don't know what to build.

11 MR. NAHARI: Semi-clear will do. We
12 used to live in a world before 2007 that
13 everything had to be really, really well-defined.
14 It no longer exists.

15 We have a new generation of hackers that
16 do not abide by the rules, therefore we have to
17 create systems that are almost right. We are
18 seeing it in the program languages, we are seeing
19 it in the design of the system, we are seeing it
20 in self-correcting systems. Sometimes somewhat
21 accurate will do.

22 MR. DEMPSEY: Do you want to respond to

1 that?

2 MS. ANTON: Sure. So this reminds me a
3 little bit about what I was talking about
4 practical encryption and anonymization. And so I
5 think there are times in certain applications
6 where that kind of risk is fine and there are
7 other instances where it's not fine.

8 And then that's where guidance from
9 PCLOB can be very helpful in terms of trying to
10 figure out what are the risk profiles and when is
11 it that we can have pretty good rules and when do
12 we have to have very, very tight, accurate,
13 hundred percent certainty kind of rules.

14 MR. DEMPSEY: Okay, thank you. At this
15 point other members of the Board will pose some
16 questions under the five minute rule. And we'll
17 go in sort of reverse order down the line here
18 starting with Rachel Brand.

19 MS. BRAND: Thank you, Jim, and thanks
20 to all of you for being here.

21 That's actually a really good segue
22 because the first question I was planning to ask

1 was, Dr. Anton, I was interested in what you were
2 saying about not letting the perfect be the enemy
3 of the good in terms of de-identification. In
4 the domestic violence context you want it to be
5 perfect perhaps, and in other contexts good
6 enough will do.

7 Can you explain what you mean by that?
8 What's an example of a de-identification method
9 that might be good enough but perhaps not
10 perfect?

11 I'm not a technologist, as you know, so
12 if you can help me out, that'd be great.

13 MS. ANTON: All right. So there are
14 certain cases of studies that have been done, for
15 instance, when the Netflix put out their data
16 online and then researchers went and looked at
17 the Internet Movie Database to try to see whether
18 they could re-identify people. They had
19 resources, it was readily available information.
20 In this context I don't think anyone was
21 personally hurt by it.

22 But there might be cases where that kind

1 of identification could be extremely damaging.

2 And so the more, we talked earlier about
3 aggregation of databases and how the ability to
4 link different kinds of information across
5 different kinds of databases could actually be
6 detrimental. It can also help us find the bad
7 guy though. And so that's the tension, right?

8 So when is it okay and when is it not
9 okay? And are there instances, for instance, for
10 Netflix or something that's available online
11 that's just not, you know, where you went to
12 school or something that's not very important.
13 It may not be really necessary to worry about
14 where you had dinner, for instance.

15 But in a context of a group that is
16 actively trying to announce a terrorist attack,
17 then that's really important.

18 MS. BRAND: So I guess that makes sense
19 in terms of when it's important and when it's not
20 important, but how do you do it? I mean like,
21 for example, how do you do the perfect in the
22 domestic violence context?

1 MS. ANTON: I think that's very
2 difficult. I think we have technology that's
3 pretty good but not perfect. And so the idea is
4 do you keep the data unencrypted and then easily
5 accessible, because it's not very important, or
6 do you actually encrypt it and then use
7 reasonable, practicable anonymization on top of
8 that?

9 So it just depends. And I think this is
10 one of those cases where technologists would
11 welcome guidance in helping us to figure out what
12 are the risk profiles, because technologists
13 don't have access to sometimes what the risks are
14 within a counterterrorism context.

15 MS. BRAND: For Mr. Bedoya, you said
16 something along the lines of, in the national
17 security context some of the FIPPs must apply
18 even if they all can't. Can you elaborate a
19 little bit more?

20 MR. BEDOYA: Yeah, sure. So the first
21 is a historical point, which is that when the HEW
22 report was issued, I was just reading, it's like

1 pages 74, 75, the committee actually says, okay,
2 we just set out these standards, clearly all of
3 them can't apply to all intelligence records, but
4 some of them must apply because the risk is too
5 high if we don't have some protections.

6 So to put that more concretely,
7 obviously the difficult ones are individual
8 participation and transparency. And I think
9 there are ways to address these, at least on an
10 aggregate level that would be really powerful.

11 So, you know, I think in the 702 context
12 the Board has -- and to take a step back, I think
13 it is shocking that one and a half years after
14 the Snowden disclosures the American public
15 doesn't have even a rough sense of how many of
16 them have had their information collected.

17 Take the telephone records program,
18 people think it's everyone, but then you have
19 news reports saying actually only 30 percent of
20 calls are actually recorded.

21 And so in the 702 context the Board has
22 recommended various measures to identify the

1 scope. In all my time in the Senate I never saw
2 anything that would lead me to believe that it
3 would actually be impossible for the NSA to
4 produce an estimate based on statistical sampling
5 of the number of U.S. persons collected in 702
6 data.

7 In the 12333 context there's a number of
8 things you could do to quantify scope. One of
9 them could just be releasing the number of
10 queries done on USP data and 12333 data.

11 So I think there are ways to address
12 these principles at the aggregate level, if not
13 at the individual level.

14 MS. BRAND: Okay. Anybody else have a
15 thought?

16 MS. ANTON: I have a thought on that in
17 terms of transparency. This is another way in
18 which, for instance, FISC technologists could be
19 helpful because when you have -- if Hadi whispers
20 in Mike's ear, I spoke with Jim Dempsey about the
21 panel, by the time that gets to Jim it's going to
22 be, I spoke with Jim about wearing flannel. It's

1 going to be something completely different.

2 So when you get lawyers talking together
3 from the NSA and the FISC about technology, and
4 you don't have a technologist there to ask
5 questions or make suggestions about, well, we
6 could actually, have you thought about including
7 this kind of metric, or collecting this kind of
8 data, or instrumenting the software in certain
9 ways, we could actually improve the ability to
10 have more transparency and more oversight in
11 technology with those discussions, bringing
12 everyone in the room.

13 MS. BRAND: Thank you.

14 MR. DEMPSEY: Chairman Medine.

15 MR. MEDINE: I'm going to try to get a
16 question in for each panelist, so I'd appreciate
17 brief responses.

18 For Annie, you said something that
19 surprised me a little bit, which is that
20 encryption is good for counterterrorism.

21 And I guess I would like to understand
22 more. I understand having or mandating a

1 backdoor weakens protections, but why? It would
2 seem as though terrorists can now hide their
3 communications, which seems to be detrimental to
4 counterterrorism.

5 MS. ANTON: I think it's a better world
6 when everyone can hide their information. And so
7 there was a case in Greece where there was a
8 phone and someone was able to actually start,
9 because of the backdoor and the known exploits,
10 they were able to actually listen to the
11 conversations, basically do a wiretap on the
12 prime minister. That's what happens when you
13 don't have encryption and you don't have security
14 by default.

15 And so to think that the terrorists
16 aren't going to do the same thing, I think is
17 naive.

18 MR. MEDINE: Alvaro, you talked about
19 the expectation of privacy, and if I heard you
20 correctly, but tell me if I'm wrong, is that
21 you're in a sense suggesting that we talk about
22 not what people expect their privacy to be,

1 because I can put up a sign saying I'm conducting
2 video surveillance and I can destroy that, but
3 their expectations of what privacy should be, a
4 more normative standard.

5 MR. BEDOYA: So I'm actually not saying
6 that. So that's a separate wonderful, powerful
7 argument.

8 What I'm saying is that technology is
9 making us realize that we do expect privacy in
10 scenarios that didn't exist ten or 15 years ago.
11 So I think technology can expand our notion of
12 privacy.

13 But I also think that the Fourth
14 Amendment doesn't just protect me and you, it
15 protects us as a society and it sets a base for a
16 relationship between a government and its
17 citizens that also needs to be protected.

18 MR. MEDINE: Okay. And I guess this is
19 for Mike, the Fourth Amendment, which is you
20 talked about the balance between government
21 requests and your customers' privacy. Do you
22 think the government should have a warrant every

1 time it accesses your customers' records,
2 particularly if they're American customers?

3 MR. HINTZE: Yeah, I mean certainly in
4 the law enforcement context we've advocated for a
5 reform of that that would in effect require a
6 warrant for access to any content, regardless of
7 the age, to precise location information, other
8 sensitive data.

9 You know, I'm not sure we would go so
10 far as to say that a warrant is required in every
11 single case for every single data type, but we
12 certainly need to update the rules so that there
13 is appropriate judicial review of surveillance
14 programs and specific requests that we get for
15 data.

16 MR. MEDINE: So in terms of the third-
17 party doctrine, would you then essentially not
18 have it be an absolute exception to the Fourth
19 Amendment, but essentially where would you go
20 with it to provide some protection, but not
21 necessarily a full warrant protection?

22 MR. HINTZE: Yeah, I mean the laws that

1 we deal with in the law enforcement context
2 provide a sliding scale, in effect.

3 I mean 2703(d) orders provide some
4 reasonable oversight and protection, something
5 below warrant and probable cause, and we've taken
6 the position that that's appropriate for some
7 types of subscriber data, etcetera.

8 MR. MEDINE: Thanks. And, Hadi, you
9 talked about, and I want to put this in the
10 context of how much information should be
11 collected, and you talked about enforceable rules
12 for collection, but you also said that collection
13 is going to be faster, cheaper, and we're going
14 to be all more connected, and that attacks will
15 increase, and that even compliance with rules may
16 be more difficult.

17 Professor Felten talked about potential
18 abuse of information and also the increased
19 possibilities of breach.

20 How would you strike the balance between
21 collection rules and essentially use rules?

22 MR. NAHARI: That's a very difficult

1 question, a very difficult one. I don't know if
2 in the technology side of the house, I don't know
3 if we really know where the balance is.

4 We take a look at the attacks, we take a
5 look at the system, we take a look at the
6 capabilities, we take a look at the mere fact
7 that all of these attacks, all of these exploits
8 are becoming so advanced that I used -- to give
9 you one concrete example, I used to need to be
10 physically around your things that you touched to
11 be able to lift your fingerprint and then have
12 access to your phone and then use that
13 fingerprint to mount an attack and use your
14 biometry.

15 With the resolution of the cameras that
16 we have these days, sometimes with a very high
17 resolution camera, I just need to have your
18 picture that was taken somewhere in China to be
19 able to zoom and zoom and zoom and then lift your
20 fingerprint and mount an attack.

21 Now, how do you reflect things like this
22 as to should we build systems that whenever

1 there's a fingerprint, it smudges it and we don't
2 expose it? There are things like this that I
3 encompass all of those use cases as it should be
4 buildable.

5 But what I'm trying to get across is
6 coming up with the rules that define those
7 capabilities or things that should be and
8 shouldn't be done is a very complex problem.

9 MR. MEDINE: Thank you.

10 MS. COLLINS COOK: So thank you guys for
11 another excellent panel.

12 My first question, and this goes back to
13 what I had said on the previous panel, which is I
14 view our job to be translating these ideas, these
15 concepts, these concerns into practical
16 recommendations.

17 So starting with you, Mr. Hintze, what
18 have you found effective as a privacy officer to
19 ensure your very large workforce, your
20 complicated workforce dealing with emerging
21 issues takes privacy seriously, your rules are
22 enforced, and that from beginning to end privacy

1 is a part of your culture?

2 Because we have a new NSA privacy
3 officer, so this is free advice to the new
4 privacy officer over at NSA.

5 MR. HINTZE: Well, thank you. You know,
6 as I alluded to in my opening remarks, you know,
7 one, there's no silver bullet. You need to take
8 a number of approaches.

9 And we've taken a number of approaches
10 to drive awareness and sensitivity around privacy
11 throughout our workforce through a number of
12 steps, some mandatory training that's required
13 for all employees that cover a range of ethical
14 and compliance issues, deeper role-based training
15 that's specific to software engineers, that's
16 specific to sales and marketing people, that's
17 specific to different roles that people play in
18 the company that impact customer privacy.

19 We have, as I mentioned, not just sort
20 of told people what the rules are and then
21 crossed our fingers and hope they abide by them.

22 We have put in checkpoints in the way

1 that we have developed our internal systems, the
2 way you develop a software and get it out the
3 door that has to go through certain checkpoints
4 and reviews to ensure that privacy issues aren't
5 missed or overlooked.

6 So there's a number of things we've done
7 along those lines to make sure that people are
8 aware and have the tools available to them to do
9 privacy right.

10 But then there's also different checks
11 along the way to ensure that mistakes don't get
12 made.

13 And nothing's perfect of course, but we
14 try to do a multifaceted approach, or a
15 multi-layered approach to make sure that we catch
16 those things.

17 MS. COLLINS COOK: And so let me follow-
18 up on this, and it's a somewhat specific example
19 but hypothetical.

20 Have you found training to be more
21 effective or effective enough in the absence of
22 pairing with mechanisms and processes?

1 That was a horrible question, so I'm
2 just going to start over again.

3 So 702, that program has certain legal
4 requirements. In the privacy sector would you
5 train to those legal requirements or would you
6 also have, for example, when an analyst is
7 sitting there attempting to target, or select, or
8 whatever they're going to do, also have at each
9 stage of the screen, or the process, or however
10 they're doing it, rules reflected in the computer
11 system that they're attempting to use?

12 MR. HINTZE: We do both. To the extent
13 that you can use technology to enforce policy
14 that's always super effective because you get
15 past or you reduce the potential for human error.

16 But that's not always possible. You
17 can't completely prevent mistakes, oversight, or
18 intentional bad acts. And so you need to do more
19 than that.

20 You have to have, you have to build the
21 awareness so that the inadvertent stuff is
22 reduced. You have to build in the technology

1 tools to try to prevent that from happening.

2 And then you need some level of checks
3 to make sure that everything went right. And if
4 it's, you know, somebody who's intentionally
5 trying to circumvent a policy for whatever
6 reason, that there's some way to catch that
7 before it creates a negative impact.

8 MS. COLLINS COOK: So I think I have
9 time for one other quick question.

10 In the Section 215 program one of the
11 features was, in fact, that not all of the call
12 detail record went to the government. In fact,
13 names are not provided originally to the
14 government, and subscriber information, simply
15 numbers to numbers. Would that be an example of
16 de-identification and anonymization?

17 MR. ANTON: Sure.

18 MS. COLLINS COOK: That was my only
19 question.

20 MS. WALD: I have a couple of very sort
21 of brief questions, which I think you can answer
22 very quickly and that way I'll get them all in.

1 I'll begin with Annie. You talked about
2 how it would be good for us, and we already do
3 have technologists on the Board. I'll ask the
4 government when we have the government board
5 here, too, but let me ask you based upon your
6 knowledge here, does the government have
7 technologists who worry at all about privacy?

8 I know they have technologists
9 obviously, but is this, as a result of your
10 observations and study in the field, something
11 that they consult with the technologists about,
12 hey, we need this kind of information for
13 national security, but we'd like to get it or as
14 much as we can, what's the balance? Does any of
15 that kind of thing go on inside the government
16 with technologists?

17 MS. ANTON: Right. So having worked a
18 lot with the government I know that they consult
19 technologists greatly with security, with
20 privacy, with compliance issues, and how do we
21 engineer software that takes all of that into
22 consideration.

1 I think if we look at the past five
2 years or so, or six years or so that you'll see
3 that the NSA was really, really focused on
4 compliance. I think the results of the reports
5 and the oversight has shown that they've done a
6 really good job with that. When there's been an
7 issue, they've dealt with it.

8 I think someone mentioned the new CPO at
9 NSA. I think what we'll see different now is
10 that not only is the, are we complying with law,
11 going to be something that's factored into all of
12 the software that's developed and all of the
13 tools and the techniques and the procedures, but
14 also now well, just because it complies with law
15 should we really be doing it, and what's the
16 extra step we're going to take to really consider
17 privacy at the onset?

18 MS. WALD: So you sound reasonably
19 satisfied with the fact that they're taking it
20 seriously and doing the best they can?

21 MS. ANTON: I absolutely do. I wish, I
22 actually feel very comforted by the fact that the

1 government has a ton of oversight and a ton of
2 laws to comply with.

3 I personally am much more worried about
4 the large collection, amount of collection that's
5 taking place in industry that people don't really
6 understand.

7 MS. WALD: All right. So I can go on to
8 my next.

9 Mr. Bedoya, you talked about how
10 important it was to limit collection to what was
11 necessary or purposeful, etcetera, but in light
12 of so many of the experts on both panels have
13 talked about almost like an almost inevitable
14 momentum of collection, collection, collection,
15 where would you look, what part of the government
16 or where would you look for the mechanism to try
17 and limit the collection, or get that kind of
18 impediment or balance done?

19 MR. BEDOYA: Certainly. So I think
20 folks have been saying that it's inevitable that
21 industry is going to collect all this data. I
22 don't think folks have been saying that it's

1 inevitable that government will collect it.

2 And I, for one, don't actually think
3 it's inevitable that industry will collect it.

4 But taking that as a given, I think the
5 question is about reconstructing the firewall
6 between government and industry with respect to
7 data collection.

8 And so I'd be surprised if anyone on the
9 panel thinks, or on the previous panels thinks
10 that it's inevitable the government will collect
11 all this data.

12 One quick other point, Judge Wald, on
13 your previous question, I should note that I
14 believe that the congressional committees that
15 conduct oversight on FISA and on foreign
16 intelligence, certainly the Senate Judiciary
17 Committee lacks a technologist, and I think
18 that's an issue that needs to be addressed.

19 MS. WALD: I think we talked a little
20 bit about that in our first report on FISA
21 reform.

22 Okay, Mr. Hintze, you talked earlier,

1 you said one of your principles was there
2 shouldn't be any bulk data collections.

3 Now terminology is varied all over the
4 place, so it would help me if I knew what you
5 meant by bulk collection there.

6 And let me just tell you, one gathering
7 of public health people and they talked about the
8 great importance of public health data, you know,
9 especially for when epidemics come along or that
10 sort of stuff.

11 So wouldn't some of that come under your
12 ban against all bulk data collection?

13 MR. HINTZE: I was talking specifically
14 about government surveillance programs that come
15 to industry.

16 MS. WALD: Okay, I just wanted to
17 clarify that because -- and what do you mean by,
18 give us an example of what you would call bulk
19 data. Because this has been a debate as to
20 whether this program or that program falls under
21 bulk data.

22 MR. HINTZE: Certainly. I had in mind

1 the 215 program in particular where government
2 goes to service providers.

3 MS. WALD: Where it's not targeted?

4 MR. HINTZE: Yes, it's not targeted,
5 correct.

6 MS. WALD: I think that's all I have
7 right now.

8 MR. DEMPSEY: We may be able to go back
9 to Board members for additional questions. I
10 would like to continue with this panel up until
11 the top of the hour.

12 We have one question from the audience
13 which I will read, and we welcome others if
14 others want to pose questions.

15 In 2005, the National Academy of
16 Sciences studied whether pattern-based data
17 mining can anticipate who was likely to be a
18 future terrorist. It concluded that this wasn't
19 feasible.

20 And the question is, is pattern-based
21 data mining in the terrorism context, is it
22 feasible today and will it be feasible ten years

1 from now? Would anybody like to address that?
2 Hadi?

3 MR. NAHARI: I don't know specifically
4 about terrorism. I'm mindful of what Ed
5 mentioned is that we have limited data.

6 But there is a program that has been
7 running in Los Angeles in LAPD. We may not
8 necessarily still be able to identify specific
9 criminals, but our predictive modeling systems
10 have been at work. They're able to make a
11 reasonably good prediction about where the
12 criminal activities are more likely.

13 It is not precisely the question that
14 you're asking, but I can assure that it is just
15 becoming better. I can assure that any service
16 provider that has the amount of data that we are
17 generating, and it's becoming more and more and
18 more generated, is just honing and fine tuning
19 and polishing their models.

20 Whether it's going to be applicable to
21 antiterrorism methods, I don't know. I think all
22 of these models are heavily data-driven. So one

1 would need a lot of data.

2 But to the point that these models,
3 these predictive modeling are able to predict
4 things may relate indirectly to terrorism or
5 criminal activities, the systems are suggesting
6 that we are going that way.

7 MR. DEMPSEY: Other thoughts on that
8 question?

9 There's a system in Chicago that the
10 Chicago Police Department has deployed, which
11 both has been touted and criticized, but it does
12 somewhat at the neighborhood or block level
13 predictive or predictions as to criminal activity
14 as well as, I understand, individual level,
15 identifying people who may be either victims of
16 crimes or perpetrators of crimes. Again, both
17 touted and highly criticized.

18 Any thoughts or comments?

19 MR. BEDOYA: One just quick one, which
20 is the risk of creating a feedback loop. You
21 know, if you predict that there will be crime on
22 corner X, you watch corner X like a hawk, you see

1 every crime that occurs on corner X and you
2 therefore draw an over-represented sample of
3 crimes at corner X, reinforcing your prior
4 conviction that you thought corner X was real
5 dangerous. So that's the main one from my
6 perspective.

7 MS. ANTON: So this is certainly not
8 necessarily my area of expertise, however
9 predictive is different from being able to
10 reconstruct after the fact. And so can we use
11 these things to then, when something has
12 happened, go back and find whether we missed
13 certain people that are still involved? Yes, I
14 do believe that's the case.

15 In terms of predictive, I think we have
16 a ways to go. By the same token I get, every
17 morning I get a crime ratings, a crime report for
18 all the crime in my area. And I can tell you, I
19 can predict where there's going to be, on a
20 weekly basis, crime in my neighborhood. So, you
21 know, we're getting there.

22 MR. DEMPSEY: Well, I mean on some level

1 that's just Comstat all over again, the systems
2 that have been available to police for decades.

3 MS. ANTON: Sure.

4 MR. DEMPSEY: One question, and I'll go
5 down the row again, and I'll pose the question
6 and I think we can just go down the row with
7 additional Board members if they have, the Board
8 members have additional questions.

9 I had said in talking to each of the
10 panelists that I didn't want this to be a panel
11 about going dark and the implications of
12 encryption, but several of you have alluded to
13 encryption and its significance here, and I would
14 ask any of you who would, to comment on the
15 following, which is, there is a growing trend
16 towards more and more devices, cheaper and
17 cheaper wearables, and the Internet of things,
18 and more and more data collection occurring.

19 There's also it seems a trend towards
20 more encryption by default, whether it's at the
21 device level or, as Mike Hintze was referring to
22 in terms of the encryption of data flowing

1 between data centers.

2 So it seems to me like we have two
3 things going on at once, which is not unusual.
4 Somebody referred to the modern era, the era of
5 the Internet of things, big data, ubiquitous data
6 flows, as the golden age of surveillance.

7 And it seems to me that both trends will
8 always be there. More and more information
9 available both to the private sector and possibly
10 to the government, and increasing pervasiveness
11 or at least increasing diffusion, if not
12 comprehensive diffusion of encryption.

13 Comments on that as a premise, first of
14 all, the premise of my question, am I right?

15 And then secondly, where does that leave
16 the government, and would you agree with my
17 assumption that there will still be huge amounts
18 of information available, both to the private
19 sector for its purposes, as well as to the
20 government?

21 I guess let's go right down the row.

22 Professor Anton?

1 MS. ANTON: So I believe that there will
2 still be a lot of data that's available to
3 government. When I say that I really support
4 encryption by default, I also really think that
5 our country really, we were the code hackers, and
6 it was really critical in World War II.

7 And I think that instead of just kind of
8 taking the lazy approach and saying, oh, leave us
9 a backdoor, that we should just get better at
10 cracking the code, because they're getting
11 smarter and we need to get smarter, too.

12 And so I leave it to the lawyers to
13 decide what the legality of when you can actually
14 apply that or break into a system.

15 But being satisfied with just having a
16 backdoor means that we're not advancing our state
17 of the craft and our tradecraft here in this
18 country and we're going to be left behind as a
19 result.

20 MR. BEDOYA: I'll actually pass.

21 MR. DEMPSEY: Yeah, my thoughts on this,
22 two trends seem to be occurring simultaneously.

1 MR. HINTZE: Yeah, I mean we're
2 certainly seeing an expanded use of encryption,
3 encryption between customers and the service
4 provider, and encryption between data centers,
5 encryption on devices, etcetera.

6 And that's being driven by customer
7 demand. I mean customers are concerned about the
8 security of their data. And they're not just
9 concerned about the security of their data
10 vis-a-vis hackers and bad guys, they're
11 increasingly concerned about the security of
12 their data vis-a-vis governments.

13 And so to the extent that there is that
14 concern out there that's driving customer demand
15 for these security features and companies will
16 continue to invest in that.

17 Does that mean that there will be no
18 data available? I don't think so. I mean the
19 nature of many cloud services requires service
20 provider access to it.

21 You can't run an effective email system
22 without being able to filter the content for spam

1 and malware.

2 And so there will be a point in the
3 communication chain where data is available, and
4 that means that if it's available to a service
5 provider, it's available to a government through
6 lawful demands. So I guess that's it.

7 MR. DEMPSEY: Hadi, any thoughts on
8 this, and then I'll yield.

9 MR. NAHARI: First off, I want to agree
10 with Dr. Anton's point, we should just get
11 better. We cannot ask industry, oh, don't
12 encrypt, don't do anything. I would love to
13 follow that when Chinese and Russians also follow
14 that as well. So that's just not going to work.

15 I'm very respectful of the problems that
16 the law enforcement agency has with the current
17 state of affairs. We just have to get better.

18 And it works, at the end it's going to
19 work better for us as a nation. So that's number
20 one, I fully agree.

21 Some of the things, so going dark, I
22 don't know if it's going dark. I know that we

1 are currently in a state that we are really able
2 to think a certain way about the system design,
3 about the system security, about maintaining
4 privacy, that world has changed.

5 The world and the industry has changed
6 rapidly. The rest of us are catching up. So I
7 think it pays dividend if we figure out, take
8 some time, figure out what are the rules of this
9 new world where we don't necessarily need to rely
10 only on encryption.

11 I'm a big fan of encryption. I think
12 it's one of the tools that security professionals
13 and everyone has, but there are others. The fact
14 that some data is encrypted is not on its own
15 necessarily the end of the world.

16 I mean how many times, I know Michael
17 mentioned that we are overusing this notion of
18 metadata, but if you think about metadata as
19 something about the data, it is meaningful when
20 you see some encrypted data is being accessed a
21 little bit more than the other. One could
22 discern, one could learn things about it.

1 Once we start learning how to deal with
2 this system, then we could maintain encryption,
3 then we could maintain stronger encryption. We
4 could also deal with the cases where we don't
5 have access to clear.

6 I think our law enforcement, I think our
7 government, I think our legal system, I think us
8 as a society are in the process of learning how
9 to deal with this new world where things that we
10 knew in the past no longer apply.

11 Lastly, the new generation have figured
12 it out. I think they're doing a lot better.
13 They're figuring out that you cannot expect
14 everything is going to be fully protected for
15 you. They're figuring out ways to live in the
16 world where they're posting a lot of things on
17 Facebook that, I mean us probably won't do.

18 They're trying to learn how to deal with
19 a system that, you know, you may not have the
20 capabilities of asserting your privacy in the way
21 that our generation did, but still have an
22 expectation about their rights.

1 MR. DEMPSEY: Does a particular Board
2 member have a question? Yes?

3 MS. BRAND: Several of you have referred
4 to oversight in one way or another and I just
5 want to ask a question about that.

6 In my view, oversight is especially
7 important in the intelligence context because of
8 the necessary level of secrecy that attends.
9 It's important in all areas of government, but
10 especially here.

11 But at the same time, when you start to
12 layer on box checking exercises and paperwork
13 there is a point of diminishing returns and you
14 sort of have oversight for its own sake that
15 doesn't actually deter misconduct or ensure
16 compliance with the rules.

17 Do any of you have thoughts on
18 principles for what's effective oversight, as
19 opposed to just another box checking exercise?

20 MR. BEDOYA: So I certainly have a few
21 thoughts for the legislature. I think that
22 there's been a lot of soul searching around how

1 the executive needs a change in practices with
2 respect to internal oversight. But I think
3 there's some pretty serious problems at the
4 legislature.

5 One of them is the technologist issue
6 that I mentioned. Another is clearances. I can
7 say with moderate to high confidence that most
8 United States senators lack a staffer with TSSI
9 clearance. I hope I'm wrong. I don't think I
10 am.

11 And the fact is that all of the key
12 briefings for these senators are conducted at
13 that level. And as a staffer, I know there's a
14 lot of staffers in the room, you don't send your
15 boss into a meeting about soybeans without a TSSI
16 staffer -- sorry, no, you don't need a TSSI
17 staffer for that, but you don't send them into a
18 meeting on an issue that seems very easy without
19 a staffer. And a lot of these folks are going in
20 on staff.

21 Now thankfully folks on judiciary and
22 intel have dedicated TSSI folks for the committee

1 that they can rely on, but outside of those
2 committees you're often flying, I don't want to
3 say flying blind, but you don't have the
4 resources you need to actually conduct that
5 serious oversight.

6 MR. MEDINE: I have two questions for
7 Professor Anton on de-identification.

8 One is you commented earlier that phone
9 numbers without names associated with them would
10 be de-identified information --

11 MS. ANTON: It's actually not
12 de-identified, because if it's my cell phone, I
13 stand corrected on that.

14 MR. MEDINE: Okay. Because obviously
15 the availability of reverse directories makes
16 that --

17 MS. ANTON: Absolutely, sorry.

18 MR. MEDINE: Then I guess you also had
19 commented earlier that by analogy of having a
20 lock on your door was a pretty good protection
21 against burglars but obviously not a perfect
22 protection.

1 And I guess the question is, in the
2 context of a massive database burglars may not
3 have the incentive or wherewithal to break into
4 everyone's home in a community, but with a
5 massive database with a brute force attack, you
6 might be able to get a very valuable return on
7 it.

8 So does that suggest that
9 de-identification needs to be essentially
10 stronger or may not even be sufficient?

11 I mean as you pointed out on the Netflix
12 example, and Professors Paul Ohm and Latanya
13 Sweeney have written articles about the ability
14 to de-identify, is it a useful tool in some
15 instances but not others?

16 And even where it's useful, does it to
17 have to be a pretty enhanced form of
18 de-identification?

19 MS. ANTON: Well, I think it's better
20 than nothing. You have to work harder at it to
21 get access to it, right, and to really be able to
22 understand it. But that's going to help us with

1 the, you know, high school kid who's just trying
2 to tinker around, right?

3 But I think this is another example
4 where encryption is really, really important, and
5 very strong encryption. And so I think it's a
6 blend of both.

7 MR. MEDINE: Thank you.

8 MS. COLLINS COOK: Just on the issue of
9 de-identification and anonymization, I had
10 understood it as a concept that could apply in
11 varying degrees. So at a period of time it has
12 been de-linked from the identifying information
13 and now they have to go to court in order to
14 re-associate it with the identifying information.

15 So I don't think I was asking you to say
16 that it had been permanently de-identified or
17 anonymized.

18 This question is for Mr. Bedoya. To the
19 extent that we're looking at evolving standards
20 or evolving notions of expectations of privacy,
21 how do you quantify it?

22 Is it because 51 percent of folks in a

1 Washington Post poll said I care about this but
2 I'm still using Facebook? Do you look at
3 conduct? Do you look at the fact that people
4 inside the beltway really care? People in ivy
5 leagues really care? I struggle with what is a
6 good way to identify emerging notions of
7 expectation of privacy.

8 MR. BEDOYA: I'm not going to pretend to
9 know the right answer to that question. It's a
10 really, really hard question.

11 I certainly think that looking at
12 conduct is extremely valuable, and there's been a
13 lot of discussion about the third-party doctrine.
14 And the fact is it doesn't remotely represent
15 what the American people think about privacy.

16 You know, if your social network only
17 had the settings of public and only me, that was
18 the only option, you know, people would say this
19 is ridiculous.

20 And I do think it sounds strange to say
21 it, but we do have something to learn from the
22 best practices of these social networks, in that

1 they very much see the world as a series of
2 segments and they respect the fact that sometimes
3 you want to share something with segment A and
4 not segment B. And so I would say that's
5 certainly valuable.

6 I don't have a good test about
7 identifying a reasonable expectation of privacy.
8 I'll just repeat myself in that I think we need
9 to see that as a standard that can expand and
10 contract.

11 MS. ANTON: If I could quickly add,
12 after the Snowden leaks there's an anonymous
13 search engine called DuckDuckGo and the number of
14 people who started doing searches on that search
15 engine increased, I think by over a hundred
16 percent. So there's one way that you can watch
17 people's actions and conduct.

18 MR. HINTZE: Just one very, very quick
19 add-on to that. It's not a binary thing. You
20 can't say that people say they care about privacy
21 but they continue to use Facebook.

22 You have to look deeper. You have to

1 look at about how they're using Facebook, whether
2 they're using the privacy controls, how they're
3 engaging in those services, because if you look
4 deeper you see some pretty sophisticated choices
5 that people are making in ways to protect their
6 privacy that's not apparent on the fact that, oh,
7 you're using a social network, you must not care
8 about privacy.

9 MS. WALD: I have a question. Between
10 the two panels, the first panel and the second, I
11 heard, I hope correctly, that there is some
12 difference of opinion on a couple of things, or
13 maybe slight.

14 I think, Ms. Anton, you suggested in
15 answer to a prior question of mine that you
16 thought the government was indeed involved in
17 trying to build privacy into the technological
18 aspects of some of the programs.

19 On the other hand, earlier I think you
20 said that in threat modeling very little privacy
21 considerations were going into that.

22 Other people said that it wasn't

1 inevitable that the government would keep
2 collecting more and more information, but I think
3 I got that impression that maybe it seemed to be
4 going that way from Mr. Felten on the earlier
5 panel.

6 So my question is basically, very
7 briefly, if there were one area of priority, if
8 you were running the government's overall privacy
9 protection that you would suggest they
10 concentrate on and could perhaps improve privacy
11 protection without endangering national security,
12 what would it be? If you can do it very quickly.

13 MS. ANTON: I think that we really need
14 to work more on privacy standards and not privacy
15 standards globally, and also that aren't rigged
16 in some way to help some government or sector of
17 industry. I think that's the number one
18 challenge right now.

19 MS. WALD: Other people?

20 MR. BEDOYA: Yeah, I would say it's
21 ending programs that involve the bulk collection
22 of American's data.

1 MS. WALD: I couldn't hear the end.

2 MR. BEDOYA: Ending programs that
3 involve the bulk collection of American's data.

4 MS. WALD: Okay. Do you have in mind
5 any except 215?

6 MR. HINTZE: I didn't have the TSSI
7 clearance so I don't know.

8 MR. DEMPSEY: Okay, Mr. Chairman?

9 MS. WALD: Wait a minute, there was
10 somebody wanted --

11 MR. DEMPSEY: Oh, I'm sorry. Yes,
12 please.

13 MR. NAHARI: One last thing, and I don't
14 know if this is the elephant in the room. One
15 thing I would put as an item priority is our
16 systems and the technology are very much built as
17 one way. So I would introduce a notion of
18 revocation.

19 So if something goes bad right now, if
20 I'm releasing all of this information, there is
21 no way for a user, for a citizen to go ahead and
22 push a button somewhere and say revoke all the

1 rights that I gave to XYZ service providers and I
2 want to go ahead and clear everything.

3 So defining what that revocation means,
4 what are the ramifications of that, and how to
5 crystallize it as a requirement for the industry
6 would go a long way for things that we could
7 build.

8 MS. WALD: That would go primarily to
9 industry, that wouldn't affect government. I
10 mean if I gave the government some information
11 under some program which I thought was going to
12 benefit me and later on it turned out it was
13 being used in a different way, would your
14 revocation principle apply there?

15 MR. NAHARI: If I have the right to
16 revoke whatever government had collected about me
17 and I knew things that our government, in the
18 possession of government and I was able to revoke
19 that, perhaps that would be helpful.

20 MS. WALD: Thank you.

21 MR. DEMPSEY: So this concludes our
22 second panel. It concludes our morning session.

1 We will reconvene at 1:15 with a panel of
2 government privacy officers.

3 (Off the record.)

4 MR. MEDINE: Good afternoon. The
5 Privacy and Civil Liberties Oversight Board's
6 meeting on defining privacy will continue with
7 our afternoon session with government panelists
8 moderated by a member, Beth Cook.

9 MS. COLLINS COOK: So welcome back to
10 folks who were here earlier, or welcome to those
11 who were not here.

12 Just quick one piece of housekeeping,
13 what we've noticed this morning is make sure, and
14 Alex, this will be particularly relevant for you,
15 make sure the microphone is actually the
16 direction you are talking, so that even if you
17 pull it in front of you but then turn to talk to
18 us, make sure the microphone is picking up. They
19 were having problems this morning and we've all
20 been gently reminded as well.

21 All right, so this panel is about the
22 privacy interests identified and addressed by

1 government privacy officials.

2 Obviously in the counterterrorism
3 context defining and expressly articulating
4 individual privacy interests while balancing the
5 needs of national security is an extremely
6 challenging task.

7 As we discussed a bit this morning,
8 widely accepted privacy frameworks like the Fair
9 Information Practice Principles or traditional
10 privacy impact assessments may very well be
11 intentioned with the necessity to protect
12 information regarding the operation of a
13 particular counterterrorism program.

14 By the same token, some counterterrorism
15 programs could be better served with greater
16 transparency about what information is being
17 collected, about the statutory authorities or the
18 authorities pursuant to which programs are being
19 operated, and about what protections the
20 government utilizes to minimize the negative
21 impacts on individuals' privacy.

22 So the panel that we have assembled

1 today for this forum is, I think, uniquely
2 situated to discuss these privacy issues that
3 arise in the context of federal counterterrorism
4 programs.

5 These officials not only assess the
6 privacy impacts of a full spectrum of
7 counterterrorism programs they have also been
8 pioneers, many of them, in the practice of
9 working proactively within the agencies to ensure
10 privacy and civil liberties concerns are taken
11 into consideration from the beginning of
12 programs.

13 And if that were not enough of their
14 duties, they also are learning to live with us
15 and work with us.

16 Joining me today are three individuals.
17 Unfortunately DHS was not able to make anyone
18 available for this as it turned out.

19 So we have three folks. They will have
20 ten minutes, given that they have a little bit of
21 extra time, few folks, but we will follow the
22 same basic framework.

1 I will then ask a series of questions
2 for a period of time and then invite my fellow
3 panelists to submit questions as well.

4 So leading us off is Alex Joel who is
5 the Civil Liberties Protection Officer for the
6 Office of the Director of National Intelligence.

7 Do you actually fit that on one card?

8 MR. JOEL: Yes, I do.

9 MS. COLLINS COOK: That's amazing.

10 So in that capacity he leads the ODNI's
11 Civil Liberties and Privacy Office and he reports
12 directly to the Director of National
13 Intelligence.

14 Prior to joining the government, and I
15 think this is also relevant based on our other
16 panels, Alex served as the privacy, technology
17 and e-commerce attorney for Marriott
18 International, where he helped establish and
19 implement Marriott's global privacy compliance
20 program, including the creation of Marriott's
21 first privacy officer position.

22 So, Alex, did you want to kick us off?

1 MR. JOEL: Yes, thank you. And I want
2 to thank the Board for --

3 MS. COLLINS COOK: Oh, I'm sorry,
4 there's a stop light function going on here,
5 green, good to go, yellow, start wrapping up,
6 red, stop, in the front row.

7 MR. JOEL: Okay. I want to thank the
8 Board for inviting us here to address the public
9 in this very important hearing.

10 And as you said, the Board does work
11 very closely with us. We feel that the Board's
12 role in providing both transparency and
13 oversight, as well as advice to the intelligence
14 community has been extremely valuable and is a
15 critical part of how the intelligence community
16 protects privacy and civil liberties.

17 So I want to thank the Board for holding
18 this hearing and for the Board's very diligent
19 and careful efforts to exercise their statutory
20 functions, which I think have been critically
21 important.

22 This topic is, of course, one that

1 consumes all of us, not specifically how to
2 define privacy, but how to apply protections
3 required to protect privacy in the context of our
4 activities and in particular in the context of
5 counterterrorism activities.

6 I'd like to just get to what I think of
7 as the heart of the matter from an intelligence
8 community perspective in any event, which is that
9 we operate by necessity within a sphere of
10 secrecy.

11 We have to be able to maintain secrets
12 in order to be effective. The more publicly
13 transparant an intelligence service is, the more
14 it informs adversaries of how the agencies are
15 collecting information and the better able those
16 adversaries are to avoid detection.

17 So as I've said in the past, a fully
18 transparent intelligence service is by definition
19 an ineffective one.

20 The key for us then is how within the
21 sphere of necessary secrecy do you make sure that
22 the intelligence agencies are acting

1 appropriately, lawfully, and in a way that
2 protects people's privacy and civil liberties
3 consistent with the values of the nation.

4 In the past what we have done, as you
5 know, is focused on ensuring that we are
6 providing full transparency to our oversight
7 entities. And our oversight system is something
8 that I would like to characterize as a system of
9 many layers with many players.

10 We have not only within each agency,
11 offices of general counsel and offices of
12 inspectors general, as well as newly created
13 privacy and civil liberties offices, but outside
14 of the agency we have entities like the
15 Department of Justice, which is responsible on a
16 government-wide basis for exercising some of
17 these authorities and oversight controls.

18 We have of course newly created entities
19 like the Privacy and Civil Liberties Oversight
20 Board, perhaps not that new anymore, which again
21 is designed to make sure that there is a secure
22 place for information to be disclosed and

1 discussed so that the oversight institutions are
2 satisfied that the activities being conducted are
3 proper ones.

4 Then of course we have Congress and the
5 judiciary, both of which exercise robust
6 oversight. And I would mention that, for
7 example, the congressional oversight committees,
8 which were established particularly after the
9 Church Committee hearings in the 1970s to provide
10 this granular level of oversight over
11 intelligence activities, has been very effective
12 in my view in providing careful oversight of what
13 we do.

14 So that's sort of the oversight part of
15 the equation. I think what we have now more
16 fully realized is the need to enhance
17 transparency.

18 So if you think of it, I mean I was just
19 thinking about this before I started talking,
20 which is always dangerous, but if you think of it
21 as operating within a sphere of secrecy, one way
22 is to make sure that the mechanisms, the rules

1 and oversight structure within that sphere are
2 robust enough to make sure that privacy interests
3 and civil liberties interests are being
4 adequately protected.

5 And then there's the other way of
6 approaching this, which we're also focusing on
7 doing, which is reducing that sphere.

8 In other words, providing greater
9 transparency into what goes on inside the
10 intelligence agencies so that the public at large
11 can get reassurance and can also provide input
12 and feedback into how we conduct these
13 activities.

14 I think if I could just continue along
15 this theme, there are two aspects in particular
16 of what goes on to regulate our activities that I
17 think is of interest. One is the rules that we
18 follow, and the other is the oversight framework
19 and mechanisms designed to make sure we're
20 following those rules.

21 So I think on the former, what are the
22 rules that we follow? We can and should provide

1 greater transparency, but a lot of those rules
2 are now currently being debated and discussed,
3 and you can think of some of the reform
4 mechanisms as attempts to modify those rules.

5 So you have the activity going on in
6 Congress, for example, the USA Freedom Act and
7 similar legislative initiatives.

8 You have as part of that also the
9 proposal to create an advocate of some kind, an
10 adversarial mechanism for the Foreign
11 Intelligence Surveillance Court.

12 Here again in my view is an attempt to
13 influence or affect what are the rules that the
14 intelligence agencies are expected to follow.

15 And then a different part of that
16 question is what oversight mechanisms, what
17 assurances do we have that the agencies are, in
18 fact, following those rules.

19 And you're part of that. I've already
20 mentioned the congressional committees, the
21 Foreign Intelligence Surveillance Court, and then
22 all the layers within the executive branch itself

1 at the intelligence community and the Department
2 of Justice level.

3 So I think, I hope that the public
4 discussion has been shifting a bit from whether
5 or not we're following the rules. I think what I
6 perceived in the public discussion is a greater
7 acceptance that we are in fact trying our best to
8 follow the rules. We're not perfect and we make
9 mistakes, but we're trying to follow those rules
10 as best as we can.

11 And now the discussion has been shifting
12 to, well, what should those rules be? What are
13 the rules, and what should those rules be?

14 I think we can and must provide greater
15 transparency into both sides of that equation,
16 and we're working on that.

17 I would also say that another thing that
18 I know the Board has been pursuing which is the
19 recommendation that the Board made in the 702
20 report regarding efficacy, you know, to what
21 extent are the counterterrorism programs and
22 measures effective and to what extent do they

1 provide value is a key part, in my view, of the
2 transparency equation as well.

3 We have to figure out ways to identify
4 the specific value associated with particular
5 programs and activities, and then be more
6 transparent about that so that the American
7 people can render a judgment, as well as everyone
8 else, on the need or desirability for a
9 particular kind of program.

10 It is very difficult to do all this
11 stuff and still maintain secrets. The
12 intelligence community is not built for
13 transparency. I've said this before, it's built
14 for exactly the opposite, of course.

15 We train, provide policies and systems
16 and reminders to our workforce of the importance
17 of maintaining secrets, you know, maintaining
18 secret the sources and methods that the
19 intelligence community uses to carry out its
20 activities. And this is vital. I mean we have
21 to do that and we're reminded of that need all
22 the time.

1 But at at the same time, we have to find
2 ways to enhance transparency. It's going to
3 involve some changes in culture, training, a look
4 at policies and processes within the intelligence
5 community and I know that you may want to ask
6 questions about that, so I look forward to that
7 discussion.

8 So thank you again. I appreciate it.

9 MS. COLLINS COOK: So turning now to
10 Erika Brown Lee, she is the Chief Privacy and
11 Civil Liberties Officer of the Department of
12 Justice. In that capacity she is the principal
13 advisor to the Attorney General on privacy and
14 civil liberties matters affecting the
15 department's missions and operations.

16 And as part of the Office of Deputy
17 Attorney General, Ms. Brown Lee oversees the
18 department's privacy and civil liberties programs
19 and initiatives implemented by department
20 components and component privacy and civil
21 liberties officials.

22 She also heads the Office of Privacy and

1 Civil Liberties, which reviews and evaluates
2 department programs and initiatives, and provides
3 department-wide legal advice and guidance to
4 ensure compliance with applicable privacy laws
5 and policies, including the Privacy Act. Thank
6 you for coming.

7 MS. BROWN LEE: Thank you, and thank you
8 to the Board for inviting me here to talk about
9 what is a very important topic.

10 You asked about private sector
11 experience and other government experience, I
12 also come from the Federal Trade Commission,
13 which in particular the Division of Privacy and
14 Identity Protection, which of course the Federal
15 Trade Commission has a very different orientation
16 toward the commercial side of privacy, but
17 nonetheless an important perspective and an
18 interesting one to bring to this position.

19 But counterterrorism is a significant
20 part of the department's mission. Since my
21 colleagues on the dias today will be talking from
22 more of an intelligence lens, I thought I would

1 orient my remarks more toward the department's
2 efforts to fight terrorism from within the
3 criminal law enforcement context.

4 The department has an elaborate
5 architecture that protects privacy in our
6 counterterrorism work, and since I only have a
7 few minutes I'll focus on the lead agency in
8 those efforts, which is the FBI and focus in a
9 little bit more on the efforts with their
10 counterterrorism activities.

11 But stepping back for a minute, of
12 course as we know after 9/11, it was recognized
13 that in order to address the current threat
14 environment, FBI's functions needed to be
15 expanded, but it was not intended that the
16 expansions would come at a cost of civil
17 liberties.

18 So in 2008, the department issued the
19 Attorney General Guidelines for Domestic FBI
20 Operations, the AGG-DOM, and later that year
21 issued the DIOG, or the Domestic Investigations
22 Operations Manual. And combined, those two

1 documents provide significant guidance for FBI
2 activities.

3 But what I wanted to talk about, and I
4 know I don't have enough time to get too far into
5 the weeds, is just to explain how privacy is sort
6 of embedded throughout the stages of an
7 investigation, from the initial phase throughout
8 the process.

9 And so, for example, one of the key
10 tenants of both documents is the least intrusive
11 method. So in other words, in any activity that
12 the FBI engages, that's the baseline.

13 But of course within the
14 counterterrorism context, it's got to be
15 calibrated against the threat to national
16 security, in which case more intrusive methods
17 would be used.

18 But in terms of a little bit more detail
19 from an operational context, when an FBI conducts
20 an assesment, for example, which necessarily,
21 well not necesssarily, but oftentimes is
22 proactive, that would involve, doesn't require a

1 factual predication, but it does require a
2 clearly defined objective.

3 And the least intrusive methods in that
4 context would be even starting with publically
5 available information, to voluntarily provided
6 information, in that perspective.

7 And then moving up from there with
8 regard to predicated investigations, which of
9 course implies by title, there requires a factual
10 predication to open that investigation, but that
11 has to have supervisory approval.

12 And both types of investigative
13 activities, whether it's assessments or
14 predicated investigations require or are, I
15 should say, subject to oversight.

16 Alex mentioned DOJ oversight on the
17 intelligence side, but also on the law
18 enforcement side for counterterrorism, the
19 department's National Security Division has
20 oversight authority for those kinds of
21 activities.

22 Now Beth mentioned and asked us to talk

1 about or think about how the FIPS apply, if
2 you're looking for the acronym, there's lots of
3 them in the documents, but it's not actually in
4 the AGG-DOM or the DIOG. However, they are
5 embedded throughout really, the principles.

6 If you think about, even from a
7 transparency perspective, right, all that I'm
8 discussing with regard to the DIOG, all 700 pages
9 of it for a little light reading, for anyone
10 who's interested it's on the web with certain
11 redactions.

12 But also we have privacy impact
13 assessments that are available. And one that I
14 wanted to just mention in particular regards the
15 eGuardian system because that is a specific
16 system or incident reporting system that is
17 designed as a platform to share terrorism-related
18 information across law enforcement, you know,
19 federal, state, local, tribal, territorial
20 jurisdictions.

21 So eGaurdian, I don't have time to go
22 into much detail about it, but it has an entire

1 architecture of privacy protections governing how
2 information comes into eGuardian, how it's shared
3 across those entities, how it's stored and how
4 it's retained.

5 Individual participation as a FIPS
6 principle, obviously that's more of a challenge
7 in a law enforcement context. It's not realistic
8 to be able to obtain individual consent in order
9 to pursue criminal investigations.

10 But nonetheless, the Privacy Act
11 provides some measure of review in the sense that
12 if access or amendment to records is denied,
13 there is judicial review of an agency's decision,
14 and subject to court order, records may be
15 amended or access may be granted.

16 On the minimization side, I mentioned
17 the least intrusive means already with the DIOG.
18 There's also a prescriptive measure in the DIOG
19 with regard to evidence collected, that if the
20 evidence collected through an assessment or
21 through a predicated investigation has no
22 foreseeable future evidentiary or intelligence

1 value, it should be returned and destroyed, and
2 then marked in the file in term of the
3 disposition of that piece of evidence.

4 Otherwise, information is retained
5 according to the schedule set by NARA, the
6 National Archives and Records Administration, and
7 approved, through which the Department of Justice
8 would seek approval for.

9 With regard to use, I think that's also
10 a challenge. On the criminal side of course
11 willful disclosures of protected information
12 under the Privacy Act are not something that any
13 agency can exempt themselves from.

14 And to the extent that information is
15 released that's not subject to a routine use or
16 other permitted disclosure, and of course, you
17 know, routine uses are subject to a compatibility
18 standard that tracks the FIPS language.

19 If the information is disclosed or even
20 shared in violaton of that, that's potentially a
21 wrongful disclosure subject to not only civil
22 damages but criminal penalties.

1 And then in terms of accountability, I
2 mentioned oversight from the National Security
3 Division, but also the FBI has the National
4 Security Law Branch, which conducts national
5 security reviews.

6 And that's a significant review
7 process in that they go out to all of the field
8 offices and review the investigative activities I
9 mentioned, the assessments, the predicated
10 investigations and look to see whether, in fact,
11 superviseory approval was obtained, whether, in
12 fact, there was a clearly defined objective for
13 any assessment, and it's written up into a
14 report.

15 That report actually comes through FBI
16 channels of course, but then also comes for
17 review by the Chief Privacy and Civil Liberties
18 Officer. And I look at those, obviously, through
19 a privacy and civil liberties lens.

20 So as Alex was mentioning, there are
21 lots of layers that are applicable.

22 I know I don't have much time remaining.

1 But in conclusion, I guess I would just like to
2 leave you with a couple of take-aways.

3 One is that FIPS, quite to the contrary
4 of certain statements is not dead, it's just
5 embedded.

6 And I would also say that the processes
7 can always be improved. Certainly I work with
8 the component, each component. There are over 40
9 components in DOJ, but each component has a
10 Senior Component Official for privacy and I host
11 regular meetings.

12 In fact, we're having a privacy forum
13 next week that will cover privacy-related
14 activities focusing on law enforcement, but other
15 components as well, activities, common privacy
16 issues across components. It is internal though
17 so none of you are actually invited unless you
18 happen to get a job by Monday at the DOJ.

19 But that's also something that is a way
20 to improve. And I would also say that while
21 privacy impact assessments are very important and
22 a critical part of our program because they're

1 sort of this tangible proof that we actually
2 evaluate privacy, that we mitigate the risks,
3 that we take into account security and
4 accountability, they really only form a part of
5 the architecture for the Department of Justice's
6 privacy program.

7 So, and I welcome your comments.

8 MS. COLLINS COOK: Thank you, Erika, for
9 a nice education about the FBI's operations, the
10 FBI in particular.

11 So Becky Richards is the National
12 Security Agency's Civil Liberties and Privacy
13 Officer. In this, I think, relatively new role,
14 I think it's fair to say, she provides expert
15 advice to the Director of NSA on all issues
16 pertaining to privacy and civil liberties
17 protections, and she conducts oversight of NSA's
18 civil liberties and privacy-related activities.

19 She also develops measures, which I hope
20 she will talk about, to further strengthen NSA's
21 privacy protections.

22 Prior to joining the National Security

1 Agency, she worked as the Senior Director for
2 Privacy Compliance at the Department of Homeland
3 Security.

4 MS. RICHARDS: Thank you, and thank you
5 for hosting us. I am very honored to have been
6 selected to be the first NSA's Civil Liberties
7 and Privacy Officer.

8 This is an exciting time to be a member
9 of the civil liberties and privacy community.
10 Our community is growing and evolving and will
11 help inform the debate as the nation reshapes its
12 expectations for and limitations on the
13 intelligence community activities.

14 Changes in the nature of the threat to
15 our national security, alongside rapid advances
16 of technology, as was discussed earlier, make my
17 job both interesting and challenging.

18 Technology provides us with both
19 opportunities and challenges, but ultimately we
20 must guide and shape its use to ensure the
21 fundamental rights we hold dear as a nation are
22 maintained.

1 Today I'd like to take a little time to
2 describe NSA's civil liberties and privacy
3 programs, both in the past, present, and a few
4 thoughts on the future.

5 Part of the NSA's mission is to obtain
6 foreign intelligence worth knowing derived from
7 foreign communications in response to
8 requirements and priorities validated and levied
9 upon us by the executive branch.

10 One such priority is counterterrorism,
11 but there are other threats to the nation, such
12 as the spread of nuclear, chemical or biological
13 weapons, or cyberattacks.

14 NSA also works directly with and
15 supports our troops and allies by providing
16 foreign intelligence for military operations
17 abroad.

18 As we consider NSA's civil liberties and
19 privacy programs over the past 62 years, it's
20 important to think about how the threat,
21 technological and sociatial landscape in which
22 NSA conducts itself signant mission has changed.

1 First, the threat has changed. NSA
2 previously operated in a cold war era when the
3 focus of collection for foreign intelligence was
4 directed at nation states, structured military
5 units, and foreign intelligence services.

6 While threats remain from nation states,
7 they now also come from non-state actors, which
8 require NSA to look at more, smaller and
9 decentralized targets to protect the nation.

10 The technology has changed. NSA again
11 previously operated in an environment where the
12 communications between foreign intelligence
13 targets were frequently conducted over isolated,
14 government-owned and operated communication
15 channels and equipment.

16 Now foreign target communications are
17 interspersed with ordinary commercial and
18 personal communications.

19 Additionally, the sheer volume and
20 ability to analyze and manipulate big data, which
21 has occurred as a result of significant advances
22 in information technology, can expose information

1 of a personal nature that may not have been
2 previosly discoverable and may not be of any
3 interest.

4 Third, how society thinks about civil
5 liberties and privacy has changed. We've come a
6 long and positive way in thinking about what
7 ought to be private.

8 Personally identifiable information was
9 not a mainstream issue 25 years ago. For
10 example, Social Security numbers were routinely
11 put on student ID cards and there was no thought
12 of HIPAA.

13 So with that I'd like to give a little
14 historical perspective. NSA's civil liberties
15 and privacy protections have historically been
16 driven primarily by the Fourth Amendment
17 analysis, which is also reflected in NSA's
18 authorities, Executive Order 12333 Foreign
19 Intelligence Surveillance Act, or FISA.

20 This analysis framed NSA's protection
21 program by asking where and how the data was
22 collected, i.e., usually overseas, and the status

1 of the individual or entity being targeted, i.e.,
2 is it a U.S. person or not.

3 NSA has consistently conducted
4 extensive legal analysis as it considers new
5 types of collection answering these types of
6 questions. It has built a strong compliance
7 program based on these, with compliance
8 activities embedded in our technologies and
9 systems.

10 As I have learned more about NSA and its
11 compliance regime, it became clear while this is
12 certainly one way to address privacy concerns, it
13 is somewhat different from how privacy concerns
14 are addressed outside of NSA.

15 Over the last 15 years Congress has
16 passed a variety of laws to protect privacy in
17 other parts of the government and the commercial
18 sector. These policies and laws focus more on
19 the nature and content of the data and how it is
20 used, not where it was collected or the
21 citizenship of the individual.

22 I believe we have an opportunity to

1 bring together NSA's current civil liberties and
2 privacy analysis with a broader approach to
3 privacy and civil liberties.

4 This new approach also supports the
5 President's PPD-28 mandate to recognize that our
6 signals intelligence activities must take into
7 account that all persons should be treated with
8 dignity and respect, regardless of their
9 nationality and wherever they might reside, and
10 that all person's have legitimate privacy
11 interests in handling their personal information.

12 To address a broader set of civil
13 liberties and privacy interests, I'm testing a
14 civil liberties and privacy assessment process
15 that expands NSA's views to include
16 considerations of frameworks the private sector
17 and nonintelligence elements of the government
18 use to assess civil liberties and privacy.

19 For example, for the first time in its
20 history, NSA is using the Fair Information
21 Practices Principles, or FIPS, as a framework for
22 considering civil liberties and privacy risks.

1 The FIPS are one framework through which
2 organizations can analyze the protections they
3 have in place for personal information.

4 While traditional NSA civil liberties
5 and privacy questions center on citizenship and
6 location of foreign intelligence targets, as well
7 as collection techniques, FIPS related questions
8 boil down to follow the data.

9 Data-centric perspectives mean privacy
10 officials ask a different set of questions. What
11 is the data being collected and how will it be
12 used?

13 As such, we've designed an initial
14 standarized template and during the next year
15 we'll refine the questions and process to ensure
16 we're building a repeatable, meaningful and
17 helpful process to identify and mitigate civil
18 liberties and privacy risks.

19 A critical part of the civil liberties
20 and privacy assessment process is to make sure
21 we're not merely checking off boxes, but
22 fundamentally weighing the risks associated with

1 the activity to form a holistic value
2 proposition.

3 In essence, we're asking should NSA
4 conduct a given activity, given its civil
5 liberties and privacy risks?

6 As part of the assessment process NSA is
7 documenting both standard protections, such as
8 minimization and control on who has access, as
9 well as any specialized tools designed to protect
10 civil liberties and privacy.

11 Much like privacy analysis performed in
12 the private sector and other parts of the
13 government, we're using the FIPS as the basis for
14 analyzing what existing protections are in place.

15 As we look to the future, I'd like to
16 spend a little bit of time talking about blending
17 the art and science of privacy.

18 Historically privacy tends to be a bit
19 of an art form. Several of us stand around and
20 think about how we're going to do the analysis.
21 This can be difficult when we're beginning to
22 think about big data and the complexity that was

1 being discussed this morning.

2 NSA is fundamentally a technology-
3 centric organization. We have and will continue
4 to contribute to advancing the discussion and
5 research of protecting civil liberties and
6 privacy.

7 Today the science of privacy has made
8 notable strides that include developing
9 technology and tools that promote privacy, such
10 as unique encryption capabilities, digital
11 rights management and trustworthy computing.

12 Great work in private sector and
13 academeia is also being developed on coding
14 privacy policies, such that technology supports
15 all specific uses.

16 But civil liberties and privacy
17 protections need to blend the art and science of
18 privacy if we're going to harness the potential
19 of technology and incorporate our core values as
20 a nation into this era of big data.

21 So despite significant progress in
22 privacy technology, basic privacy of principles

1 found in a strong scientific basis, have largely
2 proven elusive.

3 If we can better understand what
4 constitutes personal information and how such
5 information is used, we believe it will be
6 possible to determine whether we can develop more
7 practical approaches to evaluating the inherent
8 risk of privacy to the individual.

9 To that end, our initial thoughts are to
10 develop five sequential building blocks and to
11 introduce the concept of some very difficult math
12 into what is otherwise a very nice liberal arts
13 discussion of privacy.

14 The first one is to categorize personal
15 information. We would like to determine if it's
16 possible to identify and categorize different
17 types of personal information and what that risk
18 is to privacy.

19 Now we've heard different discussions
20 today, but we want to push folks to think about
21 is certain types of data more risky to privacy,
22 say like health data, than other information, say

1 your address, and can we think about those risks.

2 If we can do that, then next we would
3 like to determine if it is possible to identify
4 and categorize different types of use.

5 If we take both of these together, it's
6 possible to develop a categorization of both
7 personal information and uses of the personal
8 information, it should be possible to develop a
9 scientific process to assess risk.

10 This process could evaluate the risk of
11 the use of individual types of personal
12 information for different uses, as well as
13 aggregated uses of personal information.

14 Now with these three building blocks
15 being more of the scientific aspect, I would now
16 suggest we would move to an art form that looks
17 at how we build that to identify what needs to
18 have additional privacy impact analysis
19 conducted so that we're looking at that across
20 the board.

21 With all four of these together then we
22 would look to see if we could build a responsible

1 use framework that holds data collectors and users
2 accountable for how they manage data and any harm
3 it causes.

4 Building a technical means based on
5 principled scientific methodologies to support
6 the identification of civil liberties and privacy
7 risks can help us better protect civil liberties
8 and privacy in a fluid world of big data.

9 Success is dependent upon input from a
10 variety of disciplines ranging from
11 technologists, social scientists, privacy and
12 civil liberties experts, ethicists, attorneys and
13 computer scientists, to name a few.

14 We would welcome the opportunity to
15 discuss this in more detail and greater technical
16 depths at a later date.

17 With that, I thank you for the
18 opportunity and I'm happy to answer what I'm sure
19 are a couple of questions.

20 MS. COLLINS COOK: Thank you all for
21 your opening remarks.

22 Becky, I wanted to stick with you for

1 just a second. When we go and meet with y'all
2 and when we talk to y'all, there is frequently
3 someone from the general counsel's office,
4 someone from the compliance office, someone from
5 your office.

6 What are you doing that is different
7 than the general counsel's office and a
8 compliance shop?

9 MS. RICHARDS: That's a great question.
10 So the civil liberties and privacy office at NSA
11 is the focal point for questions surrounding
12 civil liberties and privacy, and it's been
13 brought to a senior leadership position at NSA in
14 order to focus on those efforts.

15 So generally speaking, our general
16 counsel will answer the legal question, is this
17 legal permissible? And they will often then work
18 with compliance for, what are the rules?

19 But we haven't had a person asking some
20 of these more difficult questions of, should we
21 be doing this?

22 Now frequently our oversight folks,

1 whether it's ODNI and DOJ, were playing that
2 role. And so I don't want you to take away the
3 idea that those questions weren't asked.

4 But it's really important to have that
5 type of a role inside the building where you are
6 working with the operators and the technologists
7 and can spend a great deal of time understanding
8 what we're trying to do and bring to bear those
9 questions.

10 MS. COLLINS COOK: Erika, a similar
11 question for you. FBI, for example, has its own
12 privacy officer, has its own general counsel, has
13 its own compliance shop.

14 What is your relationship and what is
15 your ability to provide recommendations or to
16 actually impose requirements on the FBI?

17 MS. BROWN LEE: So also a very
18 interesting question. My role and position is
19 department-wide, so of course I have oversight
20 over the compliance for DOJ as a whole.

21 Each component, as I mentioned, has a
22 senior official for privacy, but in addition has

1 general counsel's office that has significant
2 footprints in privacy. So at FBI they have their
3 privacy and civil liberties unit that's headed by
4 a chief.

5 I work quite significantly with that
6 person in that office to specifically address
7 compliance issues, to specifically address
8 privacy initiatives that I feel are important for
9 the bureau to consider.

10 Ultimately it is somewhat of a reporting
11 structure. In other words, if there is a
12 recommendation, or a particular policy or
13 statutory obligation, FBI has the responsibility
14 to comply.

15 But part of what my job is, is to
16 advocate and to make sure that that is occurring
17 on a regular basis and that looking for ways that
18 I can improve the process, looking for ways, for
19 example, I talked about privacy impact
20 assessments. Some of that is, if you look at the
21 E-Government Act, it's written fairly broadly.

22 I take, you know, a particularly broad

1 view of what I think should have assessments as
2 part of compliance there. And so that's what I
3 work in particular with the FBI on.

4 MS. COLLINS COOK: So Alex, a related
5 but different question for you. How do you
6 ensure that you have access, do you ensure that
7 you have access to what various agencies are
8 doing, or do you find yourself periodically
9 reading about new programs, alleged new programs
10 on the front page of the New York Times?

11 MR. JOEL: I'm surprised by that
12 question. Information sharing is perfect
13 everywhere in government.

14 MS. COLLINS COOK: I'm also seeking free
15 advice because obviously one of our biggest
16 challenges is going to be knowing what the
17 agencies are doing. You can't conduct oversight
18 of something you don't know is happening.

19 MR. JOEL: Right. I think that it's a
20 major challenge for all of us. I know that, as
21 you said, it's something that you're focused on.
22 I know that it's a challenge for everybody.

1 It's a matter of, first of all,
2 understanding the information flows within your
3 own agency and trying to put in place markers for
4 where it's important for you to be consulted.

5 The main way that I have just
6 practically done it, since I've been doing this
7 for about a decade now and when I first started,
8 you know, it was just me and then we built a
9 small staff over time, has been to form the
10 trusted relationships inside the intelligence
11 community and to make sure that the people that
12 I'm working with and that are in positions of
13 influence and authority to make decisions on
14 programs and activities, understand the
15 importance of consulting with civil liberties and
16 privacy professional.

17 In my own personal experience working
18 within the intelligence community has been that
19 when I first joined I was very pleasantly
20 surprised that people were so focused on
21 compliance and protecting privacy and civil
22 liberties, doing the right thing, following the

1 right directives, and even when they might feel
2 legally permitted to do something, they still
3 gave voice to their own doubts as to whether they
4 should be doing it.

5 And so I did not personally experience
6 an uphill battle in trying to persuade
7 intelligence officers, hey, it's important for
8 you to pay attention to civil liberties and
9 privacy.

10 In fact, it was sort of the opposite
11 where many people felt that they were already
12 doing that, and that it was their job to focus on
13 that.

14 For example, you mentioned Office of
15 General Counsel. I was at an office of general
16 counsel before coming to this job and we
17 certainly felt when I was there that that was
18 part of our job. We needed to look out for
19 privacy and civil liberties, and not just what
20 the law allowed, but what was the underlying
21 intent and what should we be doing in that light.

22 So I certainly didn't want to take away

1 that sense of responsibility from anybody inside
2 the intelligence community.

3 My approach had always been, it's all of
4 our jobs, it's part of our oath to support and
5 defend the Constitution. There are offices that
6 are particularly focused on that, Office of
7 General Counsel, Office of Inspector General.
8 There are intelligence oversight offices, as you
9 guys have learned, that are.

10 Now we're creating these civil liberties
11 and privacy offices and I do think we add value
12 because I think it is our full-time job to focus
13 on civil liberties and privacy, so we bring
14 focus, we bring an external perspective, and we
15 have specific expertise, and training and
16 experience that we can bring to bear, and then we
17 can become a voice, as Erika said, an internal
18 advocate for civil liberties and privacy.

19 But I mean I think different agencies
20 will find different ways of doing it. The ODNI
21 is a fairly small organization, and the ODNI
22 itself has mechanisms for understanding what's

1 going on across the intelligence community. So
2 when a particular program or activity bubbles up
3 to the point of a decision, either it comes
4 automatically through my office or somebody will
5 understand that I need to see it and route it to
6 me.

7 MS. COLLINS COOK: So a follow-up,
8 particularly to you, Alex, and Erika, both of you
9 have fairly small staffs considering the breadth
10 of your responsibilities, and we talked a lot
11 this morning about the increasing technological
12 complexity of what you are assessing.

13 Do you have the technological resources
14 to understand what systems are actually doing?
15 And I think that is both in terms of assessing on
16 the front-end whether systems or programs should
17 go live, or to the extent that there are
18 restrictions, for example, if the FISA Court puts
19 a restriction in place on a particular program,
20 ensuring that those restrictions are actually
21 functioning.

22 MS. BROWN LEE: So I think that's a good

1 point. So but as I mentioned earlier, oversight,
2 there are sort of a variety of roles in the
3 department that have oversight, particularly with
4 regard to counterterrorism.

5 But my office is fairly small in the
6 sense that given the large footprint of the
7 Department of Justice, but they work incredibly
8 hard and diligently with all of the components to
9 ensure compliance.

10 We rely quite a bit on internal
11 component work that is done to produce
12 information about what the privacy compliance is,
13 and then also with regard to auditing and making
14 sure that the privacy activities are actually
15 effective.

16 But I would also say that some of the
17 oversight, just to sort of again stress that,
18 some of the oversight isn't just through my
19 office, it's National Security Division, and FBI
20 also has their branch, so we work very
21 collaboratively.

22 And like Alex, I have found that within

1 the department there are a lot of people who care
2 very deeply about these issues. It's not
3 specifically in a privacy role as a title, but
4 they have oversight and I think meaningful
5 insight as to how the activities should consider
6 and be consistent with privacy initiatives.

7 But, you know, it is something that I
8 take into account and that's part of the reason
9 why we have these internal conferences and
10 whatnot that I'm trying to do to build upon that.

11 MS. COLLINS COOK: And Alex, what do you
12 do to make sure, the old adage is trust but
13 verify, what do you do to make sure you actually
14 understand the programs and the systems?

15 MR. JOEL: Right. So it's a variety of
16 things. One is, although I am not personally a
17 technologist, I have been dealing with technology
18 law, and legal issues and privacy issues
19 associated with technology for much of my
20 professional career.

21 So when I was at Marriott, I was the
22 privacy, commerce and IT lawyer there. And then

1 before that I was at a law firm in downtown D.C.
2 focused on large scale technology transactions.

3 That doesn't make me a specialist in
4 technology, but it does enable me to ask the
5 right questions and make sure that the
6 information is explained to me appropriately.

7 I don't have the staff resources to
8 engage a full-time technologist. I think that
9 would be helpful. I do think that you have to be
10 a little bit careful with that because what you
11 really want in that sense is a technology
12 generalist.

13 There are so many different aspects to
14 to technology, as you know. I mean that's just a
15 word that almost lacks meaning these days because
16 we use it so frequently.

17 But what NSA does for one particular
18 type of activity will differ significantly from
19 what FBI does, will differ significantly from
20 what all agencies do in terms of database
21 management.

22 So you've got database issues, you have

1 surveillance technologies, understanding
2 communications technologies, understanding all
3 kinds of different aspects to that issue.

4 And then of course the engineers and
5 technologists, as we know, speak a different
6 language from lawyers and so sometimes it's hard
7 for everyone to speak to each other.

8 So what I have been doing is making sure
9 that the information is clearly presented, that I
10 see the documentation, that I personally
11 understand it, that I trust the people who are
12 providing me that information are giving me a
13 complete picture, and then we also leverage
14 technical experts in the particular field that we
15 have access to within ODNI or through the agency.
16 So if something comes up that we don't quite
17 understand, we can reach out to somebody to have
18 them help us understand it.

19 I think with a larger staff I would try
20 to have more full-time technical expertise.

21 MS. COLLINS COOK: Becky, you had
22 mentioned that you've got a couple of pilot

1 experiments going and you mentioned also new
2 technologies that may or may not be available.

3 How are you working with the private
4 sector to leverage what great thinking is going
5 on, and is privacy a part of the procurement
6 process, for example? And has consideration been
7 given to that, that if we really want privacy to
8 be from the ground up, should it be one of the
9 procurement factors?

10 MS. RICHARDS: I'll start with the
11 procurement. We actually started with the
12 theory on procurement because in part that's how
13 we were doing things at DHS.

14 But it turns out NSA is a technology
15 company that has a huge research portion of it
16 and it also has a huge technology division. So
17 it's two different parts.

18 So I actually have a technical director
19 on staff who's here, Dave Marcos, and he and I
20 have been working through sort of how do we think
21 about the tech, how do we look at both what's out
22 in the world, and so we're actually working with

1 several different groups within NSA to do an
2 initial review of what is out there right now.

3 And they're conducting that right now so
4 we can get a sense of both from a policy and a
5 technology perspective what's going on, as
6 opposed to just things that we may know just, you
7 know, from knowing different people, whether it's
8 activities going on at MIT or Carnegie Mellon,
9 you know, to make sure we had a broad breadth of
10 understanding of what was the type of research
11 going on.

12 So they're doing that. We're working on
13 that right now, and then we're working with our
14 research folks and trying to just leverage all of
15 those things.

16 The procurment process is not really
17 helping this happen best at NSA. And I think
18 that that's, you know, each agency has its own
19 culture and its own aspects. And so a lot of
20 what I've been doing is taking the learning and
21 sort of shifting it to make sure that building
22 the program within NSA works for how NSA works.

1 And so that means that our privacy
2 program is going to look a little bit different
3 than FBI's or others. But it's based on sort of
4 how the organization functions and where those
5 key decisions are being made. So we're working
6 through that.

7 But it turns out procurement really
8 isn't really isn't quite the right place. So
9 we're looking through in terms of both the
10 technology, and the research director and others
11 to make sure we understand where those touch
12 points are. And that's a lot of why we're beta
13 testing the processes.

14 MS. COLLINS COOK: So I think I have
15 time for one last question before I turn it over
16 to my fellow Board members.

17 Alex, this one's for you. You
18 explicitly pointed to congressional oversight as
19 one of the things that the American people should
20 be aware of, that this happening, it's robust,
21 it's real.

22 A previous panelist pointed out that

1 there is potentially one significant flaw or
2 challenge with congressional oversight, and
3 that's the lack of cleared staff.

4 What has your perception been? Has
5 Congress struck the right -- yes, I'm going to ask
6 you to opine on Congress -- whether
7 consideration should be given to broadening the
8 range of individuals?

9 I think there's some comfort level with,
10 I think someone called it delegated oversight
11 within the Congress. But when some significant
12 majority of decision-makers in a representative
13 democracy don't have cleared staff, how is the
14 oversight nonetheless sufficiently robust?

15 MR. JOEL: So the intelligence oversight
16 committees have very substantial cleared staff.
17 And they of course have secure compartmented
18 information. We have SCIFs in which to review
19 all the classified information. And we have
20 many, many meetings, briefings and reports with
21 our oversight committees.

22 I guess my first response as a matter of

1 principle, yes, Congress should have the degree
2 of staff cleared it needs in order to assist it
3 to perform its oversight functions.

4 I think that intelligence community
5 assumption had been that by clearing the staff of
6 the oversight committees that that function was
7 being fulfilled.

8 I think some staff members are also
9 cleared from some of the other committees. I
10 don't have all of that information in front of me
11 but I believe judiciary has cleared staffers,
12 etcetera.

13 Whether or not that's enough staff to be
14 cleared, I don't know. I think Congress, from my
15 personal perspective, it would be helpful if
16 Congress figured out for itself which committees
17 are performing which function and which staff
18 members need to be cleared in order to oversee
19 our activities and then we can assess it.

20 But I would certainly support a desire
21 to make sure that there are enough cleared staff
22 to perform oversight, absolutely.

1 MS. COLLINS COOK: So transiting to the
2 member questions and while this is happening,
3 just a reminder there are folks with cards, if
4 you have questions that you'd like to submit from
5 the public.

6 And to keep everyone on their toes, this
7 time I'm going to start with Pat.

8 MS. WALD: Okay, you may be sorry about
9 that choice.

10 MS. COLLINS COOK: I might not be, they
11 might be.

12 MS. WALD: This is somewhat of a loaded
13 question, but it's one that's sort of in the back
14 of so much of the work we have done and will
15 continue to do.

16 You know, I laud all of Becky's
17 attempts, and your attempts to inject, Erika,
18 your attempts to inject privacy into all of the
19 various phases of intelligence.

20 But drawing upon what some of the people
21 in the first panel said this morning, let me just
22 pose a question that, for instance, several of

1 the panel members thought collection was a
2 primary focus of trying to enhance privacy
3 interests by limiting collection somewhat, and
4 leaving apart any debate about whether or not
5 collection by itself can be an injury to privacy,
6 I guess, and that's collection.

7 Also when you get, another expert talked
8 about the risks to privacy from aggregating data.
9 And we found out, for instance, in the 702 report
10 we did, when you got to the retention of data the
11 analysts might look at it and say, well, I don't
12 see any foreign intelligence purpose to this
13 piece of data if it came from an innocent person
14 who's not the target, but it's conceivable there
15 might be one down the line or some other person I
16 don't know about, the agency, so therefore, I've
17 got to bend to make sure that it's secured.

18 So it seems to me one of the basic
19 problems here will be, what's the tipping point?
20 In other words, assuming good faith on both
21 sides, there really is a national security
22 interest when you have to make a choice between

1 privacy and national security, but the real
2 question is, how much and at what point?

3 In other words, when we were doing 215
4 we were told many times we need a big haystack in
5 order to find the needle, and the bigger the
6 haystack, the more likely we are to find the
7 needle.

8 But of course a policy judgment has to
9 be made at some point. At this point, yes, we're
10 going to lose some national security things but
11 privacy is more important.

12 I guess I want to know what your
13 thoughts are about how that decision, which is a
14 basic policy decision, but it seems to come up in
15 every program that we look at, you know, how is
16 it made or how it should be made, even at the
17 most general level. You can all take a --

18 MR. JOEL: Okay, so I'll start. I'll
19 offer some general observations.

20 MS. WADE: Yes.

21 MR. JOEL: So I think on the collection
22 and use and retention point, I would say that

1 it's very important to look up each phase of
2 that. And that's, in fact, how the intelligence
3 community structures its determinations in many
4 ways. It's collection, then there's retention,
5 and then there's dissimulation.

6 And on the collection point --

7 MS. WALD: And aggregation.

8 MR. JOEL: Right. And then of course
9 when you aggregate data, you create additional
10 risks.

11 So there's no question that if your
12 concern is to protect privacy, the better way to
13 do it, and you're worried about what the
14 government's going to do with your data, it's
15 always better for the government not to have the
16 data. That's the best protection.

17 So if the government doesn't have the
18 data, there is no risk to privacy from the
19 government because they don't actually have it.
20 So that's why I think it's appropriate of course
21 to focus on collection.

22 Once a determination is made that the

1 government really needs this data in order to
2 carry out an important function, then you're
3 shifting to retention. And so there are --

4 MS. WALD: Let me just interrupt you.
5 I'm sorry to do this.

6 MR. JOEL: Okay.

7 MS. WALD: It's an old habit of mine
8 leftover from --

9 MR. JOEL: Yes, your Honor.

10 MS. WALD: When you say, really needs,
11 that's where the rubber hits the road.

12 MR. JOEL: Right.

13 MS. WALD: Because, sure, it's going to
14 be useful. So where the line is between
15 something which genuinely will be useful to you
16 but will be more of a privacy risk, and the thing
17 of, this is really necessary, because. And we
18 all know it's going to be drawn differently in
19 different case situations.

20 But that's what it always seems to sort
21 of come down to, and I'm wondering do you have
22 any thoughts about how that, which is a policy --

1 MR. JOEL: So this is where, and I know
2 Becky, but before you used the term tipping
3 point, which I think is a very helpful term, and
4 sometimes people think of this as a balance or as
5 a scale.

6 The way that I think of the balance
7 metaphor as it might apply here is not that
8 you're saying, well, that tips it over here so
9 therefore we're going to do it, that tips it over
10 here therefore we're not going to do it.
11 Although to some extent, of course, that happens.

12 The way that I think of it is that if
13 you're going to do something new, a new or
14 different collection program, you ask the
15 following questions, A, is it lawful? Of course
16 it has to be lawful. Is it justified? What is
17 the purpose? You know, going to sort of a FIPS
18 analysis, what is the purpose for it? Is this
19 collection focused on a valid purpose that we
20 feel should be pursued and is it important to be
21 pursued, whatever the phrasing should be?

22 And is your activity tailored to that

1 purpose? Are you doing something? Are there
2 less intrusive ways of doing it? Is this the
3 appropriate way to go about doing it in terms of
4 obtaining this information?

5 And then what are the risks to that?
6 Sort of now going to the other side of the scale.
7 And how do you guard against those risks? How do
8 you mitigate those risks?

9 And this is the way that I've always
10 thought of it. You know, it actually fits into
11 some FIPS kind of models. It also fits into some
12 privacy and assessment kind of models.

13 But if you look at that overall picture
14 it then helps inform you, either the art or
15 science side, I don't know, Becky can tell us
16 which one that is.

17 It helps inform the decision about
18 whether this is the right thing to do. And I
19 think you have to look at that to tell.

20 So if you're just going to do one
21 program, well, it's lawful and we think we need
22 it. But now you can't figure out, there are

1 major risks, but you can't figure out how to
2 adequately mitigate those risks, then that will
3 tell you one thing about the overall risk of
4 doing that activity.

5 MS. COLLINS COOK: Alex, if we could.

6 MR. JOEL: Oh, I'm sorry.

7 MS. COLLINS COOK: That's all right.

8 And Becky, did you have something specific you
9 wanted to say in response to this question?

10 MS. RICHARDS: Yes, the only thing I
11 would say is we've been asking some different
12 questions to try and tease out some of this
13 conversation as we go through different programs.

14 And the questions we've been circling
15 around, which are a little bit different than,
16 you know, is this lawful. It's more, what is the
17 type of the data? How intrusive is the data?
18 How broad is the collection? In other words, am
19 I obtaining a lot of people who are sort of an
20 incidental collection, are not part of the target
21 or not? And then what are the stated uses or
22 future uses?

1 And we've sort of been using those three
2 questions to get at, I think, the overall risk,
3 which this sort of bubbling it really up is we
4 want to stop the government from doing bad things
5 to good people.

6 And so you know, sort of looking through
7 those different lenses it helps us do that
8 analysis.

9 MS. COLLINS COOK: So thank you. David
10 -- I'm sorry.

11 MS. BROWN LEE: I was just going to say,
12 just because you wanted-- all right.

13 It's an iterative. I was just going to
14 just sort of follow-up on the comments in that I
15 think that forcing mechanism of trying to do, of
16 having ongoing vetting and ongoing evaluation by
17 the right people is where to go, because in
18 looking for the meaningful relationships and
19 developing those, as opposed to, you know,
20 retaining the isolated pieces.

21 So I would just say that trying to force
22 that mechanism of ongoing vetting is really

1 important.

2 MR. MEDINE: One of the reasons for
3 having the forum today is to get a better
4 understanding of what privacy interests are being
5 protected by your offices and our agency.

6 And Alex and Erika have both been in
7 either the private sector, in the case of
8 Marriott or at least at FTC had a private sector
9 focus. How would you compare the privacy
10 interests you were trying to protect in your
11 prior positions with the interests that you are
12 trying to protect now? What are the similarities
13 and what are the differences?

14 MR. JOEL: So I actually think there are
15 a lot of similarities, but there are of course
16 some important differences as well.

17 So on the similarity side, and I think
18 privacy officers and people in all kinds of
19 organizations, be they private sector or other
20 government agencies, share a similar challenge or
21 problem set, which is when your organization
22 wants to do something either for a business

1 purpose or for an authorized statutory purpose,
2 and in order to do that you need information.

3 And for businesses this is typically
4 information about customers or potential
5 customers. And then you want to do something
6 with that information to carry out your lawful
7 activity. So it's a given that your organization
8 will be obtaining and using personal information
9 in many cases.

10 And so then the privacy officers'
11 challenge is then making sure that that activity
12 is conducted in a way that maintains your key
13 trust relationships.

14 There are different ways of framing it,
15 but I think that's generally speaking what
16 happens.

17 And so for a business perspective, what
18 you want to make sure you're doing is delivering
19 value to your customer and that you're not using
20 that information for inappropriate means or ways
21 that are going to essentially get your customer
22 upset and have your customer take his business

1 elsewhere.

2 And so a lot of those things are
3 similar. I think that the key distinction for a
4 business is of course that it has the ability to
5 disclose a lot about what it's doing in terms of
6 obtaining that information. And the value that
7 it's providing is also something that gets
8 immediately, it should be immediately apparent to
9 the customer.

10 To the extent that the value is further
11 down the chain and the customer doesn't see it
12 that much, but is aware that the information is
13 being collected, that impacts the trust that the
14 customer has with the business.

15 I think from an intelligence community
16 perspective, it's hard for us to demonstrate the
17 value. What are we doing with the information?
18 And so as a result when people are worried about
19 information being obtained by the intelligence
20 community, the value to them seems inchoate, yet
21 the risks seem very real. Like, well, my freedom
22 could be impacted if the government misuses this

1 information.

2 We can reassure people we have methods
3 in place to make sure that the information will
4 not be misused, but I think, and we need to do a
5 better job of that, but I think the other side of
6 that equation is we have to show, better show
7 what we're doing with the information.

8 And of course for intelligence agencies
9 some of the most tightly held secrets are the
10 successful use of intelligence, because we don't
11 want our adversaries to know that that method was
12 successful.

13 MS. BROWN LEE: Okay. So just to
14 quickly answer your question, so I was also in
15 the private sector at a law firm and practicing
16 privacy.

17 Here's where they're similar, whether
18 it's clients, or even from a government
19 prospective, people tend to be reactive to
20 privacy.

21 And one of the things that I find the
22 biggest challenge is to be proactive. And it

1 means sometimes taking unpopular positions,
2 whether it's with clients or internally within my
3 organization. But sort of having principled
4 reasons for doing that, and if not forcing
5 putting, you know, very strong arguments to do
6 what you think is the right thing, I think is
7 where it's simialar and where it's hard but
8 interesting.

9 MR. MEDINE: Becky, you talked about
10 catagorizing certain types of information as
11 being sensitive.

12 In our morning discussion there was a
13 lot of talk about the mosiac theory where there
14 may be individual bits of information that are
15 innocous on their face but in combination they
16 present a perhaps sensitive profile of someone's
17 activities, thoughts and so forth.

18 Do you lose something if you focus on
19 what seems to be sensitive information and not
20 take into account the potential combinations of
21 information?

22 MS. RICHARDS: So actually the goal is

1 to take in to all those combinations. So the
2 idea and where we've been looking at is that it's
3 very difficult. You know, we want to push folks
4 and I will say that this is an uncomfortable
5 place to be as a privacy person. This is sort of
6 where I'm like, well, it'll depend.

7 But if we look at where big data is
8 today, there is a lot of data and it's very
9 voluminous and it's a lot of discrepancies. And
10 if we can start to define, which is sort of what
11 I felt like we heard in the second panel, even
12 if -- and this is where sort of I think we're
13 going to try and push NSA, is if we can start to
14 define and put some mathematics behind it.

15 So that, for example, if you have
16 vaguely anonymous or slightly de-anonymized data
17 over here and over here and the computers start
18 to put them together, we would want the system to
19 then pop something to say, hey, look at this
20 before you decide to go forward.

21 So the idea is technology is supporting
22 the privacy analysis by looking at whether or not

1 the math underneath it can work.

2 And so you're going to have to make some
3 really hard choices. Do I think health data is
4 more risky to privacy than my address? And
5 everybody gives the example of, well, then you
6 have the violence against women or, you know,
7 something along those lines.

8 But at some level if we deal with only
9 those edge cases, we're not going to move
10 forward. And I think the value, we will be
11 losing some of the value, both from a privacy
12 perspective, as well as from a technical
13 perspective.

14 Because we're sort of in this art form
15 of looking at each individual case, which I
16 recognize at NSA, I'm not going to be able to
17 look at every single, little thing. We want a
18 system to be able to identify the things that
19 need additional analysis, that need that
20 additional judgment.

21 But what I don't want to have happen is
22 have us backed into a place where the system is

1 doing things that we would find unacceptable
2 because we didn't sort of build something in to
3 help with that.

4 MS. COLLINS COOK: Thank you. Rachel.

5 MS. BRAND: Thank you all for being
6 here. For those of you who have been here all
7 day you'll know that this is a little bit of a
8 hobby horse of mine. But I want to ask about the
9 FIPS and why you are purporting to apply them,
10 although you can't really apply them.

11 So I gather, and Ms. Richards, this is
12 directed to you, at least initially. And I
13 commend you for publishing the paper on targeted
14 collection under 12333. And you said that you
15 were applying the FIPS, and I gather you were
16 talking about the 2008 DHS iteration of the FIPS.

17 But then you said that, for example, the
18 individual participation FIPPs can't really apply
19 to your activities, and the transparency one can
20 apply in a very limited way.

21 I guess I'm wondering whether it doesn't
22 make sense to come up with a new set of

1 principles that applies to surveillance activities
2 of the government? Because if you look at the
3 DHS FIPS, the transparency one as articulated in
4 this document really can't apply to you because
5 it's talking about providing notice to the
6 individual regarding collection. That's
7 obviously not going to take place. Individual
8 participation really can't apply at all.

9 MS. RICHARDS: Correct.

10 MS. BRAND: Some of these other ones are
11 very, very important. Purpose specification is
12 very important. Minimization, data security,
13 some of these are important.

14 But yet, this doesn't at all address
15 things like thresholds, evidentiary thresholds for
16 collection, which are required obviously by law.
17 But if you're talking about principles that are
18 supposed to sit on top of the fundamental legal
19 requirements, you should talk about thresholds.
20 And there are some other principles that don't
21 come into play here.

22 So I'd be interested in knowing why you

1 decided to apply the FIPS and if you've given
2 some thought to coming up with some new
3 principles.

4 I don't mean to criticize this for DHS's
5 purposes because DHS has a lot of functions that
6 involve voluntary interaction by an individual
7 with the government where this makes a lot of
8 sense. So but you're in a different position
9 than that, obviously.

10 MS. RICHARDS: So I guess what I would
11 say is it's a beginning place, and I've sort of
12 stated that a couple of different times because I
13 wanted to start with something.

14 And so from my perspective, I guess I
15 want to take the parts of the FIPS that work
16 well, which would be basically the bottom six of
17 the DHS ones and then look at how we can work
18 those through.

19 So what I would say is sometimes there's
20 analysis that needs to be done at an enterprise
21 level. So it's useful for me walking into the
22 agency, which may be readily apparent to

1 everybody, but it was just useful to go through
2 the process and say, hey, here is sort of one
3 framework that we think about for privacy, and as
4 an enterprise we don't do the first two.

5 One of the questions that led me to ask
6 in some of the conversations I've had with
7 academics and advocates is to say, okay, we don't
8 do transparency in the traditional sense and we
9 don't do individual participation. Is there some
10 proxy? Is there some additional thing that we
11 should be doing, given that?

12 And I think that gets to your question
13 of, well, are there other things that should be
14 underpinning these? And that's where we're
15 starting to work through those questions.

16 So I think it was very beneficial to
17 start with that as the beginning one and then use
18 the remaining six principles as the basis for
19 some of these questions.

20 Part of the problem though I will tell
21 you with the FIPS is they don't give you a
22 judgment. They don't tell you, well, this is

1 good enough or that's bad enough, which sort of
2 gets to your evidentiary purpose. And that's the
3 place where we are trying to then look at the
4 data. What are the risks to the data?

5 We spend a lot of time now talking
6 about, well, what is the exact risk to this
7 program to privacy and civil liberties? And so
8 we're still working through those and having a
9 lot of really fun and intellectually stimulating
10 conversations about what are the right questions
11 and how do we do that for an intelligence agency
12 at NSA.

13 But I would just say that it, for us,
14 was a beginning place. I don't think that's it's
15 necessarily the ending point, but it was
16 someplace to start with. And I don't want to
17 sort of throw everything out and start with, I
18 don't know. You know, you have to start
19 somewhere.

20 MS. BRAND: Okay. Do the other
21 panelists want to say anything about that? Alex?

22 MR. JOEL: I would just say that even

1 though the first two do not directly apply,
2 certainly not as written by DHS, they provide
3 useful measures for us to determine to what
4 extent does this raise privacy issues and in what
5 areas.

6 So that is, I think it's very helpful to
7 use as a guide in the way that Becky has been
8 using it at NSA.

9 I like the idea of developing a
10 statement of principles that would apply to the
11 intelligence community. So I'll take that path.

12 MS. BRAND: I think I probably don't
13 have time for another question, but I would
14 suggest if you're going to engage in that
15 exercise that you look at the threshold question
16 and that you also look at oversight because
17 these, you know, they talk about accountability
18 and auditing, but creating a paper trail is not
19 the same thing as effective oversight. And
20 obviously, as I said in the previous panel,
21 oversight is extremely important in this context.
22 So just food for thought.

1 MS. RICHARDS: And I think it's just
2 important that you don't have a check box. I
3 mean part of the problem I think with the FIPS
4 also is it leaves itself to a little bit of a
5 check box process.

6 Do I have a privacy statement? Yep, I
7 got a privacy statement. Okay, am I doing
8 everything in there? Yep, okay, I can do that.

9 As opposed to these sort of questions
10 of, should I be doing that? And that's I think
11 where having an individual at the agency whose
12 focal point is this, really benefits the agency
13 in terms of that conversation because it can very
14 quickly devolve to, I checked it off, I'm good.
15 You have no privacy, but I'm good.

16 MS. BROWN LEE: And I would just say
17 that the oversight perspective has to also be
18 iterative and changing because I think as
19 technology allows us to, you know, collect more
20 data and in different ways and different data
21 points that the oversight of it has less meaning
22 if you're not also adapting on that side as fast

1 as we are adapting to the technological changes.

2 MS. COLLINS COOK: Thank you.

3 Jim, do you have some questions?

4 MR. DEMPSEY: Thank you. Thank you to
5 the members of the panel.

6 I have some questions that I want to
7 ask, but I saw there are a lot of audience
8 questions. Was there one or two that stood out
9 particularly? Technically, we only have five
10 more minutes to go on this panel, so I'm happy,
11 Beth, to have you ask one or two of the audience
12 questions.

13 MS. COLLINS COOK: Sure, and I think you
14 should know you have won the jackpot thus far on
15 audience questions.

16 Alex, this one goes to you and it draws
17 on a remark from a previous panel.

18 Why can't the IC inform the American
19 people about how many phone records were
20 collected pursuant to Section 215 and make
21 similar public disclosures regarding the breadth
22 of U.S. person collection under 702 and EO 12333?

1 So the executive order, understanding
2 that you're not targeting necessarily U.S.
3 persons, but the U.S. person incidental
4 collection.

5 MR. JOEL: So that's a good question. I
6 don't want to duck it. I'll just say that I am
7 going to in certain ways.

8 No, but I don't want to, I guess I'm not
9 going to get into the specifics of like 215 or
10 702, etcetera.

11 What I'll say is that there are two
12 challenges. I understand the interest and I
13 understand the importance. One is technical
14 capability. Can you, in fact, count it? And for
15 some things, some activities, you should be able
16 to count. But for some other ones, they
17 inherently involve challenges.

18 I know that one of the PCLOB
19 recommendations in the 702 report was, in fact,
20 to count some of the 702 collection that involves
21 U.S. persons. So there are some inherent
22 challenges in doing that.

1 From a national security perspective
2 what I'll say is what I have heard internally as
3 we have pursued these kinds of questions is that
4 providing that kind of information can, in fact,
5 put at risk some kinds of collection, especially
6 if you track it over time.

7 An adversary, a sophisticated adversary can
8 put the information together in terms of the
9 volume of collection in one particular area and
10 then draw some conclusions about what
11 specifically is being obtained, what are the
12 specific channels that are being watched, and
13 therefore change behavior.

14 So our job from a transparency
15 perspective is to continue to discuss that
16 internally and see, well, you know, are there
17 ways of mitigating that? What can we, in fact,
18 disclose in this area? Because it's of strong
19 interest.

20 MS. COLLINS COOK: So, Erika, I'll
21 direct this next one to you because you mentioned
22 that part of the civil liberties protections and

1 privacy protections are consequences for
2 wrongdoing.

3 So the question from the audience is, in
4 the case of a privacy violation sufficient
5 remedial measures are critical. What, if
6 anything, do you think needs to be done, either
7 statutorily or administratively to strengthen
8 existing remedial schemes?

9 MS. BROWN LEE: So, yeah, I do think
10 that the remedies for Privacy Act violations or
11 for privacy violations are, you know, as I said
12 in my remarks everything could be examined and
13 looked at for approval.

14 I was focusing my remarks on FBI. So of
15 course they have their own investigative unit
16 that reviews. So if there's any particular
17 activity that an agent engages in, for example,
18 that is, you know, collecting information in
19 violation or specifically because of First
20 Amendment purposes, that's subject to review and
21 disciplinary action.

22 With regard to individuals, I agree. I

1 mean we talked about how the FIPS doesn't really
2 have as meaningful of really a guide for law
3 enforcement either.

4 I think, you know, it's not something
5 that I can do, but certainly it's been attempted
6 before to remedy the Privacy Act or to amend it.

7 We are, the administration is committed
8 to looking to expand the protections of judicial
9 redress for non-U.S. persons, and DHS has a
10 policy of doing so administratively.

11 But I think statutorily it's a hurdle.
12 I think it's something that I would be willing to
13 have a conversation to further that.

14 MS. COLLINS COOK: So just to keep this
15 even across the board, Becky, this one is for
16 you.

17 And I think implicit in this question is
18 a very interesting premise. Do you anticipate
19 that wide swaths of data will no longer be
20 collected now that you are asking questions about
21 whether they are really needed and the civil
22 liberties downsides?

1 So I would say the premise is that it's
2 your job to shut it down, which I think it's a
3 widely shared premise.

4 And I think the basic question is, do
5 you think you're going to be effective?

6 MS. RICHARDS: So I think that also
7 starts with the premise that the collection we're
8 doing currently -- that's starting with the
9 premise that we're collecting too much
10 information today.

11 And I think what I would say is that
12 what we're working on is sort of a premise, so if
13 NSA is filled with a lot of people who do math
14 for a living, we're in the process of third grade
15 math, which is folks need to show their work. So
16 they need to show why they're doing what they're
17 doing so that then we can have those
18 conversations.

19 I don't want to presuppose we're going
20 to do more, or less, or either way of those. But
21 I do think that what we haven't done well is
22 explain what we're doing.

1 And if you sort of consider that NSA has
2 a long history of saying absolutely nothing to
3 anyone, and in the last year and a half we've had
4 to create a voice for ourselves to explain what
5 it is we do, and recognize that most people,
6 there are a lot of Ph.D.s in math at NSA who
7 don't necessarily take well to speaking in
8 public. It's a work in progress.

9 And so my hope here is not to be judged
10 by how much we turn on or turn off, but by
11 demonstrating what the value is to the country in
12 terms of what we're doing and demonstrating that
13 we're protecting civil liberties and privacy.

14 MS. COLLINS COOK: So thank you all for
15 your remarks and your active back and forth on
16 the questions.

17 MR. MEDINE: And we'll be taking a 10 or
18 15 minute break, and at 2:45 we'll resume with
19 the private sector's views on these issues.
20 Thanks.

21 (Off the record.)

22 MR. MEDINE: Good afternoon. Thanks for

1 everyone's endurance who's been here all or most
2 of the day.

3 This is our final panel today, but an
4 important panel on what the private sector has
5 learned about privacy and how that might relate
6 to the considerations we go into with regard to
7 national security issues, and Rachel Brand will
8 moderating.

9 MS. BRAND: All right, thank you, David,
10 and thank you to all our panelists for being
11 here.

12 The way we've structured the day is that
13 the first panel this morning had to do with the
14 theoretical underpinnings of privacy and
15 exploring what interests underlie privacy. The
16 second panel had to do with technology. The
17 third panel was a government panel.

18 And this last panel is supposed to be
19 focused on solutions, and particularly those
20 solutions that folks in the private sector might
21 be able to suggest.

22 So what we'll do here logistically is

1 each panelist will start with up to seven minutes
2 of remarks. And for the panelists' benefit, Sam
3 Kaplan is sitting in the front row here with
4 yellow and red cards. So when he holds up the
5 yellow card, you'll know you have two minutes
6 left, so please pay attention, and the red card
7 means that your time is up.

8 At that point, as the moderator I will
9 ask about 20 minutes of questions, and then each
10 of my fellow Board members will have five minutes
11 of questions, and then we'll open it up to
12 questions from the audience.

13 And as with the previous panels, when I
14 start to ask questions some of our staff members
15 will stand up in the back, and Lynn Parker Dupree
16 in particular, and Prem, will stand up and hold
17 up cards and you can go get yourself a card,
18 write down your question and then the staff will
19 pass it up here.

20 So we'll just go down the row and we
21 will start with Professor Cate. I am not going
22 to go into length on their biographies because I

1 think they're all available to you.

2 But Professor Cate is a Professor at the
3 University of Indiana School of Law, and he's
4 been on a number of previous boards and
5 commissions on privacy.

6 And so, Professor Cate, let's start with
7 you.

8 MR. CATE: Thank you very much. This is
9 the time I think to say that I'm colorblind so
10 I'll have no idea what cards you're holding up.
11 So perhaps you'll wave them in a definitive way
12 and I will pay attention.

13 So first of all, I was sorry not to be
14 here for this morning, but the last panel was
15 absolutely superb, and it's a privilege, both to
16 be here, and I really want to applaud the Board
17 for taking up this I think really difficult, but
18 fundamental, issue about what is privacy and how
19 in practice might we go about protecting it, both
20 in the private and the public sectors.

21 I want to really just offer some
22 observations, as opposed to any specific, if you

1 will, recommendations or conclusions.

2 One, and this was touched on in the last
3 panel, I think the FIPPs are frankly not
4 tremendously useful.

5 I'm not suggesting abandoning them,
6 which is a big change for me. Ten years ago I
7 wrote a book chapter called, the death of the
8 FIPPs. But fortunately, I've gained a little bit
9 of knowledge here.

10 But I think we use them almost
11 talismanically, like we can roll out these eight
12 principles, or depending on what list of FIPPs
13 you use, and that that will get us somewhere.
14 And that far too frequently, both in the private,
15 and certainly in the public sector, they really
16 don't get us anywhere.

17 What we end up is we end up, just like
18 talked about in the last panel, looking for
19 substitutes for the FIPPs. Well, we can't have
20 consent, what could we have, rather than asking
21 what was the purpose to be served in the first
22 place?

1 And maybe consent's no longer relevant
2 as a tool to achieve that purpose, rather what
3 are we trying to actually do here? Really the
4 question you've been asking all day, what are we
5 trying to protect? What do we think protecting
6 privacy really means?

7 I say this, by the way, about the FIPPs
8 in part because I'm not sure that they've ever
9 worked terribly well, and certainly in the U.S.
10 environment where they've largely come to mean
11 notice and choice.

12 I'm not sure that they work well in a
13 world of massive data, whether we call it big
14 data, or whether we call it just high volume
15 data, but the notion of a sort of FIPPs-like
16 approach, particularly with a focus on the
17 individual when the broader issues may be,
18 frankly, societal. They may be the impact on the
19 economy. They may be the impact on civil
20 liberties, not of one person but of everybody.
21 And I don't know that the FIPPs help focus us in
22 a useful way on that.

1 And then frankly, I think the FIPPs have
2 led to some sort of silly results. And you know,
3 I would just mention I've always been surprised,
4 for example, the Department of Homeland Security
5 privacy impact assessment on border searches of
6 electronic devices, which focused a lot on notice
7 as a privacy protection.

8 Well, at the point that your device has
9 been seized from you and its contents copied it's
10 difficult to think that notice is meaningful
11 protection. It may be necessary, but whether
12 it's protection or not, I think it's not.

13 Second point, one of the things we are
14 seeing emerging in the debate in the private
15 sector, and we see this especially in Europe in
16 the context of discussing the general data
17 protection regulation there, is greater focus on
18 risk management, or risk assessment and risk
19 management.

20 And I don't mean to use this just
21 because it's sort of the jargon of the day but
22 rather because risk management is an incredibly

1 valuable tool that in privacy we are unbelievably
2 far behind on. You know, security we have much
3 clearer ideas what risk management mean. Privacy
4 we really lack that understanding.

5 And part of the reason is because we
6 don't know what risks we're guarding against.
7 We're very unclear what are the harms, what are
8 the impacts, what are the negative effects that
9 we think we are balancing, if you will, with the
10 positive outcomes of the use of data or what have
11 you.

12 And so one reason I think the risk
13 management approach offers a lot of value in both
14 public and private sector is that it makes us
15 stop and say, what is it we're trying to
16 accomplish? What are the positive benefits and
17 what are the potential negative impacts, not
18 measured in terms of FIPPs, but measured in terms
19 of actual impact on individuals, or on society,
20 or on the economy, as we think about it.

21 When using risk management, or if you
22 hate risk management, in either case, third

1 point, I think there's a lot of reason to focus
2 more attention on use of data.

3 And this has been a real weakness of the
4 U.S. legal system. Those of you who have
5 suffered through law school know that the Fourth
6 Amendment has almost nothing to say about use of
7 data whatsoever.

8 In fact, you can have illegally seized
9 data that the court acknowledges is illegally
10 seized and they will still allow it to be used
11 someplace else because there would be no
12 disincentive for the collection, it's only the
13 collection in the Fourth Amendment that Supreme
14 Court jurisprudence has been focused on.

15 And for this reason I think we really
16 would be better to be thinking more about
17 reasonable and effective limits on use. And in
18 fact, I think that's what the public most
19 commonly cares about.

20 And one of the practical reasons for
21 that is because there's almost always a
22 legitimate reason to collect the data. There's

1 always some reason, there's some employment
2 reason, there's some security reason, there's
3 some private sector reason. You know, Verizon
4 had a reason to collect this data. And then the
5 question was, who could access it and how could
6 it be used?

7 But our legal system has focused
8 enormous attention on collection, and then once
9 the data are in the government's storehouse then
10 we feel that the data are more commonly out of
11 control. And I think that is a critical area to
12 focus on as well.

13 Fourth, as I've mentioned, I think the
14 Fourth Amendment, while it's a critical legal
15 limit and I certainly concur -- that's yellow,
16 right? Yes? Thank you. And for the rest of
17 you, you'll know I just got a yellow card.

18 I think the Fourth Amendment of course
19 is a critical legal limit and we must of course
20 observe it. It's not a very useful guide for
21 telling you what to do in the future for a
22 positive analysis of privacy issues.

1 And I think we should again be careful
2 about that. Too often in our rhetoric we say
3 well, it's permitted under the Fourth Amendment
4 as if that tells us anything, other than it is
5 not illegal under the Fourth Amendment. But it
6 doesn't tell us anything about either the ethics,
7 or the desirability or what have you of doing it.

8 And then fifth, I would just say in
9 almost all of these areas, and I understand in
10 national security this seems particularly maybe
11 odd, I think redress is something we need to
12 continue to focus on.

13 We see many uses of data in the
14 government setting and in private sector which
15 are done without regard to redress, with just
16 sort of, well, if it affects a person
17 inaccurately every now and then, what does it
18 really matter? We'll deny boarding to people on
19 airplanes, or we'll provide extra security for
20 the wrong people.

21 This is not an efficient use of
22 government resources and it's not a good way to

1 think about privacy.

2 And I think we should be very clear in
3 those rare exceptions where we say there might be
4 no redress available here for the individual, in
5 which case we now have to provide it through
6 other means, inspector generals, or the PCLOB, or
7 other ways of approaching it.

8 But at all times we should be thinking
9 about redress, not just because of the rights of
10 the individual, but because of the interests in
11 ensuring that the system works as advertised and
12 as it should. Thank you very much.

13 MS. BRAND: Thank you very much. Our
14 next panelist is Harley Geiger. Harley Geiger is
15 Advocacy Director and Senior Counsel at the
16 Center for Democracy and Technology, and he
17 focuses on issues related to civil liberties and
18 government surveillance, computer crime and
19 cybersecurity. Thank you for being here.

20 MR. GEIGER: Members of the Privacy and
21 Civil Liberties Oversight Board, thank very much
22 for inviting me to speak at your meeting today,

1 and thank you also for your excellent work on
2 ensuring protection for privacy and civil
3 liberties in national security and terrorism
4 programs. And congratulations on having one of
5 the best acronyms in town.

6 When it comes to evaluating privacy
7 protection, the Center for Democracy and
8 Technology believes that the Fair Information
9 Practice Principles are a very important
10 framework for both government and the private
11 sector.

12 Now you can add other privacy frameworks
13 on top of that. We certainly do not disagree
14 with Professor Cate that societal impact is a
15 very useful consideration, and we certainly agree
16 that protections focused on the purpose of data
17 collection are also useful.

18 But we view the FIPPs as an
19 indispensable framework for evaluating privacy
20 protection with data collection practices.

21 Now the individual principles of the
22 FIPPs, as you know, are overlapping and mutually

1 dependent on one another. It is a framework.
2 It's not a smorgasbord that you can just choose
3 and pick, at least not unless you don't want
4 robust privacy protection.

5 And there is obviously some discussion
6 in the private sector about doing away with data
7 collection limitations or the data minimization
8 principle of the FIPPs, seeing as how we are now
9 all in an age of big data.

10 But in the time that you've given me, I
11 want to address this head-on in the context of
12 government surveillance.

13 First, CDT believes that there still
14 should be collection limitations on private
15 sector data collection, and that the data
16 minimization principle of the FIPPs should apply
17 to the private sector.

18 Second, the government should not take
19 its cues entirely from the private sector when it
20 comes to national security surveillance. Data
21 collection from the private sector is
22 fundamentally different from national security

1 surveillance.

2 Therefore, even if the private sector
3 were to collect data in a relatively unrestrained
4 manner in some alternate universe, then
5 intelligence agencies should still nonetheless
6 not follow suit.

7 The missions of the private sector and
8 the national security functions of governments
9 are totally different. That should go without
10 saying. The private sector typically does not
11 use the data that it collects to detain or take
12 kinetic action against the individuals as part of
13 its mission.

14 Several major private sector companies
15 have repeatedly responded to public outcry over
16 privacy with enhanced transparency and privacy
17 controls.

18 The national security arms of government
19 are not as transparent or responsive and are not
20 likely to be.

21 Many major companies, in addition, allow
22 or are required by law to allow consumers to

1 limit the collection of information about them.
2 More and more services are differentiating
3 themselves on the basis of strong privacy
4 protection.

5 And of course, individuals can choose
6 not to participate in a commercial service as a
7 means of limiting direct data collection about
8 them. But data collection for national security
9 purposes does not permit any meaningful choice.

10 So this is not to laud private sector
11 data collection practices because CDT does view
12 them as generally insufficiently protective of
13 privacy.

14 But because of the differences that I
15 just briefly listed, and other reasons, even if
16 the private sector fails to robustly apply the
17 FIPPs government agencies should not follow suit.

18 If anything, because of these
19 differences government should strive for a more
20 strict and consistent application of the FIPPs
21 than that of private sector data collection.

22 And so I have a small set of broad

1 recommendations to make.

2 First, the government should place
3 greater emphasis on applying the data
4 minimization principle of the FIPPs. Back-end
5 minimization procedures alone are not sufficient.
6 Front-end minimization is also critical.

7 Trust is breached at the point of
8 collection. Once the government collects
9 information, non-statutory internal restraints on
10 access and use can fall away like sand castles on
11 a beach. We saw this happen with the 702
12 backdoor search loophole.

13 So surveillance should be restricted at
14 the front-end by narrowing limiting the
15 collection of data to what is directly needed to
16 accomplish a specific purpose.

17 The data should then be retained only as
18 long as is necessary to fulfill that purpose, and
19 the data should be destroyed unless a
20 determination is made that the data are needed to
21 accomplish the specific purpose.

22 The specified purpose of data collection

1 itself should be subject to meaningful
2 restriction.

3 For example, limiting the scope of what
4 is relevant under Section 215, or the definition
5 of foreign intelligence in Executive Order 12333.

6 So the goal should be overall to move
7 from mass data collection to targeted data
8 collection of both U.S. and non-U.S. persons.

9 Second, the government should provide
10 much greater transparency regarding the
11 interpretation of surveillance laws. Section 215
12 of the PATRIOT Act exemplifies this.

13 Nobody was surprised that the NSA is
14 collecting phone records. What was surprising
15 was that the NSA has secretly interpreted Section
16 215 to allow for the collection of all phone
17 records in the entire country.

18 This is bad data minimization. And yet,
19 a fair reading of the statute does not seem to
20 grant them with this authority.

21 So declassification of FISA court
22 orders, or, when necessary, summaries of opinions

1 would substantially boost transparency. We
2 should not be a nation of secret laws.

3 Third, the government should provide
4 greater transparency around the extent and scope
5 of requests for data under national security
6 authorities. This includes government reporting
7 about its national security surveillance
8 activities, such as how many requests were made,
9 under which surveillance authorities, and for
10 what type of data, as well as how many U.S. and
11 non-U.S. persons were affected.

12 The government should authorize the
13 private sector to make similar reports.

14 Information is power and privacy is
15 control of information. An entity possessing
16 information about an individual has power over
17 that individual.

18 Large scale government collection of
19 information about individuals threatens the
20 relationship between citizens and the state
21 because it upsets the balance of power that
22 supposedly exists in democratic society.

1 Therefore, CDT urges PCLOB to recommend
2 that the government recommit to a robust
3 application of the Fair Information Practice
4 Principles, as well as other considerations,
5 regardless of what the private sector does, with
6 much more targeted data collection and greater
7 transparency. Thank you.

8 MS. BRAND: Thank you. Our next
9 panelist is John Grant. Mr. Grant is a Civil
10 Liberties Engineer at Palantir Technologies, and
11 he previously served on the staff of the Senate
12 Homeland Security Committee where, among other
13 things, he oversaw the Department of Homeland
14 Security. Thanks for being here.

15 MR. GRANT: Thank you very much, and
16 thank you for the invitation to speak today.

17 As I never tire of telling people, I was
18 a congressional staffer who worked on the
19 legislation creating PCLOB 2.0, so I take a pride
20 of parentage in the Board and I'm sure it's every
21 parent's dream to one day testify in front of
22 their children.

1 I know that the Board and a lot of
2 people are familiar with Palantir so I'll spare
3 everybody the extended commercial. Just suffice
4 it to say, Palantir builds a data management and
5 data analytics platform that works with data.

6 We started in the law enforcement,
7 intelligence space and have expanded to
8 deployments around the world and in a variety of
9 contexts in the financial sector, medicine and
10 elsewhere.

11 A core tenet of Palantir is that our
12 technology isn't successful if in the course of
13 achieving an organization's analytic mission
14 we're not also able to be deployed in a way that
15 protects privacy.

16 And that's something that the founders
17 of the company instilled from day one, and that
18 is why my job exists, a civil liberties engineer.

19 Well, one of the things I learned when I
20 went to Palantir, and this is different from the
21 Hill certainly, is when you walk into a room and
22 you say to engineers, I'm worried about this

1 thing you're building, it creates a privacy
2 problem. The response is, oh, okay, how do I fix
3 it? Which is not often what you get sometimes
4 when you raise these things in other places.

5 So it's our job as a civil liberties
6 engineering team to come up with suggestions for
7 how to fix it.

8 I am a lawyer, as you may have guessed,
9 so I do not necessarily possess a lot of
10 technical skill. So the main role for us is to
11 translate between the lawyers and the engineers
12 and back.

13 So what I wanted to focus on today a
14 little bit is some of the technology at a high
15 level, and then I had some actually suggestions
16 for moving forward that I think are actually
17 fairly low hanging fruit.

18 So just briefly to provide a little
19 context, as I said, Palantir is data management
20 and data analytics, so we're not dealing with the
21 collection of data. So this gets more to
22 Professor Cate's point about the use of data.

1 And we have two sort of high level
2 categories of technology that deal with managing
3 or protecting privacy with the use of data, and
4 that's access controls and oversight mechanisms.

5 But I want to start by pointing out, and
6 I think this is something to keep in mind, that
7 just as technology has expanded the power of
8 surveillance today and the amount of data that
9 can be collected, it's also significantly
10 expanded the level of privacy protection that is
11 available at the agencies.

12 If you imagine 50 years ago if there was
13 an FBI file, this was probably pieces of paper in
14 a Redweld sitting on a desk somewhere, or maybe
15 locked in a desk drawer, hopefully locked, or
16 maybe in a dusty basement archive or something
17 like that.

18 And you know, there'd probably be very
19 limited tracking of where the file was, you know,
20 hopefully a log book with a name and who had the
21 record. But who knows?

22 And anyone who accessed the file would

1 be able to see whatever was in the Redweld.
2 You'd just be able to rifle through it and you
3 could see anything, even if it wasn't directly
4 relevant to what you needed.

5 Oversight into how the file would be
6 used would really be nonexistent. You wouldn't
7 see exactly who added information to the file,
8 who deleted information from the file. And
9 deletion would largely be hopefully a burn bag or
10 a shredder, probably just crumpling it up and
11 throwing it in the trash. A more precise
12 deletion would be a black magic-marker redacting
13 a few points of information.

14 Today. So today technology allows us to
15 do a lot more management of data and oversight,
16 and management at a granular level, and that's
17 what the access control point, which is you can
18 now build access controls to manage data very
19 precisely on a data point by data point basis.

20 And you can do it in a more nuanced way.
21 You don't have to make a choice between access or
22 not access. There are ways to sort of have

1 gradations of access. You can make the access
2 controls dynamic.

3 So there's a lot of options. And the
4 many options you have to configure those access
5 controls give you a near infinite variety of
6 options in how to manage the data, who can see
7 the data and what they can do with the data.

8 The other point is oversight mechanisms,
9 and this is really thinking a lot about audit
10 logging and also using technological, electronic
11 work flows to control exactly how data flows
12 around an organization, and who can see data, and
13 exactly what kinds of analysis they can do with
14 it, even automating, or at least hardwiring in an
15 approval chain for use of data and things like
16 that.

17 And these can be very detailed. So the
18 hardwired approval process and things like that,
19 that can be very complex. It can involve
20 multiple actors, it can involve multiple
21 stakeholders.

22 And then the auditing of how data is

1 used itself can be incredibly granular and
2 incredibly detailed.

3 And I'm skipping over a lot here, but I
4 want to get to some of the other points. But
5 just these two capabilities are a significant
6 improvement of what existed before and can get us
7 a long way.

8 And there are things that exist today.
9 Now, I'm obligated to say that of course Palantir
10 does these the best, but these are not
11 technologies that are exclusive to Palantir. And
12 they can be deployed and they can be used in a
13 lot of different contexts.

14 So what is the problem today, and why
15 aren't these capabilities being used more than
16 they could be and at the level that we think they
17 could be?

18 A couple of things. One issue is
19 technical awareness. Lawyers don't know
20 technology and engineers don't know law, and you
21 need people who know both of these things to be
22 able to make the decisions of how to use these

1 technologies, how to incorporate them effectively
2 into programs.

3 Lack of resources. You need people who
4 can actually manage the data. And we talked
5 about this in the earlier panel. Alex Joel has a
6 very small staff. Erika has a very small staff.
7 And they're managing huge amounts of data and
8 huge organizations. They need resources, they
9 need infrastructure to actually be able to do
10 this.

11 Privacy is hard. How exactly do you
12 look at an audit log? How do you use it
13 effectively? How exactly do you manage access
14 controls at this data point by data point level,
15 especially when you're dealing with mass amounts
16 of data?

17 And the last one is death by anecdote.
18 The argument, the debate, the cost benefit
19 analysis right now tends to be the national
20 security sector saying one time we caught this
21 bad guy using this information, and the civil
22 liberties community saying one time this unjust

1 thing happened to a person because of this
2 program.

3 There needs to actually be a much more
4 -- you can't just make this argument on anecdotal
5 grounds. You have to actually look at the data
6 and you can find out more specifically how these
7 programs are working, how effective they are.

8 So solutions. Obviously we suggest some
9 of the solutions in listing the problems.

10 Education. I think, and Palantir
11 actually sponsors fellowships with Paul Ohm's
12 Silicon Flatirons Project and other places to
13 make sure lawyers can learn technology and that
14 engineers can learn law.

15 Engineers don't have to be lawyers, but
16 it actually should be a requirement to have an
17 engineering ethics program and to have courses
18 that teach engineers privacy, because they're
19 going to build the technology that's going to hit
20 the streets and it's going to be months or years
21 before the law catches up.

22 So shouldn't engineers be able to catch,

1 you know, how what they're building is going to
2 affect privacy and be able to start thinking
3 about these things?

4 Infrastructure. If privacy is an
5 important value for us as a society then we need
6 to invest in infrastructure to support it.

7 Concrete guidance. We actually need to
8 go beyond just systems should have use
9 limitations. We need to actually tell people how
10 are you're going to do it? And I can get into
11 that more if people have questions.

12 But we need to be writing really
13 specific guidance, rather than just the, you need
14 to have notice and consent, you should be
15 thinking about use limitations, things like that.

16 And last, everything in the world can be
17 datafied these days, including how these systems
18 are working and how effective they are. And we
19 can do the analysis, and we can get beyond
20 anecdotes, and we can start analyzing data and
21 figuring out is this effective, is this not
22 effective, is this having negative effects, is

1 this creating bias analysis, etcetera.

2 Thanks very much.

3 MS. BRAND: Thank you. And our last
4 panelist is Chris Inglis. He is currently a
5 venture partner at Paladin Capital Group and is
6 the former Deputy Director of the NSA. Thanks
7 for being here.

8 MR. INGLIS: Great, thank you. And I'm
9 honor bound to say that I spend most of my time
10 teaching at the Naval Academy in the Computer
11 Science and the Cyber Operations Department.

12 First, I, like the other panelists, am
13 grateful that you've established this venue for
14 what I think is a really important dialogue, and
15 I'd like to make four quick comments and then
16 help us get to question and answers.

17 First and foremost, I absolutely agree
18 with the panel's premise, which I believe is, is
19 that the framers of the Constitution did not
20 intend for security and privacy to be in mortal
21 combat and we're therefore trying to figure out
22 how do we achieve both.

1 And it may well be that we cannot trade
2 one for the other. I think that's right, we
3 cannot, but we have to work harder to achieve
4 both. And I think technology and practice from
5 the private sector can be helpful there.

6 Two, I agree that government is
7 different, not simply in the powers, the tools
8 that it might bring to bear on its citizenry or
9 others, and therefore should be constrained, but
10 the government alone has the requirement to
11 essentially meet the standards of the First,
12 Fourth and Tenth Amendments within the
13 Constitution.

14 I will tell you that from my NSA
15 experience, the Tenth Amendment was the most
16 significant of those, which essentially says
17 unless you have the authority to do something,
18 you do not, you know.

19 And against what has been said, which is
20 that backdoor searches or 215 was NSA's
21 interpretation, both of those were specifically
22 permitted under court approved procedures and

1 specifically were interpretations of the law that
2 went through three branches of government.

3 I think that's right and proper. That
4 doesn't necessarily justify them. It may be bad
5 policy at the end of the day, but the rule of law
6 has to pertain, right, in terms of how the
7 government gets things done.

8 Point three, I would say that largely I
9 agree with what John had to say. Matter of fact,
10 I wholly agree with what John had to say, that
11 the aspects of law and technology are often at
12 odds with one another, not because they cannot be
13 reconciled, but because they're perceived as
14 independent biases on any particular solution.

15 And I would add a third, which is that
16 what typically plays out in any one of these
17 systems is that you're trying to effect a
18 technology, law, and the operational practice of
19 those who essentially make use of the technology.

20 And the unsurprising result is that
21 because they do not change at the same rate, they
22 essentially change at very different rates,

1 keeping them reconciled or synchronized from
2 moment to moment is really hard.

3 Therefore, mechanisms, FIPPs-like
4 mechanisms or other things are not likely to
5 satisfy the need.

6 What you need are threads or systemic
7 solutions that essentially you pull through and
8 you take both art and science process to
9 essentially try to figure out how to make some
10 solution here.

11 I'll wholly agree with John that
12 education's going to be absolutely essential. At
13 NSA ultimately when we found ourselves in the
14 midst of some compliance incidents for which no
15 one had intentionally made a mistake, we actually
16 had to sit down and figure out how do you achieve
17 a horizontal join between the technologists, the
18 legal practitioners and the operators, all of
19 whom were trying to achieve something that was
20 slightly different, but ultimately invested in
21 the same problem set.

22 The last point I would make is that I do

1 believe that there's a role for big data, what is
2 sometimes called mass collection. There's a role
3 for big data, but the principles that should
4 pertain to the government's collection of that
5 should be the same as surgical data, which is
6 necessity and proportionality.

7 The government should be able to justify
8 on what basis this is necessary, such that it
9 could then argue, not for an encroachment upon
10 civil liberties or privacy, but how do we then
11 work harder to achieve the sustainment of privacy
12 and civil liberty. And it should only achieve
13 that in proportion to that need.

14 Therefore, I think that all those four
15 comments aside, I would say that the private
16 sector probably has a lot of experience in this
17 regard that the government can take advantage of.

18 My own sense is that the government
19 collects far less information than is perceived
20 by the public, and certainly far less information
21 than the private sector does.

22 Again, I don't excuse the government for

1 that. The government should be held to account,
2 but the government can, in fact, bring
3 technologies in that might well scale quite well
4 for the government's purposes because we'd have
5 to scale them down, as opposed to scale them up.

6 I'm open to any questions you may have.

7 MS. BRAND: Thank you. Just a reminder
8 to the audience that there are PCLOB staffers in
9 the back with cards and if you'd like to direct a
10 written question to the panelists, hold up your
11 hand, find one of them and then write down your
12 question.

13 And for the benefit of the audience and
14 the cameras, for the panelists, when you're
15 answering a question if you wouldn't mind moving
16 the mic back and forth. I'm sorry, we don't have
17 as many mics as we probably should.

18 So I'd like to start by asking about
19 oversight, and I'd like, Mr. Grant, to direct
20 this question to you first.

21 Both in your oral statement and in the
22 written statement that you submitted to us, you

1 talked about a wide range of mechanisms, paper
2 trails, electronic work flows and things like
3 that, and frankly, on the written statement it
4 seemed like an overwhelming array of different
5 ways to engage in oversight.

6 I think for a couple of reasons you need
7 to choose your oversight mechanisms. One is that
8 any agency is going to have limited resources to
9 dedicate to oversight.

10 And secondly, as I mentioned in a
11 previous panel, there may come a point where
12 there are diminishing returns on oversight. You
13 need to leave these people doing the work at the
14 NSA or other agencies time to actually do their
15 job, not just comply with oversight mechanisms
16 all day long. So you have to find some balance.

17 So have you given some thought to what
18 constitutes an effective oversight mechanism?
19 How do you rank different mechanisms in terms of
20 their effectiveness?

21 MR. GRANT: Yes, so I think we should
22 actually think about oversight as a big data

1 problem and then apply the same thinking to it
2 that we would apply to trying to analyze signals
3 intelligence and trying to analyze huge amounts
4 of transactional data for marketing.

5 It's a similar issue. You have a huge
6 amount of data, as you say. There are massive
7 amounts of audit logs, for example, in an
8 organization like the NSA, and that's a lot of
9 information.

10 But you can use technology and analytic
11 tools to make sense of that information and
12 derive the insights that you're looking for.

13 So but part of the issue is, A, you need
14 to do it, you need someone. So we see this all
15 the time in Palantir and I know other
16 organizations see this as well, which is,
17 everybody checks the box on FISMA for audit logs.
18 We've got the audit logs and we will go through
19 an enormous number of hoops to make sure it's
20 logging exactly the information that it's
21 supposed to.

22 We get fewer requests to actually look

1 at the audit logs once the auditing mechanisms
2 are turned on.

3 And looking back to my congressional
4 experience, there aren't many laws that I can
5 recall that tell anyone they actually have to
6 look at the audit logs, they just have to.

7 It's the Seinfeld joke about renting a
8 car. Everybody can take the reservation but you
9 have to hold the reservation. You have to use
10 the information.

11 So I think, I mean to me that's how you
12 make oversight more effective, you use these
13 techniques.

14 And that's another thing. The oversight
15 people and the information security people and
16 things like that, they should be as good as your
17 analysts, and you need to have good people who
18 are also doing the analysis and conducting the
19 oversight.

20 So to get to your last question, which
21 is the most effective? I think it's using that
22 auditing data. I think it's using that big data

1 that you've got and having a team of people that
2 can proactively comb through it.

3 And not only are you going to look for
4 people doing something wrong, but you can also
5 ask questions such as, you know, does our data
6 retention policy make sense?

7 You could look at the data and say, you
8 know what, it turns out we keep data, this data
9 set for five years. Nobody ever uses the data
10 older than three years in that data set, so let's
11 change the data retention policy to fit with the
12 actual usage of the data.

13 MS. BRAND: Thank you. Mr. Inglis, I'd
14 especially like your thoughts from your time in
15 government, what did you view as an effective
16 oversight mechanism?

17 MR. INGLIS: So first and foremost, if
18 there is an authority that is granted or a burden
19 that's imposed, and they come hand in glove, you
20 know, that's not a one time thing. There cannot
21 be a repurposing somewhere later simply having
22 gotten past that threshold.

1 At NSA the typical events might be
2 constituted as collection, processing of data,
3 analysis of data, dissemination of that data, and
4 the burden was imposed at every step according to
5 whatever the authorities were that were granted
6 for the acquiring of that data, the acquisition
7 of that data in the first place.

8 And what we ultimately found is that in
9 order to achieve that, because data ultimately is
10 aggregated, synthesized, a typical
11 counterterrorism analyst, we take the iconic
12 analytic effort, doesn't simply use data from one
13 source, they use data from many sources.

14 And at that point it is really hard, if
15 there are different expectations of the different
16 data sets to try and keep it straight in your
17 head as to what you're going to do about that.

18 So the focus has to be how do you bind
19 the attributes for a particular data element at
20 the moment that it comes into being?

21 MS. BRAND: Could you pull the mic a
22 little closer.

1 MR. INGLIS: At the moment you collect a
2 piece of data, how do you bind the attributes to
3 that data that essentially include, but perhaps
4 some other things as well, what was the authority
5 under which this data was collected? What are
6 the burdens? What are the imposed constraints
7 that come along with that? What are the
8 proscriptions, if any, associated with that?

9 And that should be atomically bound to
10 that data element through its life, through its
11 life of collection, processing, analysis and
12 dissemination.

13 Now at some point there's going to be a
14 second order use of that data where someone
15 essentially reads a broad swath of material,
16 synthesizes that in their head and then
17 constructs a document across an air gap.

18 That gets hard, but at least in that
19 primary use of that data if you had a systemic
20 view of it from start to finish, you make the
21 auditor's job or the compliance oversight much,
22 much easier.

1 And you therefore then in your system,
2 in your technology essentially impose a
3 constraint or a check every time something
4 exercises privilege against that data, whether
5 it's a collection, or analysis, or processing, or
6 in dissemination. That makes the auditor's job
7 much easier.

8 And frankly, it has a nice deterrent
9 effect on those inside the system because they
10 know at every moment that they are held to
11 account.

12 But in my experience in government it's
13 not so much the deterrent as it is the assist in
14 an otherwise very, very rule-laden environment.

15 A typical counterterrorism analyst at
16 NSA would often deal with hundreds of constraints
17 on the data sets that are available to them
18 because various orders of the court,
19 interpretations of the court, kind of sharing
20 arrangements with various other nations would all
21 come along with their independent assessments of
22 how the data can or should be used.

1 So the bottom line is that technology
2 can help us by essentially doing an atomic bind,
3 right, meaning that it's organic to the data
4 itself of what's its provenance, and that
5 provenance should never be lost through the
6 history of that system.

7 MS. BRAND: Thank you. I'd like to turn
8 to the FIPPs, and Mr. Geiger, I was happy that
9 you raised those, and Professor Cate as well. So
10 I'd like to direct this question first to the two
11 of you.

12 So, Mr. Geiger, I noticed that in the
13 written statement that you sent to us, you talked
14 about the FIPPs but you didn't really talk about
15 the individual participation FIPP.

16 And I guess when I talk about the FIPPs
17 I'm referring primarily to the DHS version.

18 You said in your oral statement just now
19 that the FIPPs are not a smorgasbord, they're a
20 framework, you can't just pick and choose among
21 them. And if that's the case and if you have to
22 employ the individual participation FIPP, how can

1 that work in a surveillance context?

2 MR. GEIGER: So that is the toughest
3 FIPP to apply in this context, absolutely.

4 One way that you could do it, which is
5 not politically viable and perhaps not even good
6 policy, would be to loosen standing requirements
7 on individuals to bring suit for violations of
8 law.

9 But my, I think, more reasoned answer is
10 that if the individual participation FIPP is
11 lacking in the national security context, then
12 the rest of the framework has to work overtime to
13 compensate.

14 And that includes data minimization,
15 which is why I emphasize collection limitations
16 and transparency, as well as the rest of the
17 framework.

18 And I mean I absolutely recognize the
19 challenges in applying individual participation,
20 but this is one area, again, where government is
21 different than the private sector and I think
22 that difference should express itself in

1 particular in the data minimization principle.

2 MS. BRAND: Professor Cate, do you have
3 thoughts on that?

4 And I would ask also, there's been a lot
5 written and said in public more recently about
6 how perhaps the consent and individual notice
7 FIPP really doesn't work very well in the private
8 sector, either because nobody really understands
9 what they're consenting to. Even if they
10 understand it they don't have any other option,
11 so they have to consent to get the service, and
12 it's kind of a meaningless exercise.

13 Do you have thoughts on that and whether
14 the individual participation FIPP can work in
15 this context?

16 MR. CATE: Thank you very much. I do
17 have thoughts on that, especially being one of
18 the people who's written some of that.

19 I think the challenge of the FIPPs is
20 that the they often lead us in the wrong
21 direction. And I think this is a real challenge.
22 I'm not in any way trying to make it sound easy

1 or make it sound like there's a simple answer
2 here.

3 But, for example, if we think about the
4 FIPPs in sort of their classic 1980s OECD FIPPs,
5 we're talking about notice and consent, we're
6 talking about purpose specification, we're
7 talking about use limitation to the purpose
8 specified, and then we add things like data
9 minimization and individual participation.

10 And frankly, almost all of these seem
11 challenged in a modern data environment, private
12 sector or public sector.

13 In other words, how does that really
14 work? You know, there are 60 people in the room,
15 they all have cellphones, they have recording
16 devices, they have video, they have audio, I
17 don't have a policy statement from any of them.
18 I don't know about my individual participation
19 rights. I suspect they would look down on my
20 wanting to interview them each about it.

21 It's not a meaningful way to approach
22 the issue. The issue is an important one, which

1 is how to protect privacy. But shifting the
2 burden to the individual, which is what the FIPPs
3 have the larger effect of doing, is a very
4 difficult way to approach that. And I think it's
5 an impossible way to approach it in the public
6 sector environment.

7 But it also may lead to completely wrong
8 results. In other words, one of the surprising
9 things to me, and I can't believe I'm going to
10 say this in a place that's being recorded, but
11 about the Section 215 was that the NSA collected
12 all this data and did so little with it. It was
13 astonishing.

14 And so you would like to say, you know,
15 when people talk about atomically binding the
16 limits on what you can do with the data with the
17 data, I'd like to think if we thought of
18 something new we might do with the data that
19 might really have a major effect on national
20 security, we'd have a process for some sort of
21 risk analysis, what's the benefit, what's the
22 risk, what are the processes in place to protect

1 it, now let's do that thing.

2 In other words, data has real value. It
3 does in the national security environment, it
4 does in the private sector environment.

5 And I think we need to be thinking about
6 approaches here that aren't binding everything to
7 some mythical transaction that took place at
8 which in the FIPPs world we say the individual
9 agreed to this, even though I can't think of a
10 case in which the individual actually agreed to
11 it or it was meaningful consent.

12 And then in the national security world
13 we just overlook that. We just say, well, we've
14 agreed for the individual because we think it was
15 important, without again doing a clear and well-
16 documented type of risk assessment using clearly
17 articulated values and harms, benefits and harms.

18 MS. BRAND: Go ahead.

19 MR. GEIGER: If I can just make three
20 additional comments on the FIPPs. One, so it
21 does sometimes lead programs in the wrong
22 direction.

1 It is a useful framework for evaluating
2 privacy protection, but the application of the
3 FIPPs, what you're actually doing with the
4 program, you may pass muster under your privacy
5 impact assessment, but the actual the way the
6 program is conducted on the grounds may not in
7 fact be privacy protective.

8 So I don't think that the FIPPs are a
9 silver bullet, but the principles themselves I
10 think are very useful for the evaluation of the
11 program.

12 Second, there's been a long-standing
13 controversy about notice and consent being
14 inadequate, but that is why I said at the outset
15 that the FIPPs is a framework. I mean each
16 principle is dependent on the other.

17 This came up very clearly in the
18 healthcare context. People don't know what
19 they're consenting to when they receive a notice
20 from their doctor. They don't know what the
21 HIPAA privacy notice really says or means, or
22 what HIPAA does, which is why there has to be a

1 lot of additional privacy protections in place to
2 actually meaningfully protect that individual's
3 privacy.

4 And then lastly, FIPPs are not the only
5 framework. I think that it is a very useful, I
6 think it's an indispensable framework, but there
7 are certainly other frameworks that can be
8 applied and should be applied to the evaluation
9 of security or data collection programs writ
10 large.

11 MS. BRAND: Although this was the
12 subject of the first panel today and not
13 necessarily this panel, I want to ask about it
14 anyway. So apologies if I'm springing this on
15 you.

16 But I'd like to give you all a chance to
17 give any views you might have on privacy, what is
18 privacy, the sort of nature of the underlying
19 privacy right.

20 And Mr. Inglis in particular, when you
21 were at the NSA, I assume you spent some of your
22 time thinking about how to protect privacy and

1 civil liberties and as you were doing that, what
2 did you think that meant? What privacy interests
3 were you trying to protect?

4 MR. INGLIS: I would say I don't think
5 that has changed over time, though the technology
6 might hold that at risk in different ways and
7 there might be some downstream consequences,
8 given the scope and scale. But the fundamental
9 question always comes back to two things.

10 One, with respect to the perspective of
11 the individual, is there a reasonable expectation
12 of privacy for, fill in the blank what that
13 information might be.

14 That's the stuff of great legal debate,
15 but operators think about that as well,
16 particularly the operators inside the government
17 because they're constrained by the Tenth
18 Amendment to think about what is it they're
19 actually authorized to do, everything else then
20 being proscribed.

21 But the second way to think about the
22 issue of privacy is then what might you learn if

1 you take these discrete data sets and combine
2 them in a way that might then give you some
3 insight into things that were not self-evident
4 from any one of the discrete data sets.

5 You have to therefore think about the
6 problem in the aggregation, synthesis downstream.
7 Again, you might have some thresholds there that
8 you have to think your way through that you don't
9 want to go beyond at that particular point in
10 time.

11 I would tell you that at the National
12 Security Agency ethos is as important as the
13 compliance rules, the FIPPs mechanisms and things
14 of that sort. Absent ethos, absent the art,
15 right, the science will lead you astray and
16 you'll essentially get into a place where science
17 alone cannot help you essentially navigate the
18 challenge, the question of how do you achieve
19 both security and privacy in a world where they
20 are massively converged in a place called the
21 Internet.

22 MS. BRAND: Professor Cate, do you have

1 a thought on the nature of privacy?

2 MR. CATE: I was afraid we might run out
3 of time before you got to me on this.

4 I would say two things. One, this is an
5 area where I think public sector versus private
6 sector is a really important distinction and I
7 think it has to be kept clearly in mind.

8 In the private sector I think of privacy
9 mainly in terms of, if you will, harms or impacts
10 on individuals or on groups of individuals.

11 So whether that's the way we think about
12 it in the Fair Credit Reporting Act, like a
13 higher price for credit or denying someone a
14 benefit, or whether it's some other way in which
15 we think about an individual being manipulated or
16 being driven to pay a higher price or what have
17 you.

18 In the public sector I think that is
19 also true. I think all those specific impacts,
20 those harms, if you will, although I don't mean
21 to limit them to physical or financial harms, are
22 present as well.

1 But I think there's probably something
2 more in the public sector, which is privacy, from
3 I think the very beginning of the constitutional
4 debate, was seen as something about the balance
5 of power between the individuals and their
6 government, between the citizenry and the
7 government.

8 There is something quite striking, and
9 this I completely agree with Harley about, the
10 more the government knows about individuals, the
11 greater the risk that that information will be
12 used in a way that alters that balance of power,
13 that makes the government more powerful and makes
14 the individual less powerful.

15 And it's, you know, a widely observed
16 but an ironic twist as we've gone into the
17 twenty-first century, we've in many ways gotten
18 less transparency to the citizen about the
19 government and more transparency about the
20 citizen to the government.

21 That is a clear alteration in that
22 relationship, that power relationship or that

1 oversight relationship.

2 So in that sense that's why, again,
3 whether one focuses on collection or use it may
4 be a not so significant matter, but I think at
5 the end of the day it is use that matters. It's
6 knowing how can the government use this
7 information in a way that might affect me, as
8 opposed to is the information out there, which
9 seems to almost be the answer is yes now.

10 MS. BRAND: Mr. Grant.

11 MR. GRANT: I don't have necessarily the
12 answer, but I think I have sort of a framework
13 for thinking about it, which is to start to think
14 about it from the perspective of social media
15 right now because I think in that space you're
16 seeing how, especially younger people, are
17 viewing privacy.

18 If you ask, so most of the engineers at
19 Palantir are, they appear to be about 14, and we
20 had some discussions internally about sort of our
21 own information security policies and should the
22 company be able to look at social media like

1 LinkedIn, Facebook, publicly available
2 information, but look at it as part of our own
3 inside policy. There are ways to detect phishing
4 and things like that using this kind of data.

5 And they vigorously objected to their
6 own employer looking at that data, again, for a
7 reason of information security.

8 So it was interesting to explore with
9 them and to say, but you tweeted, you tweeted
10 that, which means people are going to read that.
11 It is a tool for communication to the world.

12 And they still felt, yeah, it is
13 publicly available, anybody can Google it, but
14 they still have an objection to government
15 collecting it, or even government reading it, and
16 then their employer reading it and things like
17 that.

18 So I don't know exactly what that means
19 in terms of coming up with a final definition of
20 privacy, but it suggests that people, there is a
21 different view of it. And that even public
22 information, there's still privacy inherent in

1 public information somehow.

2 And like I said, I think talking through
3 sort of attitudes towards social media and
4 understanding that could help us figure out what
5 is this, the newer conception of privacy in this
6 technological age.

7 MS. BRAND: Did you have something to
8 say Mr. Geiger?

9 MR. GEIGER: Sure. I mean, I said most
10 of it during my opening remark. I mean I do view
11 privacy in the lens of control. I view it as an
12 individual's ability to control information about
13 herself, but then also the control that the
14 entity holding information can exercise over
15 individuals.

16 I think it is very important not to just
17 look at privacy harms, or privacy interests, or
18 the extent that privacy can translate to control
19 over a individual or their decisions in the
20 context of today's technology.

21 I think that it's very important to try
22 to look out the next couple of decades and sort

1 of see what is coming down the pike. And there
2 are some very pervasive, very privacy intrusive
3 technologies that are, that I think we will see
4 in our homes and maybe even in ourselves in our
5 lifetimes and certainly in our children's
6 lifetimes.

7 And the laws have absolutely not kept
8 pace, and without a change in the law, again, I
9 reiterate that internal protections on use and
10 access, while important, are not sufficient
11 because they can change. They have changed.

12 When we talk about protecting privacy, I
13 think that we should be looking, as I said, to
14 what we are protecting several generations down
15 the line.

16 MS. BRAND: Just to get back to the
17 topic of this panel again, Professor Cate brought
18 up use restrictions. We've been talking about
19 that throughout.

20 We're focusing on how the private sector
21 might have solutions that the government might
22 learn from. Private companies are obviously

342

1 doing something to control the use of information
2 they collect. They have to. They have a privacy
3 policy that says what they're going to do with
4 your information and they have to comply with it.

5 Are there mechanisms that the private
6 sectors has used for enforcing their use
7 limitations that are particularly effective that
8 the government might learn from?

9 Mr. Grant, do you have a view on that?

10 MR. GRANT: So we see this a lot
11 obviously in terms of, so we, ourselves, don't
12 hold data but our customers hold data, and trying
13 to help them implement compliance.

14 Honestly, actually, they use the same
15 basic mechanisms that I described in my testimony
16 and often they have the same basic weaknesses.

17 You know, do they have the
18 infrastructure to manage access control to the
19 granular level? A lot of them do not because it
20 costs money and it takes time.

21 Are they conducting the oversight of the
22 data? Probably more so than some people and

1 possibly the government, again, because of
2 limited resources. But they're still probably
3 not doing it at the level that you would hope.

4 One thing I notice is that a lot of
5 them, there is, even in Europe where you have
6 more commercial privacy law and more commercial
7 privacy compliance requirements, a lot of times
8 it's best guess.

9 So, for example, one that we've been
10 running into recently now is looking into
11 cybersecurity and information security, data
12 exfiltration risks in the private sector.

13 And in these giant, multinational
14 companies they're trying to deal with employee
15 privacy laws that are all over the map.

16 And they're asking questions like, if a
17 German employee sends an email to a U.S.
18 employee, what privacy rules apply to the content
19 of that email?

20 In Germany you have to actually tell the
21 employee, I'm about to start monitoring your
22 email. In the United States you can pretty much

1 do whatever you want with a few exceptions. They
2 don't know what the answer is so they make their
3 best guess.

4 So I think there are interesting lessons
5 in terms of what the privacy is trying to do, but
6 I actually think they're facing a lot of similar
7 problems that are related to scale, that are
8 related to lack of understanding of what the
9 rules should be, as the government.

10 MS. BRAND: Anyone else have a thought
11 on that question?

12 MR. INGLIS: If I can add to it. So my
13 own sense is that there's probably a lot of great
14 technology out there that can be used, but any
15 technology can fall short of your expectations if
16 you don't use it in the right process, and
17 therefore, we ought to give as much time and
18 attention to process within which that
19 technology might be used as the technology
20 itself.

21 In the following process it might be
22 useful to consider that first and foremost before

1 you acquire any capability, whether it's in the
2 government or within the private sector, you
3 think your way through the necessity
4 proportionality considerations, you know, is this
5 necessary and have I done this only to the degree
6 that it is necessary.

7 And then what we're trying to achieve is
8 not simply the balance between security and
9 privacy, but transparency is the third leg of
10 that stool. And absent transparency, you often
11 find yourself in a place where people don't
12 believe that you achieved the right balance of
13 the first two.

14 That then derives, you know, the
15 possibility in the government the need to
16 essentially acquire explicit authority, which
17 always comes with constraints, constraints are
18 bound to that, and some measure of accountability
19 for those constraints.

20 The process elements that then are
21 essentially implemented to pull that off, I think
22 should have the aspect of continuous compliance,

1 not discrete compliance at various phase points,
2 but continuous compliance. You think about it
3 all the time, first, middle and last.

4 Kind of a stretched analogy is part of
5 the problem with the absence of cybersecurity in
6 so many environments is you think about that as a
7 bolt-on. Until such time as we build our
8 systems, operate our systems continuously with
9 that foremost in mind as the primary attribute,
10 it'll break our hearts.

11 The second process element of
12 implementation is an external component.
13 Internal components are really essential. You
14 have to hold the people accountable internal with
15 the system.

16 But unless there's an externally imposed
17 accountability mechanism, you can wind up with
18 mismatched expectations or the system might, in
19 fact, go rogue.

20 And then three, there has to be at
21 various phase points required reporting, which is
22 important because that then forces some

1 synthesis, some kind of retrospective that says,
2 how do we actually aggregate our experience in
3 this to come to some conclusions.

4 So is it meeting our expectations? Is
5 it working as it should? Are we a little bit
6 right of the course, left of the course such that
7 we actually need to invest some time and energy
8 in the process itself?

9 Absent that, you find that you're the
10 frog in the beaker and it's just getting a degree
11 hotter moment by moment, all of a sudden you're
12 the boiled frog. And you hadn't realized because
13 you didn't step back and take hard look at it
14 that you actually got off course a little bit
15 some time ago.

16 MS. BRAND: Thank you, and I think my
17 time is up, so we'll start with Mr. Dempsey and
18 go down the line.

19 MR. DEMPSEY: Thank you, and thank you
20 to the members of the panel for giving us your
21 time today.

22 In a way building off of something that

1 Chris Inglis said, or at least that I heard you
2 saying that we need the technology controls, we
3 need to build the technology in a way that
4 implements these controls, but at the same time
5 we need policies that surround them. You need
6 the legal rules, etcetera.

7 I think, John Grant, my first question
8 to you, you talked a lot about the potential in
9 terms of tagging information, and audit controls,
10 and permission controls are very granular, but
11 just to state the obvious, that's not a
12 substitute for legal rules and policies.

13 MR. GRANT: Absolutely not. We try to
14 say, you know, even when we talk about our
15 privacy enhancing capabilities and stuff, if you
16 think you're buying a switch that you can flick
17 that protects privacy, it's not going to happen.
18 It's not possible.

19 You have to be able to respond
20 dynamically to changing situations. You have to
21 be able to make human-driven nuance decisions
22 about data and about how it's used and is it

1 being used appropriately. And that's just
2 something machines can't do.

3 And it's the same reason we argue at
4 Palantir that you can't build a find terrorist
5 button, that you need a human at the top of the
6 decision-making chain and at the top of the
7 analysis chain to do it.

8 And so I distrust any technology that
9 says don't worry about it, we've got privacy
10 covered. And so what the goal should be for
11 technologists is, what kinds of tools do policy
12 makers need and then the oversight officers, the
13 oversight boards, and the civil liberties
14 protection officers and things like that, what do
15 they need and what makes their job easier or
16 possible, especially when you're dealing with
17 data at scale.

18 So an easy example is there's a lot
19 work, a lot of research going into improving
20 access control interface. When you're dealing,
21 with terabytes of information in the
22 cybersecurities space, how can you create

1 technological shortcuts to allow a human to make
2 the decisions about how to manage that data?

3 And that's how you do it. You think
4 about how do you support the policy, not how do
5 you replace the policy.

6 MR. DEMPSEY: Let me go to Fred. Fred,
7 totally accepting your point about the
8 limitations of the FIPPs and totally accepting
9 your point about the importance of focusing on
10 risk and focusing on use, you're not saying that
11 collection is irrelevant, that obviously the
12 Fourth Amendment is in some ways a collection
13 limitation.

14 And that, you know, in a commercial
15 context that company that had the flashlight app
16 that was out collecting data, nobody even got to
17 the harms analysis, that collection was
18 inappropriate in and of itself.

19 MR. CATE: Right. You are absolutely
20 right and I agree completely. In other words,
21 I'm not suggesting collection is irrelevant, I'm
22 suggesting we've made collection too much of the

1 end of the story, so that once you cross, you
2 know, it's like a spillway in a dam, once you're
3 over the collection limit, then anything else
4 goes.

5 MR. DEMPSEY: Well, the ironic thing is
6 that at NSA, as Chris Inglis said, their view is
7 they never thought of it that way, that they
8 thought that you have your collection
9 authorization which is critical, your retention,
10 your use, your dissemination, your retention
11 limit, that each one of those --

12 MR. CATE: But if I can just respond to
13 that. I think there's something of a mismatch
14 here. And I'm not in any way doubting either
15 what NSA was doing or what Chris is saying.

16 But one of the astonishing things, for
17 example, when I read the Section 215 report that
18 came out from the NSA's civil liberties office, a
19 well-written report, it was full of all of the
20 limits on what they were doing and the incredible
21 what can only be described as bureaucracy around
22 that, both technical bureaucracy and human

1 bureaucracy.

2 But it sort of ignored the fact, which
3 is what I think has struck most of the American
4 people, is how was the authorization obtained in
5 the first place?

6 You know, we had a law that said
7 relevant to a specific investigation, you know,
8 99 out of 100 people through relevant to a
9 specific investigation meant, might be focused on
10 specific individuals.

11 Apparently the 1 out of 100 who didn't
12 was a FISA judge, and then had other judges there
13 along with him, and apparently some members of
14 Congress.

15 So I think one of the critical issues
16 when thinking about going forward is if this were
17 the private sector there would have been
18 immediate customer feedback.

19 You know, if that were Facebook
20 interpreting that to say, by the way, you know
21 under that privacy policy that says we'll only
22 collect data for limited purposes, it means that

1 we're going to collect absolutely everything, and
2 then there would be customer reaction.

3 What do we create that will mimic that
4 in the classified environment, in the
5 intelligence environment? Maybe that's the
6 PCLOB. I mean maybe that's literally having the
7 outside of the agency but focused on privacy and
8 civil liberties that says we understand the
9 challenge but we think you've got the wrong end
10 of the stick.

11 But I think it is being overly focused,
12 for example, on the Fourth Amendment that creates
13 this problem. As you well know, the FISC just
14 dismissed the Fourth Amendment issues by saying,
15 well, third-party doctrine, there's no problem at
16 all. Let's go ahead.

17 And somebody should have been saying,
18 wait a minute, you're talking about collecting
19 data on everybody. And then that would have
20 focused the discussion in a way that all of the
21 technological controls and all of the
22 bureaucratic controls that have been now well-

1 documented in the agency, somehow never did.

2 MR. DEMPSEY: That's very helpful. I
3 don't want to further rehash 215, the history of
4 215, and anyhow I have a red card so I guess
5 that's the end.

6 MR. MEDINE: So let me just follow-up
7 quickly on that point. Maybe what we need to do
8 is supplement the FIPPs with the OMG standard,
9 which is, you know, in private practice I would
10 have a client and I'd say, everything you've
11 proposed to do is perfectly legal, but are you
12 nuts?

13 I mean how do we embed that stepping
14 back and saying, okay, the lawyers have
15 technically signed off, everyone has technically
16 signed off, but this is a crazy thing to be
17 doing?

18 MR. CATE: Well, I mean I think one
19 positive step is adding someone like Becky
20 Richards and an office to support her within the
21 agency. I think that's one way.

22 So you get people who aren't just

1 thinking about the law, but rather people who
2 will say, I understand legal clearance is taken
3 care of, but I still have the oh, my God
4 response.

5 Are you allowed to refer to God at a
6 PCLOB hearing?

7 MR. MEDINE: It's free speech.

8 MR. CATE: I feel very nervous about
9 that.

10 I think the PCLOB is another way. In
11 other words, you say we're going to have some of
12 those similar roles, not by any means identical,
13 but outside of the agency.

14 I think this is where I would say,
15 although this just may reflect my naivete, you
16 know, I would like to think that although we
17 certainly need to have secret operations, we
18 wouldn't have secret law.

19 And so if a law that said one thing was
20 being interpreted to mean the opposite, that
21 someone would feel the need to signal that, as
22 opposed to going out of their way to continue to

1 say, no, it doesn't mean what we actually think
2 it means, and it means what only you think it
3 means.

4 And so that we would build in avenues
5 for transparency about the law, so that at least
6 we all knew what the rules were going into it.

7 And I think that's a huge problem when
8 the law itself is effectively classified because
9 of the way in which the interpretative process
10 works.

11 MR. MEDINE: Sure, John.

12 MR. GRANT: Can I just jump in on that?
13 How we embed that in the private sector, or
14 certainly in our company, and it goes back to my
15 point about education.

16 Engineers and technologists think of
17 things in terms of does it work or does it not
18 work, and they just want to make things more
19 efficient.

20 But it's not because they don't care
21 about privacy and civil liberties. They end up
22 living in the world they create. It's just they

1 don't realize that this raises an issue.

2 So if you improve education across the
3 board so that the technologists throughout the
4 NSA and throughout the private sector that are
5 building the capabilities and things like that,
6 if they're all conscious of privacy and civil
7 liberties, they're going to raise these questions
8 too. They're going to say, what are we building?

9 And especially technology is an
10 interesting place because it's the place where
11 the engineer, the lowly engineer is more powerful
12 than the CEO, because if the engineer says, I'm
13 not going to build this, then that's it. And if
14 the CEO says, I'm going to fire you, they say,
15 okay, I've got four more job offers to go
16 somewhere else. So there's a really interesting
17 power imbalance there within the organization.

18 So if you instill the values that you're
19 looking for throughout the organization in the
20 people, that's where you're going to get the OMG
21 response.

22 MR. MEDINE: I have a question for

1 Harley and Chris. In our 702 report we noted
2 that most of the information that was collected
3 wasn't reviewed and therefore wasn't minimized,
4 and that even of the information that was
5 collected oftentimes it wasn't minimized in terms
6 of being deleted because there wasn't a
7 determination about whether it had foreign
8 intelligence value. Harley proposes doing the
9 minimization up-front when it comes in.

10 So I have a question for each of you.
11 One is, Harley, is that a practical matter given
12 how much information is coming in?

13 And I guess to Chris, if that's not a
14 practical way, how do we do minimization better?

15 MR. GEIGER: First, an unsolicited
16 answer to your first question, which is in
17 addition to the proposals that have just been
18 discussed I think a FISA court special advocate
19 would also help with the OMG standard.

20 I think that it's a multi-layered
21 solution having privacy and civil liberties
22 offices in agencies, a PCLOB and a FISA court

1 special advocate hopefully gets us there.

2 In terms of whether front-end, so what I
3 had said was that front-end minimization and
4 back-end minimization are important. And so I
5 actually, one of the things that I had said was
6 that the determination ought to be made whether
7 the information was needed and then flush it as a
8 default unless that determination is made.

9 This is different than the way that I
10 think it's done, at least in some agencies where
11 they keep the information unless they make a
12 determination that they don't need it, which is
13 very different. And that sometimes causes
14 information to languish. I think that that
15 should be flipped.

16 In terms of front-end information data
17 collection, I do think that it can be feasible,
18 but it also depends on the specific program, it
19 depends on the purpose.

20 And if the purpose is we're going to
21 collect everything, that sets off the OMG
22 standard for me.

1 But if the purpose is narrower, and I
2 think generally speaking it should be, then yes,
3 there should be data collection limitations.

4 I understand that there are technical
5 limitations there and that depending on the
6 actual means of data collection, sometimes it may
7 be unavoidable that you collect more than you
8 need, but then you should be flushing the
9 information that you don't need.

10 MR. MEDINE: I'm probably going to run
11 out of time, so Chris, if you have any reactions
12 to that?

13 MR. INGLIS: Yes, so on both parts, so
14 the question of 215, I know we don't really want
15 to rehash whether that's good or bad policy, but
16 from an NSA perspective three branches of
17 government participated in the creation of that
18 program, sustainment of that over years time,
19 multiple administrations, more than three dozen
20 judges.

21 And so from an NSA perspective, charged
22 to essentially effect the will of government,

1 short of a referendum amongst 315 million people,
2 which we do every two years, I don't know how you
3 actually kind of make a significant change in
4 terms of how the government comes to some of
5 those conclusions.

6 The PCLOB is an extremely valuable
7 addition, but you know, I think that we're always
8 going to find ourselves in a place where
9 stakeholders stand in the shoes of those they
10 serve.

11 With respect to your specific question,
12 it's problematic on a couple of counts. You
13 know, first and foremost, if you try to minimize
14 at the point of collection you then ironically,
15 paradoxically begin to focus on things that you
16 shouldn't.

17 The strange truth in the world is that
18 there are two ends of every communication in the
19 world, sometimes more, right, if you add in the
20 courtesy copies and the blind courtesy copies.

21 And if your interest is legitimately in
22 party one and you begin to then focus on party

1 two, right, who is involved in that conversation,
2 without merit, without some reasonable or
3 probable cause, you then begin to encroach upon
4 their expectation of privacy, absent some kind of
5 reason to do so.

6 So the policy at this moment essentially
7 uses this, upon recognition, which isn't a sloppy
8 policy. It just says do not focus undue
9 attention on that, and when you do encounter
10 someone who deserves further protection, take it.
11 You must take it.

12 Built into that then are some time
13 limitations for how long you can hold that data,
14 and some necessity and proportionality conditions
15 that say how much data is enough, for what
16 purpose, and how long are you going to keep that
17 without some meritorious reason.

18 So if it participates or contributes to
19 a report you keep that for longer. If it
20 doesn't, then there are time limitations, you age
21 it off. And those are always prescribed by those
22 who essentially grant us our authority.

1 MR. MEDINE: Thank you.

2 MS. BRAND: Ms. Cook.

3 MS. COLLINS COOK: So following up
4 actually on a phrase that's been used a number of
5 times today and asking the same question I asked
6 a previous panel, there's this notion of
7 reasonable expectation of privacy.

8 To the extent that that evolves over
9 time, which I think that it does, how does one
10 ascertain what is a reasonable expectation of
11 privacy?

12 Is it based on a Washington Post poll
13 that 50 percent of Americans are uncomfortable
14 with X, Y or Z? Is it the conduct that
15 individuals nonetheless engage in, that they're
16 uncomfortable about communications surveillance
17 but people still use their phones, they still
18 engage in the world?

19 If we were going to look to reasonable
20 expectation of privacy as a touchstone, how
21 should we ascertain what it is?

22 This is a question for the panel.

1 Chris, I'll start with you because you had
2 indicated that the NSA did look to reasonable
3 expectation of privacy as one of their
4 guidelines.

5 MR. INGLIS: First and foremost, there's
6 a basis of law which doesn't, if the technology
7 changes over time give us, say, a free pass to
8 say because the law allowed us to use the old
9 technology in this way, the new technology, which
10 is more intrusive, can simply just continue
11 unabated.

12 But there is a wide practice of law and
13 the NSA considers that, you know, as it makes its
14 appeals for authorities, which are always
15 conditioned upon a Department of Justice
16 representation and the right authority, either
17 under 12333 or the courts.

18 Second, there is an expectation at a
19 place like NSA that you think through the eyes of
20 those whose privacy would be encroached upon,
21 right. So you think about what's the expectation
22 of the individual and is their expectation such,

1 regardless of what the law might say, that this
2 is something that deserves some aspect of
3 privacy.

4 And that necessarily then has to inform
5 the conversation about what authorities you seek
6 and what then provisions you seek those
7 authorities for.

8 Interesting dialogue earlier about the
9 215 program and the internal bureaucracy. At NSA
10 we thought that was a feature, right, that the
11 court essentially proscribed use of that database
12 for anything but the very surgical and narrow
13 application of it.

14 The sense at NSA was, is that if we had
15 even requested to use that for other purposes,
16 say, domestic terrorism, which is not our
17 provenance, or say, weapons of mass destruction,
18 rogue nations, that that would have been an
19 encroachment into privacy that was excessive and
20 therefore not meritorious right up front with
21 respect to the possibility we might ask for that.

22 The program as designed was very

1 surgically, narrowly framed on something alone,
2 which was warranted and justified under the
3 concept of necessity and proportionality.

4 And we had to avoid the creep beyond
5 that because of an expectation based upon the
6 consumer looking back at us, as to what they
7 might think.

8 MS. COLLINS COOK: John, you also used
9 the phrase as well I think here, and so if you
10 have some thoughts on this.

11 MR. GRANT: The thing that jumps to my
12 mind and it gets back into, again, when I was
13 talking about analyzing data to sort of support
14 the effects of this program, I think it's
15 reasonable to expect that the government won't
16 look at data that's not useful.

17 That is a reasonable expectation of
18 privacy, that the information that has not proven
19 effective for some purpose, that that won't be
20 collected and analyzed.

21 And that's what we've been doing, as I
22 said, rewriting our internal information and

1 security policies, and as we've surveyed
2 everybody at the company they've said, I'm fine
3 with you looking at some of this data, just tell
4 me that it's useful, tell me why you're looking
5 at it.

6 Because of course they're interested in
7 protecting our own internal information security
8 at Palantir, and of course we're interested in
9 protecting our own national security.

10 So I mean this isn't the only standard.
11 Obviously utility can't be the only analysis
12 point because there obviously are interests
13 beyond that, but I think it's a significant
14 question that we don't answer very well right
15 now.

16 And this is, you know again, across the
17 board from that sector to the private sector,
18 everybody wants data and they think they can do
19 all of this stuff with data.

20 And we get customers all the time who'll
21 come in and say, I've got to understand the
22 Twitter. And we'll say, well, what do you want

1 to know? And half the time, we'll say that
2 information, if you want to understand do a lot
3 of people like Justin Bieber or cats, then
4 Twitter's great. If you want to understand more
5 complex, nuanced theory, then maybe we should
6 think about something else.

7 And I think that government should do
8 the same. And I think the government can answer
9 those questions, again, looking at, analyzing how
10 data is used and using that data about data.

11 So to me that's one area where you would
12 sort of expand that definition of reasonable
13 expectation of privacy, which is it's reasonable
14 to expect no one will look at data that isn't
15 useful.

16 MR. GEIGER: The question you pose is a
17 very difficult one. I mean courts are wrestling
18 with it all the time. And everyone has a
19 personal opinion about it, and so do I. I
20 believe that reasonable expectation of privacy is
21 a terrible framework actually.

22 The Fourth Amendment is supposed to

1 protect against unreasonable searches and
2 seizures. The reasonable expectation of privacy
3 is a judicial-made creation that has now allowed
4 for some very unreasonable searches and seizures.
5 Section 215 is a great example of that.

6 Under the reasonable expectation of
7 privacy framework, U.S. versus Jones
8 notwithstanding, because I know that's kind of a
9 mysterious opinion, but the Supreme Court seems
10 to be sort of moving, inching along perhaps in a
11 direction where they are doubting the reasonable
12 expectation of privacy framework as it's been
13 applied in the past several decades.

14 But under current law would it be okay
15 under the reasonable expectation of privacy test
16 to have a network of drones or a network of
17 ground-based cameras that watch everything that
18 you do the moment you step outside of your house?

19 I mean there is a very strong argument
20 that, yes, that is okay under the reasonable
21 expectation of privacy framework.

22 So I think that it's the wrong framework

1 to be viewing a lot of this stuff. I think that
2 it does not have to be left out of the
3 conversation, just like the FIPPs, it is one
4 framework.

5 There should be multiple lenses, but
6 none of them, including reasonable expectation of
7 privacy, like the FIPPs, are going to be a silver
8 bullet. And they're not going to provide you
9 with a clear answer.

10 MS. COLLINS COOK: I think if I have
11 time for one additional question, I'm still
12 seeing yellow.

13 So moving up the analysis of data and
14 requiring agents or analysts to make an
15 assessment of whether or not information is
16 relevant or is necessary to maintain, rather than
17 potentially letting that information simply age
18 off of your system, what about the privacy
19 implications of that type of approach, which to
20 me, I have been unable to get past this notion
21 that that would require agents or analysts to put
22 eyes on more communications than they would

1 otherwise review. And so what is your answer to
2 the privacy implications of that shift?

3 MR. GEIGER: I mean I suppose that there
4 are two ways to do it. You could require the
5 agent to look over every piece of data that
6 they've collected.

7 If the amount of data is small, which is
8 my main point, I mean having, not data retention
9 but collection limitation at the front-end. If
10 the data population is small that is less of a
11 problem.

12 If you're requiring the agents to look
13 through a large amount of data that you know
14 contains information about individuals who are
15 not connected to a crime or terrorism, that
16 becomes more of a problem.

17 Then on the flip side I suppose you
18 could have the agent merely looking at data that
19 they know is connected to other parts of their
20 work.

21 I mean I don't think there's a hard and
22 fast rule. It's going to be depend on the

1 program, it's going to depend on what the agent
2 is looking for.

3 For that reason I think that data
4 minimization, again, on the back-end is not the
5 answer. It has to be part of the framework. And
6 collection limitation at the front-end is a
7 crucial part of that framework.

8 MS. BRAND: Judge Wald.

9 MS. WALD: Whether or not you think that
10 it's important to limit collection or you think
11 perhaps you can wait a while or see and go after
12 it more forcefully at the use end, I'm interested
13 in what you think the role of the courts are.

14 In our other systems like criminal
15 justice, ultimately, and even under the Fourth
16 Amendment, the courts are kind of the final
17 analysis. And even in many of our civil
18 regulatory systems ultimately they come up.

19 So the question is two parts. At what
20 stage, whether you believe in collection
21 limitations or you believe more in use, do you
22 think the internal, all of the internal audits

1 and various other techniques that we've talked
2 about are not enough, that you need some kind of
3 an outside look at it?

4 But secondly, I think as a former judge
5 I ask this question, if you were scared to come
6 before -- and that is, do you really think that
7 the limited role that the FISA court has been
8 allowed to play in terms of the secrecy of its
9 operations, and even with our recommendation and
10 other people's suggestion about adding an
11 adversary, and even some of the judges on that
12 court, not only did they come out in different
13 ways, all judges do, but they were frustrated
14 themselves in terms of the technology sometimes.

15 Judge Bates remarked that it was
16 practically impossible, given all of the
17 complexity of the technology we've talked about
18 and the fact that these judges would come in from
19 their regular work for a week at a time and then
20 go back again, is that the best kind of outside,
21 not outside surveillance, outside look, an
22 independent look, or is there some better way to

1 get the notion of an independent, the Supreme
2 Court always talks about independent and neutral?

3 It's a big question. Go at it, starting
4 with Professor Cate, any way you want.

5 MR. CATE: Thank you very much, Judge
6 Wald. I would say I think the role of the courts
7 is absolutely essential. I think the important
8 feature of that role is it needs to be an
9 independent role, and I think one of the concerns
10 with the FISC is that as this set of opinions
11 went back and forth and, you know, small
12 modifications, and updates, and briefings and
13 corrections, it involved the court in the more
14 daily operation of the agency than I think we
15 would typically think appropriate or desirable,
16 that we really want an independent, neutral and
17 detached court.

18 The challenge of technology is huge for
19 all of us. Even engineers have difficulty
20 keeping up with the technology. I think there
21 are, and we have seen some ways of dealing with
22 it. One is court-appointed experts.

1 Another, as we saw in the Supreme
2 Court's most recent privacy opinion this summer
3 it cited heavily to amicus briefs from CDT, and
4 from EPIC and others where they explained the
5 technology and the impact of the technology, and
6 the court clearly relied on them. And I think we
7 shouldn't overlook that.

8 And then of course courts also have
9 remarkable powers to compel the parties to
10 explain the technologies in clear and
11 understandable language and to not accept their
12 filings or to not rule on their filings until
13 they do.

14 So I could say more but let me share the
15 microphone.

16 MR. GEIGER: I absolutely agree with
17 everything Professor Cate just said. The courts
18 play a very crucial role in the oversight of
19 national security surveillance programs. I think
20 that the court is constrained by a lot of
21 statutory limitations.

22 I think we would welcome, at least the

1 privacy advocacy community would welcome court
2 oversight of minimization procedures and on the
3 ground controls on privacy.

4 I know the court does some of that, but
5 I know that it is also limited to sometimes just
6 a certification.

7 We have talked about having a special
8 advocate. I don't necessarily view that person
9 as an adversary because I think that in many
10 cases the court and the government are also
11 trying to protect privacy, they just maybe differ
12 on the strength of that privacy protection. So I
13 think that the special advocate could, in fact,
14 be an ally.

15 But then also technical experts and
16 amicus. One of the problems that we're seeing in
17 the debate over bringing in amici or bringing in
18 a special advocate is that there are some forces
19 in the court, perhaps formerly of the court, who
20 would like to see greater restriction placed on
21 those parties, so that it is the FISA court that
22 instead gets to decide what role and what access

1 to information these amici will play, which will
2 severely undercut their effectiveness and their
3 ability to help the court. So I would urge
4 resisting those calls.

5 MS. WALD: Don't you think, this is a
6 follow-up just on the point you made, don't you
7 think that in some cases, even the legal or even
8 possibly constitutional reasonableness of
9 something is dependent on understanding the
10 technology of it?

11 I mean I think Judge Bates felt that
12 way --

13 MR. GEIGER: Certainly.

14 MS. WALD: In one of the cases that was
15 declassified and put out that way.

16 So you think that they are equipped to
17 do that now, or do you think the advocate will
18 fill that role, or do you need more?

19 MR. GEIGER: So I don't know enough
20 about the judges to make a determination about
21 their level of familiarity with technology.

22 But I mean this technology that is

1 being exploited in some of these instances can be
2 extremely complicated, and so, no, I would not
3 imagine that most lawyers have that sort of
4 training and so I think that there -- I know that
5 the court already has powers to some extent. I
6 think those should be loosened to bring in
7 technical experts as amici to explain this in as
8 clear a manner as possible, because I think
9 you're absolutely right, technology does have a
10 direct bearing on the rights that are being
11 manipulated.

12 MR. GRANT: And so I'll just jump off
13 that one. I think that it's critical to have a
14 translator role for the court, someone to help in
15 an unbiased way try to explain the technology.

16 And you know, this isn't just an issue
17 for the court, it's an issue for Congress. You
18 know, I was trying to write cybersecurity
19 legislation before I left and one of the
20 challenges was you have to have a really complex
21 technical debate and members are naturally going
22 to be uncomfortable taking a strong stand when

1 they're not a hundred percent sure what the
2 technological considerations are. And the end
3 result is you sort of paralyze things.

4 I think the critical question, so the
5 court role is vital and it's important that it
6 takes time because, you know, by nature that
7 briefs out the issues and it helps you understand
8 things.

9 The challenge is what are you doing in
10 between. Because technology becomes ubiquitous
11 even in a matter of months sometimes, and it
12 starts to have a real effect on people's lives
13 right away, and it's going to take 10, 15 years
14 sometimes for the court to eventually settle on
15 what they want to do.

16 So what do you do in the meantime and
17 how should people be guided? Should there be
18 ethical limitations on what the private sector
19 wants to do? Should the government figure out
20 ways to sort of slow walk in technology? And
21 what's the framework for making that decision and
22 implementing that? I think that's the real

1 challenge.

2 MR. INGLIS: I largely agree with what's
3 been said. I think that with respect to the role
4 of the court neutral and detached is, I think,
5 the right way with respect to their opinion on
6 the efficacy of the policy or the government's
7 representation. But they have to have a solid,
8 if not exquisite understanding of the technology,
9 and I would distinguish between the two.

10 I think the role of an adversary and a
11 technology expert at the court, you know, has
12 great merit and would, I think, add to their
13 ability to at least understand the technology.

14 And we have to hedge our expectations,
15 not because the government wouldn't want to
16 reform, but at NSA could be perhaps exhaustive
17 about technology at some moment in time in its
18 presentation to the court, but at best it can
19 only be illustrative as to where that technology
20 is going to go. Nobody knows where the
21 technology's going to go.

22 And the use of a certain technology,

1 even if the technology doesn't change, change is
2 in and of itself. People make different use of
3 technologies.

4 And so forecasting that is, I wouldn't
5 say a fool's errand, but it's really hard.

6 MS. BRAND: Thank you. We have a couple
7 of public questions. We may only have time to
8 get to one of them.

9 But Professor Cate, I think this is
10 directed at you. It says, if you don't like the
11 FIPPs, what alternative do you suggest?

12 MR. CATE: So first of all, to be clear,
13 I'm not saying I don't like the FIPPs, I just
14 don't think the FIPPs are the be all and end all.

15 And second of all, I suggested risk
16 management as a pretty useful tool as a way of
17 identifying both potential negative impacts and
18 also beneficial impacts.

19 And you know, one of the things we
20 haven't talked about is the value of the use of
21 data for national security or foreign
22 intelligence gathering or whatever.

1 And one advantage of a risk management
2 approach is it helps focus on both sides of that
3 equation. It helps drive towards specificity.
4 So if you ever want a documented decision that
5 reflects that analysis, it's one way to help
6 focus attention on it.

7 And then as we identify those potential
8 harmful impacts, negative impacts, whatever we
9 want to call them, we can then look for tools
10 that help minimize those impacts.

11 So if the harmful impact is if you
12 collect all this data it might be stolen, we can
13 talk about security.

14 If we collect all this data and the fear
15 is that the government might repurpose it for
16 some other use, then we can talk about use
17 limitations that would help address that.

18 But I think a great advantage of doing
19 this is it makes clear in a way that the FIPPs do
20 not, where should we be focusing our attention,
21 whether we are academics, or the PCLOB or, you
22 know, with the process within an agency.

1 MS. BRAND: Okay, thank you.

2 Mr. Chairman.

3 MR. MEDINE: Thanks again to the
4 speakers on this panel and all the panels
5 throughout the day, as well as the audience
6 members who submitted questions.

7 I think we've had a remarkably
8 informative and thoughtful discussion. We've
9 heard from academics, government officials,
10 advocates, technologists in industry, which is a
11 lot, and we've covered a broad range of topics,
12 FIPPs, Fourth Amendment, collection and use,
13 encryption, de-identification, oversight,
14 accountability, technology, mosaic theory and
15 bulk data all in one day.

16 So you've given us a lot to chew on. I
17 think this is very helpful for us as we consider
18 how to move forward carrying out our mission to
19 balance national security with privacy and civil
20 liberties.

21 So unless any other Board members have
22 any comments, today's Board activities are

1 complete.

2 We encourage anyone who has comments,
3 whether panelists, or members of the audience, or
4 others to submit written comments. We're
5 accepting comments on regulations.gov through the
6 end of the year.

7 A transcript, again, of this day's
8 activities will be posted on our website,
9 pclob.gov.

10 And with that, I move to adjourn the
11 hearing. All in favor of adjourning say aye.

12 (Vote taken.)

13 MR. MEDINE: We are adjourned. It is
14 now 4:15. Thank you very much.

15 (Whereupon, the hearing was adjourned.)

16

17

18

19

20

21

22

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

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of
the State of Maryland, Baltimore County, do
hereby certify that the proceedings contained
herein were recorded by me stenographically; that
this transcript is a record of the proceedings.

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

As witness my hand and notarial seal
this _____ day of _____,
2014.

Lynne Livingston

Notary Public

My commission expires: December 10,
2014

A	64:4 168:18	127:15,19	accumulating	282:6 301:12
abandon 19:10	absolutely 42:18	130:6 131:7	33:4 139:17	336:12
38:13	84:14 132:21	132:4,18	accumulation	acting 107:11
abandoning	146:16,19	146:10 153:16	45:7	208:22
288:5	151:4 152:3	162:13 168:6	accuracy 93:14	action 28:1
abide 158:16	177:21 194:17	170:12 188:20	93:17,19	69:19 281:21
172:21	254:22 284:2	191:5 195:21	accurate 41:9	298:12 385:11
ability 44:17	287:15 313:17	221:12,15	48:15 84:14	actions 22:11,19
48:12 111:2	316:12 327:3	233:8 241:6,7	93:9,12 94:1	198:17
121:1 161:3	327:18 341:7	249:15 293:5	158:21 159:12	active 135:16
165:9 195:13	348:13 350:19	300:10 306:4	accurately	284:15
228:20 239:15	353:1 374:7	307:17,18,21	18:22 99:3	actively 113:5
266:4 340:12	375:16 378:9	307:22 308:1,1	achieve 86:4	144:3 145:20
377:3 380:13	absolutist 73:8	308:4 310:13	114:17 289:2	161:16
able 23:11 41:11	abundance	341:10 342:18	313:22 314:3	activities 14:2
64:5 89:14	139:12	349:20 376:22	316:16,19	28:20 39:13
90:19 135:12	abundant	accessed 94:5	317:11,12	45:15 46:14,21
146:2,2,5	138:14	190:20 306:22	323:9 335:18	50:6 128:13
155:5,6 166:8	abuse 30:18,19	accesses 39:9	345:7	130:8 182:12
166:10 170:11	31:7 62:6 85:4	168:1	achieved 345:12	183:5 208:4,5
170:19 181:8	86:6 94:18	accessible 75:1	achieving	210:2,11
182:8,10 183:3	113:22 169:18	162:5	304:13	211:13,16
184:9 188:22	abused 55:16	accomplish	acknowledged	214:5,20
190:1 195:6,21	abuser 114:2	291:16 300:16	95:16 123:10	217:10 218:2
202:18 205:17	academeia	300:21	132:8	219:13,21
208:11,15	234:13	account 36:13	acknowledge...	223:8 224:14
221:8 270:16	academics 274:7	37:2,5 68:16	84:11,15	224:15 225:18
270:18 279:15	382:21 383:9	104:6 225:3	acknowledges	226:13 230:8
285:21 304:14	academy 181:15	231:7 247:8	292:9	231:6 242:14
307:1,2 309:22	313:10	268:20 318:1	acquire 42:20	246:14 247:5
310:9 311:22	accept 40:6 70:6	325:11	345:1,16	251:8 254:19
312:2 317:7	98:16 99:9	accountability	acquired 151:1	268:17 271:19
338:22 348:19	101:4 375:11	21:19 22:1	acquiring 323:6	272:1 279:15
348:21	acceptance	24:13,17 52:16	acquisition	302:8 383:22
ably 101:21,21	213:7	71:13 72:19	43:12 323:6	384:8
abroad 227:17	accepted 95:8	73:18,19 83:22	acromyn 220:2	activity 5:1
absence 173:21	97:5 106:11	84:8 85:7 86:2	acronyms 296:5	20:18 21:3,10
346:5	149:19 204:8	94:6 126:5	act 14:7 21:7	31:2 39:11
absent 335:14	accepting 350:7	127:9 129:2	22:6,7,18	53:17 65:3
335:14 345:10	350:8 384:5	223:1 225:4	77:22 103:6,14	70:22 183:13
347:9 362:4	access 45:4 75:9	276:17 345:18	130:14 212:6	212:5 218:11
absolute 23:10	78:11 93:2	346:17 383:14	216:5 221:10	233:1,4 245:2
31:22 32:9	104:19 112:15	accountable	222:12 229:19	248:18 260:22
	115:6 127:14	237:2 346:14	240:21 281:10	262:4 265:7,11

281:17	230:12 231:12	adopts 12:1	383:10	281:17 371:5
actors 94:21	236:1 240:6,7	advance 10:10	affairs 33:12	371:18 372:1
107:15 228:7	270:4 272:14	69:14,16 86:12	189:17	agents 107:12
308:20	297:11 382:17	advanced 40:14	affect 20:1	370:14,21
acts 26:20	addressed 3:10	91:17 170:8	202:9 212:13	371:12
174:18	6:5 20:22	advances 27:5	312:2 338:7	aggdom 217:20
actual 154:7	179:18 203:22	226:15 228:21	affiliation 37:13	220:4
156:4 291:19	230:14	advancing 77:5	afraid 336:2	aggregate 61:3
322:12 332:5	addresses 49:20	77:6 187:16	afternoon 203:4	61:7 77:22
360:6	adequate 24:12	234:4	203:7 284:22	89:7,15 163:10
adage 247:12	24:17 29:22	advantage 12:18	afterward 38:21	164:12 258:9
adapt 146:6	30:11 61:17	317:17 382:1	age 25:15 74:21	347:2
149:17	83:21 154:19	382:18	168:7 186:6	aggregated
adapting 277:22	adequately	advantages	297:9 340:6	77:15 129:17
278:1	22:22 72:18	38:18	362:20 370:17	236:13 323:10
add 10:20	94:7 211:4	adversarial	agencies 39:3	aggregating
119:10 198:11	adequatly 262:2	130:13 212:10	40:13 41:4	40:2 256:8
244:11 296:12	adhering 125:15	adversaries 89:6	74:2 81:9 91:1	aggregation
315:15 329:8	adjourn 384:10	208:14,16	114:10 133:1,5	47:4 48:2
344:12 361:19	adjourned	267:11	205:9 208:14	50:17 61:15
380:12	384:13,15	adversary	208:22 211:10	77:3,14 78:1
added 307:7	adjourning	135:16 280:7,7	212:14,17	161:3 258:7
adding 60:12	384:11	373:11 376:9	241:7,17	335:6
354:19 373:10	adjudicated	380:10	244:19 248:20	ago 123:14
addition 115:21	70:16	adverse 56:3	264:20 267:8	137:16 149:19
239:22 298:21	adjudicator	60:7,18 62:4	298:5 299:17	167:10 229:9
358:17 361:7	29:18	adversity 55:9	306:11 319:14	288:6 306:12
additional 12:18	adjust 100:14	advertised	358:22 359:10	347:15
81:9 154:13	admendment	295:11	agency 3:14	agree 8:9 31:13
181:9 185:7,8	281:20	advice 172:3	63:3 189:16	50:11 52:2
236:18 258:9	administration	207:13 216:3	209:10,14	65:22 77:8
270:19,20	44:15,20	225:15 241:15	217:7 222:13	78:3,13 84:17
274:10 331:20	128:18 222:6	advising 124:19	226:1 242:3	87:10 89:16
333:1 370:11	282:7	advisor 25:6	249:15 251:18	96:20 97:1
additionally	administrations	215:13	256:16 264:5	98:3,10 108:2
129:9 228:19	360:19	advocacy 42:6	273:22 275:11	125:21 146:13
addon 198:19	administrative	295:15 376:1	277:11,12	149:13 186:16
address 26:5	29:21 30:9,12	advocate 85:21	319:8 335:12	189:9,20
46:20 47:1,21	59:3 95:7	212:9 240:16	353:7 354:1,21	281:22 296:15
50:7 67:5	administrativ...	244:18 358:18	355:13 374:14	313:17 314:6
105:4,7 114:13	281:7 282:10	359:1 376:8,13	382:22	315:9,10
132:8 163:9	adopt 145:9	376:18 377:17	agencys 221:13	316:11 337:9
164:11 182:1	adopted 100:4	advocated 168:4	225:12	350:20 375:16
207:8 217:13	adoption 125:8	advocates 274:7	agent 23:6	380:2

agreed 6:19 331:9,10,14	226:15	383:12	308:13 310:19	132:7 157:1
agreement 97:4 97:19 100:8 129:16	alphabetical 109:18	amendments 87:22 314:12	312:19 313:1	anonymity 5:3
ahead 51:2 201:21 202:2 331:18 353:16	alteration 337:21	american 16:12 131:6 163:14 168:2 197:15 214:6 252:19 278:18 352:3	321:18 323:3 324:11 325:5 330:21 349:7 350:17 367:11 370:13 372:17 382:5	anonymization 113:6,13,19 159:4 162:7 175:16 196:9
aim 21:15	alternate 30:12 298:4	americans 119:22 122:7 122:16 200:22 201:3 363:13	analyst 174:6 323:11 325:15	anonymized 113:10 196:17
air 324:17	alternative 381:11	amici 376:17 377:1 378:7	analysts 256:11 321:17 370:14 370:21	anonymous 198:12 269:16
airbags 40:8	alternatives 113:3	amicus 375:3 376:16	analytic 39:4 304:13 320:10 323:12	answer 26:9,10 58:10 76:10 102:18 103:9 107:8 155:14 175:21 197:9 199:15 237:18 238:16 267:14 327:9 329:1 338:9,12 344:2 358:16 367:14 368:8 370:9 371:1 372:5
airplanes 294:19	alters 337:12	amount 23:1 63:7 72:18 91:4 137:18 150:2 152:12 178:4 182:16 306:8 320:6 371:7,13	analytics 35:5 35:17 47:9 114:22 304:5 305:20	answering 141:15 230:5 318:15
airport 58:15	altogether 32:7	amounts 186:17 310:7,15 320:3 320:7	analyze 34:3 105:1 117:16 228:20 232:2 320:2,3	answers 76:2 108:11 313:16
akin 26:16	alvaro 3:4 117:3 117:3,8 146:21 166:18	analogy 40:4 133:19 194:19 346:4	analyzed 37:11 366:20	anticipate 58:11 181:17 282:18
alex 3:11 203:14 206:4,16,22 219:16 223:20 241:4 245:8 246:22 247:11 252:17 262:5 264:6 275:21 278:16 310:5	amassing 104:17	analysis 11:7 37:17 40:18,22 41:9 50:22 62:9,12 65:17 90:19 91:7,13 91:18 94:3 101:13 105:13 111:12 115:13 117:15 229:17 229:20 230:4 231:2 233:11 233:20 236:18 260:18 263:8 269:22 270:19 273:20 293:22	analyzing 40:3 233:14 312:20 366:13 368:9	antilock 40:8
alike 137:8	amazon 93:13 93:15		ancient 8:10	antiques 25:22
alleged 130:20 241:9	ambitious 7:22		anecdotal 311:4	antiterrorism 182:21
allies 227:15	amend 282:6		anecdote 310:17	anton 3:3 110:12,19 116:17,22 142:8,21 144:11,18 145:14,17 146:16,19 159:2 160:1,13 162:1 164:16 166:5 175:17 176:17 177:21
allow 91:17 292:10 298:21 298:22 301:16 350:1	amended 221:15		anecdotes 312:20	
allowed 78:21 243:20 355:5 364:8 369:3 373:8	amendment 12:20 14:22 27:22 29:13 42:2,14 43:6 52:10 53:7,14 64:13,22 70:1 71:15,17,22 72:6,7,8,21 80:19 81:8 82:1,2 103:18 107:5,9 121:5 121:6 167:14 167:19 168:19 221:12 229:16 292:6,13 293:14,18 294:3,5 314:15 334:18 350:12 353:12,14 368:22 372:16		anew 53:12	
allows 14:8 34:21 38:20 52:10,10 132:17 277:19 307:14			angeles 182:7	
alluded 172:6 185:12			animate 98:14	
ally 376:14			animates 85:4	
alongside			annie 3:3 110:12 110:18 165:18 176:1	
			announce 161:16	
			announced 4:9	

184:7 185:3	107:10 135:2	approaching	argue 63:3,9	87:2 100:12,20
186:22 187:1	272:1	211:6 295:7	89:10 118:19	100:22 105:20
194:7,11,17	apply 46:1	appropriate	317:9 349:3	182:14 196:15
195:19 198:11	64:11 75:16	25:13 32:19	argued 38:12	229:21 233:3
199:14 200:13	80:22 81:11,14	71:12 73:1	argues 150:13	238:19 262:11
antons 189:10	82:9,13,16	94:5 168:13	arguing 129:11	282:20 288:20
anybody 55:16	86:18 113:7	169:6 258:20	argument 18:11	289:4 318:18
58:7 64:9 81:4	114:3 119:15	261:3 374:15	18:12 43:14	343:16 363:5
164:14 182:1	162:17 163:3,4	appropriately	90:2 120:8	asks 41:2 104:5
244:1 339:13	187:14 191:10	52:22 73:7	167:7 310:18	aspect 48:10
anymore 149:21	196:10 202:14	94:1 130:6	311:4 369:19	58:4 236:15
209:20	208:2 220:1	209:1 248:6	arguments 18:9	345:22 365:2
anyway 64:21	260:7 271:9,10	349:1	18:12 268:5	aspects 8:9 11:5
106:16 333:14	271:18,20	appropriation	arises 29:1	15:19 42:1,5
apart 256:4	272:4,8 273:1	5:9	arm 56:20	45:16 54:12
apologies 33:10	276:1,10	approval 219:11	arms 68:18	55:2 59:11
333:14	297:16 299:16	222:8 223:11	298:18	101:12 199:18
apologize 10:10	320:1,2 327:3	281:13 308:15	arrangements	211:15 248:13
app 350:15	343:18	308:18	325:20	249:3 251:19
apparatus 89:14	applying 3:17	approved 222:7	array 62:15	315:11
apparent 199:6	46:11 82:7,10	314:22	319:4	asspersions
266:8 273:22	112:12 271:15	arbitrary 102:5	art 233:17,19	123:16
apparently	300:3 327:19	architect 3:7	234:17 236:16	assembled
352:11,13	appreciate	62:20 134:15	261:14 270:14	204:22
appeals 364:14	25:11 116:3	architecture	316:8 335:14	assert 112:11
appear 6:19	132:6,21	217:5 221:1	article 45:12	asserting 191:20
338:19	134:21 165:16	225:5	46:6	assertion 27:4
appears 17:15	215:8	archive 306:16	articles 54:3	assess 205:5
80:8	approach 5:18	archives 222:6	195:13	231:18 236:9
applaud 287:16	12:8 40:1	area 96:5	articulable	254:19
apple 112:3	53:21,22 61:21	105:20 184:8	60:13	assessesment
applicable	72:7 88:3	184:18 200:7	articulated	218:20
182:20 216:4	98:20 105:8	280:9,18	272:3 331:17	assessing 245:12
223:21	111:11 125:3	293:11 327:20	articulating	245:15
application	126:17,20	336:5 368:11	204:3	assessment
106:18 299:20	173:14,15	areas 46:14	arts 235:12	221:20 223:13
303:3 332:2	187:8 231:2,4	69:19 192:9	ascertain 363:10	231:14 232:20
365:13	244:3 289:16	276:5 294:9	363:21	233:6 261:12
applications	291:13 329:21	arent 20:17	aside 58:17	290:5,18
32:17 137:2	330:4,5 370:19	24:15 29:19	97:21 317:15	331:16 332:5
143:5 159:5	382:2	166:16 173:4	asked 157:9	370:15
applied 6:7 72:1	approaches 39:3	200:15 309:15	216:10 219:22	assessments
333:8,8 369:13	172:8,9 235:7	321:4 331:6	239:3 363:5	204:10 219:13
applies 42:15	331:6	354:22	asking 80:18	220:13 223:9

224:21 240:20 241:1 325:21 assist 254:2 325:13 assistant 25:7 136:10 associate 124:22 associated 194:9 214:4 232:22 247:19 324:8 association 11:3 associations 16:19,19 153:3 assume 64:11 107:13 333:21 assuming 92:19 256:20 assumption 186:17 254:5 assurances 130:17 131:13 212:17 assure 55:15 182:14,15 astounding 330:13 351:16 astray 335:15 atheist 140:18 atmosphere 54:18 atomic 326:2 atomically 324:9 330:15 attach 34:10 attack 141:8 161:16 170:13 170:20 195:5 attackers 112:1 attacks 111:16 112:15 138:1 141:3,6,10,12 169:14 170:4,7 attempt 7:21 130:17 212:12	attempted 282:5 attempting 11:14 174:7,11 attempts 68:20 131:8 212:4 255:17,17,18 attendance 16:19 attends 192:8 attention 5:4 95:11 150:2 155:15 157:4,5 158:6 243:8 286:6 287:12 292:2 293:8 344:18 362:9 382:6,20 attitudes 340:3 attorney 29:5,8 112:10 206:17 215:13,17 217:19 attorneys 237:12 attracts 95:11 attribute 346:9 attributes 323:19 324:2 audience 6:13 9:21 88:9 102:3 109:1,9 110:5,7 141:22 154:12 181:12 278:7,11,15 281:3 286:12 318:8,13 383:5 384:3 audio 329:16 audit 31:19 93:3 94:4 95:3 308:9 310:12 320:7,17,18 321:1,6 348:9 auditing 57:21	246:13 276:18 308:22 321:1 321:22 auditors 324:21 325:6 audits 56:8 372:22 authenticated 112:16 authorities 204:17,18 209:17 229:18 302:6,9 323:5 364:14 365:5,7 authority 107:11 219:20 242:13 301:20 314:17 322:18 324:4 345:16 362:22 364:16 authorization 351:9 352:4 authorize 302:12 authorized 112:16 131:7 265:1 334:19 authors 16:13 automatically 142:6 245:4 automating 308:14 automotive 26:4 autonomously 142:6 autonomy 27:4 availability 194:15 available 14:15 14:19 15:3 32:22 35:19 36:21 40:7 75:5,12 90:8 92:6 106:4,13	160:19 161:10 173:8 185:2 186:9,18 187:2 188:18 189:3,4 189:5 205:18 219:5 220:13 250:2 287:1 295:4 306:11 325:17 339:1 339:13 avalanche 34:18 35:13 37:2 ave 1:13 avenues 356:4 average 141:8 152:14 avoid 68:8 208:16 366:4 avoiding 5:6 avoids 12:14 awang 7:15 aware 79:17,18 153:12,17,18 154:14 157:12 173:8 252:20 266:12 awareness 79:15 172:10 174:21 309:19 awful 43:11 96:11 axes 45:3 aye 4:18 384:11	184:12 203:9 217:11 255:13 284:15 286:15 305:12 318:9 318:16 321:3 334:9 341:16 347:13 354:14 356:14 366:6 366:12 373:20 374:11 backdoor 166:1 166:9 187:9,16 300:12 314:20 backdoors 111:18 112:17 backed 270:22 backend 300:4 359:4 372:4 background 36:5 106:22 135:6 backwards 60:1 bad 18:8,15 20:18 24:15 46:22 161:6 174:18 188:10 201:19 263:4 275:1 301:18 310:21 315:4 360:15 bag 307:9 bailiwick 86:10 106:15 balance 8:17 19:20 22:22 33:5 52:4 53:1 53:7,11,13 64:5 73:6,9,10 73:10,12 133:8 133:12 134:1,4 134:6 167:20 169:20 170:3 176:14 178:18 260:4,6 302:21
---	---	--	--	--

319:16 337:4 337:12 345:8 345:12 383:19 balanced 19:18 130:7 balancing 19:15 25:2 52:14 53:22 64:12,14 64:22 65:16,18 65:21 66:13 67:16 68:15 72:9 204:4 291:9 ballot 27:17 ballroom 4:6 baltimore 385:5 ban 123:12 180:12 banning 121:15 bar 29:16 base 167:15 based 9:7 17:18 18:13 44:10 48:19 53:17 65:13 81:21 125:20 147:5 156:11 164:4 176:5 206:15 230:7 237:4 252:3 363:12 366:5 baseline 81:8 218:12 basement 306:16 basic 61:8 136:18 205:22 234:22 256:18 257:14 283:4 342:15,16 basically 72:9 104:22 121:17 138:18 166:11 200:6 273:16	basis 54:6 184:20 209:16 233:13 235:1 240:17 274:18 299:3 307:19 317:8 364:6 bates 373:15 377:11 battle 243:6 bay 113:18 beach 300:11 beaker 347:10 bear 239:8 244:16 314:8 bearing 378:10 bears 89:4 becky 225:11 237:22 249:21 260:2 261:15 262:8 268:9 276:7 282:15 354:19 beckys 255:16 becoming 13:16 138:21,22 139:3 147:18 148:9 170:8 182:15,17 bedoya 3:4 117:3,9 146:22 147:14 162:15 162:20 167:5 178:9,19 183:19 187:20 192:20 196:18 197:8 200:20 201:2 beginning 171:22 205:11 233:21 273:11 274:17 275:14 337:3 begins 60:17 behalf 65:21	behave 37:21 95:20 behavior 16:7 16:10 34:20 35:1,3 68:7,8 68:19 69:3 85:6 280:13 behavioral 36:2 behemoths 44:1 belief 125:4 beliefs 153:4 believe 17:6 32:8 65:22 113:12 115:15 127:13 130:1 131:4 137:17 150:20 151:2 164:2 179:14 184:14 187:1 230:22 235:5 254:11 313:18 317:1 330:9 345:12 368:20 372:20,21 believes 42:6 296:8 297:13 beltway 197:4 benchmark 119:7 bend 256:17 beneficial 274:16 381:18 benefit 50:22 123:5 202:12 286:2 310:18 318:13 330:21 336:14 benefits 50:13 50:21 52:2,5 52:14,18,21 106:22 107:2,3 112:21 277:12 291:16 331:17 benign 152:10	best 12:10,11 38:6 63:15 88:3 105:8 112:12,22 148:2 177:20 197:22 213:7 213:10 251:17 258:16 296:5 309:10 343:8 344:3 373:20 380:18 beta 252:12 beth 88:8 203:8 219:22 278:11 better 25:2 31:10 50:3 53:1 112:14 129:21 143:15 146:6,14 166:5 182:15 187:9 189:11,17,19 191:12 195:19 204:15 208:15 235:3 237:7 258:12,15 264:3 267:5,6 292:16 358:14 373:22 beyond 21:14 39:22 61:20 74:22 82:1 312:8,19 335:9 366:4 367:13 bias 313:1 biases 315:14 bieber 368:3 big 35:4 44:1,22 49:16 50:14 52:2,8,14,21 77:18,20 93:16 114:22 186:5 190:11 228:20 233:22 234:20 237:8 257:4	269:7 288:6 289:13 297:9 317:1,3 319:22 321:22 374:3 bigger 257:5 biggest 92:8 121:8 241:15 267:22 bilaterally 153:14 bill 8:12 billion 141:9 binary 198:19 bind 323:18 324:2 326:2 binding 330:15 331:6 biographies 286:22 biological 227:12 biometry 170:14 bios 10:3 bit 45:6,14 53:21 54:19 57:18 92:18 159:3 162:19 165:19 179:20 190:21 204:7 205:20 213:4 217:9 218:18 233:16,18 246:10 248:10 252:2 262:15 271:7 277:4 288:8 305:14 347:5,14 bits 268:14 black 307:12 blank 334:12 blend 196:6 234:17 blending 233:16 blind 194:3
---	---	---	--	---

361:20	73:3 74:7	331:18 333:11	broadening	135:3 138:16
blinking 22:14	boil 232:8	335:22 338:10	253:7	140:4 155:8
block 183:12	boiled 347:12	340:7 341:16	broader 33:6	157:20 158:3
blocks 235:10	bolton 346:7	344:10 347:16	231:2,12	232:16 235:10
236:14	bolts 96:1	363:2 372:8	289:17	236:14 237:4
blurring 108:5	book 93:16	381:6 383:1	broadly 19:9	239:5 251:21
board 1:3 2:1	288:7 306:20	breach 62:6	45:17 240:21	305:1 312:1
4:12,13 6:10	books 93:13	169:19	broke 16:17	347:22 357:5,8
6:10,11 9:18	boost 302:1	breached 300:7	brought 57:15	builds 134:16
10:12 11:13	border 132:18	breaches 38:3	238:13 341:17	304:4
25:11,14 26:14	290:5	breadth 245:9	brown 3:13	built 105:14
27:15 28:3	boss 23:5 193:15	251:9 278:21	215:10,17	126:9,11
32:5,15 41:2	bottom 50:4	break 7:4 109:2	216:7 239:17	136:17 157:18
51:12 56:9,13	273:16 326:1	187:14 195:3	245:22 263:11	201:16 214:12
74:12 85:20	bound 57:16	284:18 346:10	267:13 277:16	214:13 230:6
96:14 98:15	313:9 324:9	brennan 2:13	281:9	242:8 362:12
101:6 110:4	345:18	10:7	brute 61:21	bulk 15:15
116:10 120:21	bounds 22:8	brief 7:2 18:6	89:21 90:3	90:17 114:13
128:15 140:12	42:8	31:12 50:9	195:5	128:7,9,12
141:17,19	box 192:12,19	76:2 79:6	bubbles 245:2	180:2,5,12,18
159:15 163:12	277:2,5 320:17	102:7 165:17	bubbling 263:3	180:21 200:21
163:21 176:3,4	boxes 232:21	175:21	build 35:21	201:3 383:15
181:9 185:7,7	bradfordfran...	briefings 193:12	37:22 41:4,11	bullet 172:7
192:1 207:2,8	7:14	253:20 374:12	56:7 61:2 85:8	332:9 370:8
207:10,17	brakes 40:8	briefly 10:5 53:4	112:3 125:14	burden 322:18
209:20 213:18	branch 2:14	87:8 92:17	127:12 135:11	323:4 330:2
213:19 216:8	25:5 212:22	200:7 299:15	135:17 138:11	burdens 324:6
236:20 252:16	223:4 227:9	305:18	138:18 140:14	burdensome
282:15 286:10	246:20	briefs 375:3	142:1 155:1,7	74:20
287:16 295:21	branches 73:20	379:7	155:11,12	bureau 240:9
303:20 304:1	315:2 360:16	bring 88:10	156:2,7,11	bureaucracy
357:3 367:17	brand 2:4 4:14	110:9 216:18	158:10 170:22	351:21,22
383:21,22	80:14,15 81:22	231:1 239:8	174:20,22	352:1 365:9
boarding	82:21 83:3	244:13,14,16	199:17 202:7	bureaucrat
294:18	87:6 159:18,19	314:8 318:2	236:17,22	22:11
boards 4:4 5:18	161:18 162:15	327:7 378:6	247:10 271:2	bureaucratic
7:13 32:20	164:14 165:13	bringing 165:11	307:18 311:19	353:22
203:5 207:11	192:3 271:5	376:17,17	346:7 348:3	burgeoning
207:18 287:4	272:10 275:20	brings 50:20,21	349:4 356:4	78:18
349:13	276:12 285:7,9	broad 12:2	357:13	burglars 194:21
bodes 88:16	295:13 303:8	61:16 152:7	buildable 135:4	195:2
bodies 32:21	313:3 318:7	240:22 251:9	140:21 158:5	buried 27:7
72:5 94:11	322:13 323:21	262:18 299:22	171:4	burn 307:9
body 33:2 49:1	326:7 328:2	324:15 383:11	building 86:12	business 11:14

108:13 125:17 126:10 127:2 264:22 265:17 265:22 266:4 266:14 businesses 265:3 button 201:22 349:5 buy 24:7 25:1 buyin 23:20,21 buying 348:16	cant 17:6 22:22 23:6,16 32:1 32:10 48:20 53:8 59:19 64:4 65:9 70:20 71:4 76:10 77:16 79:15 84:16 86:22 94:8 107:14 116:1 145:4 162:18 163:3 174:17 188:21 198:20 241:17 261:22 262:1 271:10 271:18 272:4,8 278:18 288:19 311:4 326:20 330:9 331:9 349:2,4 367:11 capabilities 170:6 171:7 191:20 309:5 309:15 348:15 357:5 capability 279:14 345:1 capabilities 234:10 capacity 41:5,12 206:10 215:12 capital 3:20 313:5 car 26:2 106:3 321:8 card 6:15 9:12 9:12 17:21 37:5 59:22 66:14 67:10 110:1,2 206:7 286:5,6,17 293:17 354:4 cards 6:15 110:7 229:11 255:3	286:4,17 287:10 318:9 care 8:15 15:20 15:22 17:8 138:15 149:20 150:1 197:1,4 197:5 198:20 199:7 247:1 355:3 356:20 career 247:20 careful 207:19 210:12 248:10 294:1 carefully 88:1 140:11 cares 292:19 carnegie 251:8 carried 136:15 carry 137:10 214:19 259:2 265:6 carrying 383:18 cars 106:1 case 65:9 67:4 76:8 81:17 86:11 95:21 133:14 166:7 168:11 184:14 218:16 259:19 264:7 270:15 281:4 291:22 295:5 326:21 331:10 cases 48:12 53:15 71:19 83:7,12 113:20 114:7 153:10 160:14,22 162:10 171:3 191:4 265:9 270:9 376:10 377:7,14 cast 52:4 123:16 castles 300:10	cat 8:5 catagorization 236:6 catagorize 235:14,16 236:4 catagorizing 268:10 catalogue 27:9 catch 173:15 175:6 311:22 catches 311:21 catching 190:6 cate 3:18 286:21 287:2,6,8 296:14 326:9 328:2,16 335:22 336:2 341:17 350:19 351:12 354:18 355:8 374:4,5 375:17 381:9 381:12 categories 152:2 306:2 cates 305:22 cato 66:16 cats 368:3 caught 310:20 cause 20:15,20 29:17 46:14,15 46:22 47:1 53:17 65:3,14 73:1 81:21 104:18 169:5 362:3 caused 50:6 104:15 causes 16:6 20:19 47:17 237:3 359:13 causing 17:3 cdt 297:13 299:11 303:1	375:3 cell 194:12 cellphones 329:15 census 122:9,15 123:10,11 center 2:13 3:4 3:19 33:13 40:3 62:2 117:4 132:13 156:3 232:5 295:16 296:7 centers 10:7 130:18,21 186:1 188:4 centralized 127:1 centric 234:3 century 337:17 ceo 357:12,14 certain 13:7 16:15 37:5,6 42:1 46:14 52:12 63:4 68:9,9 71:5 73:17 76:15 83:12 84:4 85:18 102:21 103:15 106:6 159:5 160:14 165:8 173:3 174:3 184:13 190:2 220:10 224:4 235:21 268:10 279:7 380:22 certainly 17:9 17:15 43:2 45:2,4 58:5 59:9 60:7 64:3 70:21 84:17 94:14 98:16 108:14 146:13 149:5,15,17
--	--	--	--	--

153:19 154:9	challenges 26:1	cheaper 138:13	77:22	229:14 231:1,3
157:15 158:7	226:19 241:16	148:10 169:13	chosen 13:9	231:12,14,18
168:3,12	279:12,17,22	185:16,17	chris 3:20 313:4	231:22 232:4
178:19 179:16	327:19 378:20	check 59:5	348:1 351:6,15	232:17,19
180:22 184:7	challenging	277:2,5 325:3	358:1,13	233:4,10 234:5
188:2 192:20	204:6 226:17	checked 277:14	360:11 364:1	234:16 237:6,7
197:11 198:5	championed	checking 192:12	church 73:22	237:12 238:10
224:7 230:12	50:16	192:19 232:21	210:9	238:12 240:3
243:17,22	chance 13:12,13	checkpoints	circling 262:14	242:15,21
254:20 276:2	333:16	126:13 172:22	circulate 9:22	243:8,19
282:5 288:15	change 16:7	173:3	circumstance	244:10,13,18
289:9 293:15	123:9 137:20	checks 173:10	12:5	275:7 280:22
296:13,15	145:18,21	175:2 320:17	circumstances	282:21 284:13
304:21 317:20	146:1 193:1	chemical 227:12	13:6 64:20	289:19 295:17
333:7 341:5	280:13 288:6	chertoff 25:6	80:1 84:17	295:21 296:2
355:17 356:14	315:21,22	cheshire 8:5	99:14 101:8	303:9 304:18
377:13	322:11 341:8	chew 383:16	circumvent	305:5 310:21
certainty 159:13	341:11 361:3	chicago 183:9	175:5	317:10,12
certification	381:1,1	183:10	cited 375:3	334:1 349:13
376:6 385:1	changed 16:10	chief 3:7 117:6	citizen 140:10	351:18 353:8
certify 385:6,9	17:15 70:13	124:11 133:13	201:21 337:18	356:21 357:6
chain 189:3	137:5,6,8	134:15 215:10	337:20	358:21 372:17
266:11 308:15	149:15 190:4,5	223:17 240:4	citizenry 314:8	383:19
349:6,7	227:22 228:1	childhood 13:8	337:6	civilizations
chair 74:13	228:10 229:5	13:13	citizens 132:9	8:11
108:17 110:13	334:5 341:11	children 303:22	133:10 167:17	claims 9:7
chairman 2:3	changes 137:13	childrens 341:5	302:20	clarify 180:17
4:11 25:10	147:8,11 215:3	chill 21:3,4,5	citizenship	clash 20:22
27:10 101:21	226:14 278:1	chilling 21:9	230:21 232:5	class 136:3
109:8 165:14	364:7	79:2	civial 215:14	classic 329:4
201:8 383:2	changing 33:19	china 170:18	civil 1:3 4:3	classified
challenge 253:2	110:21 277:18	chinese 189:13	111:4 116:9	253:19 353:4
challenge 83:16	348:20	choice 23:13,16	135:15 203:5	356:8
84:21 92:9	channels 223:16	23:17,18 66:1	205:10 206:5	clause 64:14
200:18 221:6	228:15 280:12	66:2,3,4 78:2	206:11 207:16	clear 90:20
222:10 241:20	chaplains	126:3 255:9	209:2,13,19	123:8,15 128:8
241:22 264:20	122:21	256:22 289:11	211:3 215:11	131:12 133:16
265:11 267:22	chapter 288:7	299:9 307:21	215:18,20	149:22 158:9
328:19,21	characteristics	choices 106:10	216:1 217:16	158:10 191:5
335:18 353:9	46:10	199:4 270:3	222:21 223:17	202:2 230:11
374:18 379:9	characterize	choose 297:2	223:19 225:12	295:2 331:15
380:1	209:8	299:5 319:7	225:16,18	337:21 370:9
challenged	charged 360:21	326:20	226:6,9 227:2	375:10 378:8
132:11 329:11	chatty 139:4	chooses 77:22	227:18 229:4	381:12 382:19

clearance 193:9 201:7 355:2	cold 10:10 228:2	200:2 208:15	296:17,20	287:9
clearances 193:6	collaboratively 246:21	281:18 283:9	297:7,14,15,21	com 93:13
cleared 85:21	colleagues 148:20 216:21	301:14 339:15	299:1,7,8,11	comb 322:2
253:3,13,16	collect 9:22 34:2	350:16 353:18	299:21 300:8	combat 313:21
254:2,9,11,14	40:15 61:22	collection 15:15	300:15,22	combination 268:15
254:18,21	62:4,11,20	15:15 20:13,17	301:7,8,16	combinations 268:20 269:1
clearer 146:14	63:4 70:2	30:20,22 34:5	302:18 303:6	combinatorial 138:3
291:3	79:22 87:7	36:11 37:18	305:21 317:2,4	combine 36:15
clearing 254:5	106:9 118:1,14	38:13,17,19,20	323:2 324:11	47:7 75:13
clearly 80:10	118:15 120:9	38:22 39:2	325:5 327:15	76:12 335:1
119:15 163:2	121:14 178:21	40:19 46:4	333:9 338:3	combined 41:8
219:2 223:12	179:1,3,10	56:2 61:15	350:11,12,17	217:22
249:9 331:16	277:19 292:22	63:10 66:9	350:21,22	combing 14:16
332:17 336:7	293:4 298:3	69:8 77:14,17	351:3,8 359:17	combining 76:13
375:6	324:1 342:2	77:20 78:13,22	360:3,6 361:14	come 16:22
clie 136:9	352:22 353:1	82:6 84:7,16	371:9 372:6,10	29:11 57:15,17
client 29:5,8	359:21 360:7	87:12 89:12,22	372:20 383:12	77:6 104:12
354:10	382:12,14	90:4,9,11	collections 180:2	124:18 132:16
clients 267:18	collected 5:11	92:21 102:13	collectively 11:4	134:12 140:20
268:2	15:12 19:8	102:14,15	collectors 237:1	142:9 180:9,11
close 13:8	21:15 37:11	104:17 108:4,4	collects 15:21	180:14 216:12
140:22 141:14	63:7 79:18	108:7 118:7,20	16:3 298:11	217:16 228:7
closely 88:4	84:3 90:14	118:21 120:4	300:8 317:19	229:5 257:14
133:2 207:11	99:19,19 118:9	120:20 124:4,7	college 137:2	259:21 271:22
closer 323:22	121:16 123:3	126:3 128:7,10	157:9,10	272:21 289:10
closing 115:14	126:2 127:16	128:12 136:6	collins 2:7 4:14	305:6 319:11
cloud 125:8	152:8 163:16	147:19 169:12	88:14 92:8	322:19 324:7
136:22 151:11	164:5 169:11	169:12,21	171:10 173:17	325:21 347:3
151:14,17	202:16 204:17	178:4,4,10,14	175:8,18 196:8	367:21 372:18
188:19	221:19,20	178:14,14,17	203:9 206:9	373:5,12,18
code 187:5,10	229:22 230:20	179:7 180:5,12	207:3 215:9	comes 10:11
coded 32:6	232:11 266:13	185:18 200:21	225:8 237:20	12:9 21:9 25:2
coding 234:13	278:20 282:20	201:3 228:3	239:10 241:4	40:13 53:6
codirector 10:7	306:9 324:5	230:5 232:7	241:14 245:7	63:13 123:19
coerce 104:1	330:11 358:2,5	256:1,3,5,6	247:11 249:21	133:14 149:11
coercive 44:7	366:20 371:6	257:21 258:4,6	252:14 255:1	221:2 223:15
58:22	collecting 36:7	258:21 260:14	255:10 262:5,7	223:16 245:3
coffee 77:3	36:20 39:4,10	260:19 262:18	263:9 271:4	249:16 296:6
coffin 150:12	40:1 55:17	262:20 271:14	278:2,13	297:20 323:20
cogent 41:19,20	62:12 75:15	272:6,16	280:20 282:14	334:9 345:17
cognizable 98:14	77:19 118:13	278:22 279:4	284:14 363:3	
	142:5 165:7	279:20 280:5,9	366:8 370:10	
		283:7 292:12	colorblind	
		292:13 293:8		

358:9 361:4	commission	communities	140:5	239:13,20
comfort 253:9	85:13 216:12	121:12 123:20	compartmented	240:7 241:2
comfortable	216:15 385:18	community	253:17	242:21 246:9
24:16,19	commissions	214:12 242:18	compatibility	246:12 316:14
comforted	287:5	community 30:4	222:17	324:21 335:13
177:22	commitment	42:6 90:18	compel 375:9	342:13 343:7
coming 17:21	116:10 125:6	92:2 118:11	compelled 99:15	345:22 346:1,2
88:12 171:6	131:1	146:7 195:4	99:16	compliant 146:3
216:6 243:16	commitments	207:14,15	compensate	complicated
273:2 339:19	126:6	208:8 213:1	100:16 327:13	37:16 63:14
341:1 358:12	committed	214:19 215:5	competing 8:17	171:20 378:2
commencing	282:7	226:9,10,13	9:2	complies 177:14
1:14	committee	242:11 244:2	competition	comply 38:19
commend	30:11 73:22	245:1 254:4	67:12	145:10 178:2
271:13	119:12 163:1	258:3 266:15	competitors	240:14 319:15
comment 50:9	179:17 193:22	266:20 276:11	130:22	342:4
185:14	210:9 303:12	310:22 376:1	compiled 148:8	complying
commentators	committees	companies 24:2	complain 54:4	177:10
8:9	85:13 179:14	44:6,8,21,22	complete 86:2	compoments
commented	194:2 210:7	45:2 83:7	249:13 384:1	224:15
194:8,19	212:20 253:16	90:15 91:3,5	completely	component
comments 5:17	253:21 254:6,9	104:1,4 112:4	31:13 86:6	22:20 48:16
7:9 67:18 76:2	254:16	112:17 127:20	165:1 174:17	76:4 83:20
128:17 134:10	common 18:8	129:9 131:3,6	330:7 337:9	215:20 224:8,8
183:18 186:13	30:3,6 46:9,10	140:1 149:10	350:20	224:9,10
225:7 263:14	115:4 224:15	188:15 298:14	complex 38:9,11	239:21 246:11
313:15 317:15	commonality	298:21 341:22	74:19 94:12	346:12
331:20 383:22	96:12,18	343:14	143:1 171:8	components
384:2,4,5	commonly	company 91:19	308:19 368:5	215:20 224:9
commerce	292:19 293:10	102:21,22	378:20	224:16 246:8
247:22	commonsense	103:2,16	complexity	346:13
commercial	14:21	126:18 134:16	37:19 38:4	comprehensive
39:7,8 43:12	communicating	136:5,12	233:22 245:12	10:18 127:5
75:7,9 108:3	153:1	156:15 172:18	373:17	186:12
111:19 119:4	communication	250:15 304:17	compliance 38:3	comprehensiv...
216:16 230:17	189:3 228:14	338:22 350:15	38:5,8,11 95:2	31:2
299:6 304:3	339:11 361:18	356:14 367:2	95:3,16 127:10	compromise
343:6,6 350:14	communicatio...	comparatively	143:2 146:11	14:10
commercializ...	29:6 43:16	58:18,21	169:15 172:14	compromised
104:10	103:14 128:14	compare 264:9	176:20 177:4	15:8
commercially	166:3 227:7	compared 58:21	192:16 206:19	computer 33:12
39:17	228:12,16,18	comparison	216:4 226:2	33:19 61:11
commerical	249:2 363:16	11:17 67:1	230:6,7,11	74:21 110:15
228:17	370:22	compartment...	238:4,8,18	134:17,18

174:10 237:13 295:18 313:10 computers 22:14 269:17 computing 110:13 234:11 comstat 185:1 conceivable 256:14 concentrate 45:20 200:10 concept 8:6,13 12:2,11,11,14 13:3 14:21 17:5 49:22 76:20 80:19,22 82:9 97:19 120:22 121:4 138:19 144:15 147:5 155:10 196:10 235:11 366:3 conception 18:13,14 72:2 340:5 conceptions 25:19 48:1 concepts 61:17 92:9 171:15 conceptualizing 45:13 concern 61:18 127:15 132:3 135:3 147:7 188:14 258:12 concerned 45:8 56:13 149:9 188:7,9,11 concerns 107:5 127:18 171:15 205:10 230:12 230:13 374:9 concluded 45:19 181:18	concludes 202:21,22 conclusion 224:1 conclusions 280:10 288:1 347:3 361:5 concrete 92:13 170:9 312:7 concretely 93:4 163:6 concur 293:15 concurrences 76:7 conditioned 364:15 conditions 9:6 362:14 conduct 31:15 73:6 148:10 179:15 194:4 197:3,12 198:17 211:12 233:4 241:17 363:14 conducted 70:11 193:12 210:2 228:13 230:3 236:19 265:12 332:6 conducting 167:1 251:3 321:18 342:21 conducts 218:19 223:4 225:17 227:22 conference 154:3 conferences 247:9 confessional 27:19 confidence 57:2 57:5 130:5	193:7 confidences 13:18 confidential 122:12 confidentiality 29:5 122:14 confidentially 123:3 configure 308:4 configuring 112:5 confinement 59:6 conflict 67:15 confluence 108:15 confusing 96:16 conglomerate 8:14 congratulations 296:4 congress 11:13 12:7 32:22 65:20,21 73:22 74:4 85:16 95:4 122:14 123:12 128:19 130:14 210:4 212:6 230:15 253:5,6,11 254:1,14,16 352:14 378:17 congressional 179:14 210:7 212:20 252:18 253:2 303:18 321:3 connect 39:13 connected 138:21,22 169:14 371:15 371:19 connecting 49:3	conscious 357:6 consent 79:11 79:12 80:11 81:3,18 98:7,8 152:16 221:8 288:20 312:14 328:6,11 329:5 331:11 332:13 consenting 103:7 328:9 332:19 consents 289:1 consequence 55:9 56:3 60:8 consequences 20:11 36:7 60:19 62:4 281:1 334:7 consequential 54:2 consider 5:22 113:16 114:9 177:16 227:18 240:9 247:5 284:1 344:22 383:17 consideration 114:21 143:13 154:19 176:22 205:11 250:6 253:7 296:15 considerations 111:7 199:21 231:16 285:6 303:4 345:4 379:2 considered 115:7 considering 231:22 245:9 considers 230:4 364:13 consistent 209:3 247:6 299:20	consistently 230:3 consistently 95:20 123:18 consists 8:19 constantly 54:21 constituents 153:22 constitues 235:4 constituted 323:2 constitutes 319:18 constitution 42:1 131:4 244:5 313:19 314:13 constitutional 42:9 98:13 129:12 147:4 337:3 377:8 constitutional... 97:21 constrained 314:9 334:17 375:20 constraint 325:3 constraints 324:6 325:16 345:17,17,19 constructs 324:17 consult 176:11 176:18 consulted 242:4 consulting 2:14 25:5 242:15 consumer 366:6 consumers 125:9 298:22 consumes 208:1 contain 34:16 34:22 35:2 contained 385:6
---	---	--	--	---

contains 371:14	131:12 134:7	340:18 342:1	247:11 249:21	115:11 133:15
contemplated	181:10 188:16	342:18 349:20	252:14 255:1	141:9 217:16
149:18	198:21 203:6	controlling 13:3	255:10 262:5,7	310:18
content 132:13	211:14 234:3	13:4 86:5	263:9 271:4	costs 68:13,21
151:22 152:19	255:15 280:15	142:15 143:20	278:2,13	342:20
153:2 168:6	294:12 355:22	controls 12:20	280:20 282:14	couldnt 81:6,17
188:22 230:19	364:10	38:13 71:13	284:14 363:2,3	104:7 201:1
343:18	continued	93:2 94:8	366:8 370:10	counsel 96:4
contents 36:10	130:10	199:2 209:17	cooks 88:8	117:6 124:12
290:9	continuous	298:17 306:4	cooperation	209:11 238:16
context 3:2 6:1,8	345:22 346:2	307:18 308:2,5	104:20	239:12 243:15
14:6,7 60:6	continuously	310:14 348:2,4	coordination	243:16 244:7
75:17 81:1,12	346:8	348:9,10	91:5	295:15 385:10
82:13 83:11	contract 102:22	353:21,22	copied 290:9	counsels 238:3,7
84:13 85:2	103:1,5 198:10	376:3	copies 361:20,20	240:1
88:21 93:10,20	contractors	controversial	core 29:2 118:22	count 279:14,16
93:22 94:2	104:8	65:6	120:22 124:9	279:20
95:9,10 109:12	contractual	controversy	125:4 234:19	countermeasu...
114:20 119:15	103:12	332:13	304:11	69:3
132:11 133:21	contrary 151:5	convenient	corner 183:22	counterterrorism
135:13 144:18	224:3	113:3	183:22 184:1,3	205:3
160:4,20	contrast 31:3	converged	184:4	counterterror...
161:15,22	35:22 59:8	335:20	corporate 79:9	6:1,8 109:12
162:14,17	113:12	conversation	79:17 108:13	111:4,14
163:11,21	contribute	135:6 262:13	144:15	114:16 119:9
164:7 168:4	41:21 234:4	277:13 282:13	corporation	144:19 162:14
169:1,10	contributes	362:1 365:5	107:1,4	165:20 166:4
181:21 192:7	362:18	370:3	correct 48:14	204:2,13,14
195:2 204:3	control 5:10	conversations	87:1 181:5	205:7 208:5
205:3 208:3,4	12:13,22 14:1	166:11 274:6	272:9	213:21 216:19
217:3 218:14	15:8 16:4,5	275:10 283:18	corrected	217:6,10
218:19 219:4	17:16,20 28:8	convey 34:19	194:13	218:14 219:18
221:7 276:21	28:8 31:15	36:9	correction 31:6	227:10 246:4
290:16 297:11	37:21 42:20,20	conviction 184:4	55:10 56:7	323:11 325:15
305:19 327:1,3	64:1,7 67:22	convinced 11:12	57:6,13	countertrroris...
327:11 328:15	68:2 69:7,20	cook 2:7 4:14	corrections	3:2
332:18 340:20	71:5,7,9,11	88:13,14 92:8	374:13	country 10:22
350:15	78:10 80:17,20	171:10 173:17	correctly 45:20	44:12,22 187:5
contexts 32:18	83:21 87:1,16	175:8,18 196:8	73:11 166:20	187:18 284:11
134:2 160:5	106:5 121:2	203:8,9 206:9	199:11	301:17
304:9 309:13	156:3,4 233:8	207:3 215:9	correctness 87:3	countrys 110:15
continually	293:11 302:15	225:8 237:20	correspond	counts 361:12
24:20 134:3	307:17 308:11	239:10 241:4	34:15	county 385:5
continue 124:8	340:11,12,13	241:14 245:7	cost 50:22 115:9	couple 102:2

138:8,9 175:20	373:7,12 374:2	209:18	critize 273:4	342:12 367:20
199:12 224:2	374:13,17	creates 49:11	cross 132:18	cuts 147:15
237:19 249:22	375:6,20 376:1	50:17 175:7	351:1	cyber 111:15,22
273:12 309:18	376:4,10,19,19	305:1 353:12	crossed 172:21	133:3 313:11
319:6 340:22	376:21 377:3	creating 72:17	crucial 114:22	cyberattacks
361:12 381:6	378:5,14,17	135:4 140:17	372:7 375:18	227:13
course 5:15	379:5,14 380:4	158:3 183:20	crumple 40:9	cybersecurities
51:15,19 76:18	380:11,18	244:10 276:18	crumpling	349:22
90:14 99:8	courtappointed	303:19 313:1	307:10	cybersecurity
110:8 119:14	374:22	creation 206:20	cryptographer	295:19 343:11
136:14 150:17	courtesy 361:20	360:17 369:3	134:18	346:5 378:18
173:13 207:22	361:20	credit 336:12,13	cryptography	cycle 126:13
209:18 210:4	courts 8:20	creep 366:4	40:15 91:17	
214:14 216:14	11:13,17 65:18	crime 133:3	138:2	D
217:12 218:13	66:18 97:6	183:21 184:1	crystallize 202:5	d 1:14 4:8
219:9 222:10	130:11 132:12	184:17,17,18	crystallizing	110:14 124:22
222:16 223:16	133:15 364:17	184:20 295:18	148:14	145:19 169:3
239:19 249:4	368:17 372:13	371:15	cues 297:19	248:1 284:6
253:17 257:8	372:16 374:6	crimes 183:16	culture 95:1	daily 34:6
258:8,20	375:2,8,17	183:16 184:3	172:1 215:3	374:14
260:11,15	cover 172:13	criminal 53:17	251:19	dam 351:2
264:15 266:4	224:13	65:3 182:12	current 44:19	damage 115:8
267:8 281:15	covered 14:13	183:5,13 217:3	58:14 101:7	damaged 128:6
293:18,19	105:15 349:10	221:9 222:10	189:16 217:13	damages 222:22
299:5 304:12	383:11	222:22 372:14	231:1 369:14	damaging 161:1
309:9 347:6,6	covers 97:2	criminals	currently 70:5	dan 2:15 28:4
347:14 367:6,8	101:20	110:22 111:17	190:1 212:2	31:22 50:12
375:8	cpo 177:8	113:1 182:9	283:8 313:4	65:22 71:2
courses 311:17	cracking 187:10	critical 11:1	customary 51:9	98:2,17 103:21
court 12:1,4	craft 87:21	31:16 55:10	customer 125:7	dangerous
14:12,16,18	187:17	89:11 111:14	125:19 127:7	184:5 210:20
54:5 65:5,8,13	cramped 19:11	113:7,21	132:12 150:5	daniel 18:2
71:17 72:1	crazy 354:16	114:15 116:12	172:18 188:6	dans 77:9
74:22 76:8	create 34:18	119:7 125:7	188:14 265:19	dark 185:11
129:8 130:4	47:11 75:13	132:22 187:6	265:21,22	189:21,22
147:16 150:14	76:15 104:19	207:15 224:22	266:9,11,14	darlings 136:13
151:12 196:13	105:3 117:21	232:19 281:5	352:18 353:2	data 18:19,20,21
212:11,21	126:8 132:16	293:11,14,19	customers 125:5	19:1,2,3,4
221:14 245:18	140:5 158:17	300:6 351:9	125:9,15	20:13,17,20
292:9,14	212:9 258:9	352:15 378:13	127:13 131:21	21:14,16 24:3
301:21 314:22	284:4 349:22	379:4	149:8,22 150:7	33:20,22 34:2
325:18,19	353:3 356:22	critically 207:20	150:21 167:21	34:2,3,14,14
358:18,22	created 151:15	criticized 112:9	168:1,2 188:3	35:5,12,15
365:11 369:9	152:8 209:12	183:11,17	188:7 265:4,5	36:2,7,15,22

36:22 37:14	162:4 164:6,10	305:22 306:3,8	61:2,6 75:4,8,9	deanomoized
38:3 39:7,20	164:10 165:8	307:15,18,19	77:17 79:9	269:16
40:2,2,18,19	168:8,11,15	307:19 308:6,7	102:11 161:3,5	dear 226:21
40:20 43:17	169:7 178:21	308:7,11,12,15	datacentric	death 288:7
46:3 47:3,5,9,9	179:7,11 180:2	308:22 310:4,7	232:9	310:17
49:1,4,10,10	180:8,12,19,21	310:14,14,16	datadriven	debate 96:14
49:13,15 50:15	181:16,21	311:5 312:20	182:22	129:3 180:19
50:16,17 52:2	182:5,16 183:1	317:1,3,5	datafied 312:17	226:11 256:4
52:8,14 55:17	185:18,22	319:22 320:4,6	datas 52:21	290:14 310:18
61:22 62:2,3	186:1,5,5	321:22,22	date 37:6 237:16	334:14 337:4
62:10,13,13,14	187:2 188:4,8	322:5,7,8,8,9	dave 250:19	376:17 378:21
62:21 63:4,7	188:9,12,18	322:10,11,12	david 2:3 10:18	debated 154:5
63:10 68:12	189:3 190:14	323:2,3,3,6,7,9	263:9 285:9	212:2
70:19 76:12,14	190:19,20	323:12,13,16	day 88:17 97:21	debates 59:14
77:2,15,20	200:22 201:3	323:19 324:2,3	101:22 133:1	115:5 131:16
79:13 82:6	228:20 229:21	324:5,10,14,19	150:6 271:7	debating 113:5
87:1,3 90:14	230:19 232:8	325:4,17,22	285:2,12 289:4	decade 242:7
91:6,11 94:4	232:11 233:22	326:3 327:14	290:21 303:21	decades 123:20
102:11 104:17	234:20 235:21	328:1 329:8,11	304:17 315:5	124:21 185:2
105:1,1,2,13	235:22 237:1,2	330:12,16,17	319:16 338:5	340:22 369:13
113:8,10 114:6	237:8 256:8,10	330:18 331:2	383:5,15	december
114:22 117:15	256:13 258:9	333:9 335:1,4	385:13	385:18
117:16,18,19	258:14,16,18	339:4,6 342:12	days 57:4	decentralized
118:7,8,21	259:1 262:17	342:12,22	170:16 248:15	228:9
119:1 120:21	262:17 269:7,8	343:11 348:22	312:17 384:7	decide 51:13
121:15,19,22	269:16 270:3	349:17 350:2	de 53:6	100:14 187:13
122:1,11,16	272:12 275:4,4	350:16 352:22	dead 224:4	269:20 376:22
123:3,11,19	277:20,20	353:19 359:16	deal 93:17	decided 8:21
124:1,6 125:12	282:19 289:13	360:3,6 362:13	100:13 105:15	78:19 273:1
126:1,2,3,4	289:14,15	362:15 366:13	133:22 135:15	decision 74:17
127:8,14,15,19	290:16 291:10	366:16 367:3	155:15,15	133:15 145:22
128:7,10,12	292:2,7,9,22	367:18,19	169:1 191:1,4	221:13 245:3
129:17 130:6	293:4,9,10	368:10,10,10	191:9,18 239:7	257:13,14
130:18,21	294:13 296:16	368:14 370:13	270:8 306:2	261:17 379:21
131:2 132:5,13	296:20 297:6,7	371:5,7,8,10	325:16 343:14	382:4
132:18 139:10	297:9,15,15,20	371:13,18	dealing 88:19	decisionmakers
139:16,18	298:3,11 299:7	372:3 381:21	137:9 150:5,6	253:12
140:6,6 141:10	299:8,11,21	382:12,14	155:19 171:20	decisionmaking
147:20 149:17	300:3,15,17,19	383:15	247:17 305:20	116:8 349:6
150:8 151:14	300:20,22	database 60:14	310:15 349:16	decisions 5:1
151:14,15,20	301:7,7,18	79:17 160:17	349:20 374:21	48:18 49:4,5,6
152:1,8,17	302:5,10 303:6	195:2,5 248:20	dealings 103:1	57:20 115:5
153:5 154:3	304:4,5,5	248:22 365:11	dealt 72:18	140:13 145:7
156:2 160:15	305:19,20,21	databases 59:17	177:7	151:12 242:13

252:5 309:22	339:19 368:12	27:16 33:4	3:13 25:8	342:15 351:21
340:19 348:21	definitions 5:13	66:6 253:13	100:5 122:5,6	deserve 42:6
350:2	11:9,11	295:16 296:7	122:15 123:16	deserves 14:22
declaration 51:6	definitive 100:3	democratic	183:10 209:15	362:10 365:2
declaring 51:14	287:11	54:13 55:3	213:1 215:11	deserving 43:6
declassification	degree 59:7	56:1,6 302:22	215:19 216:2	design 61:16
301:21	103:13 119:22	demonstrate	217:4,18 222:7	125:17 126:17
declassified	254:1 345:5	266:16	225:5 226:2	135:17 142:12
129:6 377:15	347:10	demonstrating	246:3,7 247:1	142:13 143:11
decrypt 112:6	degrees 8:16	284:11,12	290:4 303:13	143:17 144:8
dedicate 319:9	196:11	dempsey 2:6	313:11 364:15	144:15 146:15
dedicated	deidentification	4:14 96:7,8	departments	154:18,20,22
119:13 126:21	111:10 113:5	97:11 98:19	215:15,18	155:16,17,17
193:22	114:4,11,13	99:16,20 101:9	216:20 217:1	158:19 190:2
deemed 57:7	115:17 160:3,8	102:1 109:6,8	219:19	designed 209:21
deeper 172:14	175:16 194:7	117:2 124:10	departmentwi...	211:19 220:17
198:22 199:4	195:9,18 196:9	134:8,11	216:3 239:19	232:13 233:9
deeply 40:22	383:13	141:16 144:6	depend 269:6	365:22
95:22 247:2	deidentified	144:12 145:12	371:22 372:1	designs 134:16
default 112:4,13	194:10,12	145:15 146:12	dependent	desirability
115:16 166:14	196:16	146:17,21	237:9 297:1	214:8 294:7
185:20 187:4	deidentify	149:5 150:11	332:16 377:9	desirable 374:15
359:8	195:14	151:21 153:7	depending	desire 4:22
defend 244:5	delegated 85:15	154:11 158:8	288:12 360:5	254:20
defense 122:6	253:10	158:22 159:14	depends 58:10	desired 38:10
123:16	deleted 307:8	164:20 165:14	102:19 162:9	desk 306:14,15
define 7:22	358:6	181:8 183:7	359:18,19	despite 14:14
138:4 140:5	deletion 307:9	184:22 185:4	deploy 78:21	38:6 234:21
155:5 171:6	307:12	187:21 189:7	deployed 127:4	destroy 167:2
208:2 269:10	deliberately	192:1 201:8,11	183:10 304:14	destroyed 222:1
269:14	68:9	202:21 278:4	309:12	300:19
defined 45:17	delineated 53:16	347:17,19	deployments	destruction
45:18 219:2	65:12	350:6 351:5	304:8	118:8 365:17
223:12	delinked 196:12	354:2	depot 141:11	detached 374:17
defines 42:1	delivering	denial 112:14	depths 237:16	380:4
defining 1:5	265:18	denied 60:4	deputy 3:20	detail 175:12
2:10 4:4 5:21	demand 24:8	221:12	25:7 215:16	218:18 220:22
51:15 202:3	188:7,14	denominator	313:6	237:15
203:6 204:3	demanding 24:9	46:9	derive 320:12	detailed 34:22
definitely	demands 129:13	deny 59:17	derived 227:6	75:14 122:15
104:11	189:6	77:10,10	derives 26:22	129:12 130:1
definition 11:15	democracies	294:18	345:14	308:17 309:2
11:19 157:16	32:10	denying 336:13	describe 227:2	details 151:16
208:18 301:4	democracy 3:19	department	described	detain 298:11

detect 339:3	155:20 156:4,7	39:12,12 47:4	235:11 238:20	250:18 252:10
detection 208:16	156:20 185:21	48:3 63:18	269:3 287:17	295:15 313:6
deter 192:15	290:8	68:10 79:3	290:10 330:4	directories
determination	devices 39:16	89:17 94:10,11	368:17	194:15
258:22 300:20	136:2 137:9	96:17 97:2,3	difficulty	disagree 89:16
358:7 359:6,8	138:5,14,16,18	103:11 157:16	374:19	296:13
359:12 377:20	138:19 139:4,8	161:4,5 165:1	diffusion 186:11	disagreement
determinations	142:5 143:12	172:17 173:10	186:12	25:18 26:13
258:3	155:11 158:4	177:9 184:9	diginity 231:8	disappear
determine	185:16 188:5	202:13 212:15	digital 49:2	156:17
114:10 235:6	290:6 329:16	216:15 230:13	136:10 234:10	disappearing
235:15 236:3	devolve 277:14	232:10 235:16	diligent 14:15	140:8
276:3	dhs 205:17	235:19 236:4	207:18	discard 101:6
determined	250:13 271:16	236:12 238:6	diligently 246:8	discern 190:22
34:14 113:18	272:3 273:5,17	241:5 244:19	diminish 52:18	discharge 123:4
determining	276:2 282:9	244:20 248:13	147:9	disciplines
40:19	326:17	249:3,5 250:17	diminishing	237:10
deterrent 325:8	dhss 273:4	251:1,7 252:2	192:13 319:12	disclose 34:6
325:13	dialogue 154:6	259:19 260:14	diminishment	99:3 102:20
detrimental	313:14 365:8	262:11,13,15	52:19	129:12 266:5
161:6 166:3	dias 216:21	263:7 265:14	dinner 161:14	280:18
develop 39:3	didn't 13:14	273:8,12	diog 217:21	disclosed 79:11
114:18 126:18	81:18 136:21	277:20,20	220:4,8 221:17	209:22 222:19
148:6 173:2	147:1 167:10	297:22 298:9	221:18	discloses 150:16
235:6,10 236:6	185:10 201:6	304:20 309:13	direct 102:5,6	disclosing 34:8
236:8	243:22 271:2	314:7 315:22	115:9 280:21	91:18 142:6
developable	326:14 347:13	316:20 319:4	299:7 318:9,19	disclosure 5:7
92:6	352:11	319:19 323:15	326:10 378:10	13:19 81:19
developed	differ 93:20	323:15 327:21	directed 102:10	84:9 97:16,17
114:20 117:14	248:18,19	334:6 339:21	228:4 271:12	97:19,20 98:3
127:4 148:8	376:11	359:9,13	381:10	98:8,8,21 99:5
173:1 177:12	difference 43:19	373:12 381:2	direction 203:16	99:6 222:16,21
234:13	44:3,3,5,5	differentiating	328:21 331:22	disclosures 16:9
developing	52:19 73:16	299:2	369:11	16:11,14 57:10
54:17 91:22	199:12 327:22	differently 21:7	directives 243:1	120:6 163:14
92:10 153:14	differences	21:8,8 259:18	directly 30:17	222:11 278:21
154:8 234:8	264:13,16	differs 93:19	34:6 43:10	discontinue
263:19 276:9	299:14,19	difficult 36:8	206:12 227:14	32:6
development	different 6:10	37:20 38:12	276:1 300:15	discount 69:14
5:3 126:12	10:16,17 11:9	86:18 138:5	307:3	discourse 17:3
developments	11:21,22 12:3	143:2 162:2	director 3:11,20	discoverable
129:5	18:18 21:5	163:7 169:16	112:9 117:4	229:2
develops 225:19	27:8 28:16	169:22 170:1	206:6,12	disciplinary
device 136:15	32:18 33:15	214:10 233:21	225:15 226:1	281:21

discreditable 18:16	displayed 43:20	documented 331:16 354:1 382:4	266:5,17 267:7 268:4 271:1 274:11 277:7	120:15 123:1,2 132:21 137:17 143:3 144:9
discreet 89:6	disposition 222:3		277:10 279:22	148:22 149:20
discrepancies 269:9	dispute 58:6,7	documenting 233:7	282:10 283:8	152:4 155:4,21
discrete 335:1,4 346:1	disruption 46:14	documents 218:1,10 220:3	283:16,17,22	157:13,14
discrimination 123:7,21	disruptions 45:21	doesnt 13:9	284:12 294:7	158:10 160:20
discuss 9:5 10:1 36:6 63:11 105:11 205:2 237:15 280:15	disrupts 47:18	15:21,22 20:1 20:6 23:9 36:9 42:21 46:21 50:2 52:7 59:4	297:6 319:13 321:18 322:4 326:2 330:3 331:15 332:3 334:1 342:1 343:3 351:15 351:20 354:17 358:8 366:21 379:9 382:18	162:13 163:5 165:4 166:13 166:13 170:1,2 171:1 173:11 178:5,22 179:2 182:3,21 188:18 189:11 189:12,22 190:9 191:4 193:9,14,16,17 194:2,3 196:15 198:6 201:7,13 218:4 220:21 223:22 239:2 241:18 248:7 249:16 253:13 254:10,14 256:11,16 258:19 261:15 267:10 270:21 272:20 273:4 274:4,7,9,21 274:22 275:14 275:16,18 276:12 277:2 279:6,8 283:19 284:7 288:16 289:21 290:20 291:6 297:3 307:21 309:19 309:20 311:15 317:22 318:16 328:10 329:17 329:18 332:8 332:18,20 334:4 335:8 336:20 338:11
discussed 79:1 119:2 154:4 204:7 210:1 212:2 226:16 234:1 358:18	dissemination 323:3 324:12 325:6 351:10	65:11 69:12 71:22 72:11 80:12 82:9 93:17 97:22 100:15 149:20 151:6 163:15 167:14 192:15 197:14 218:22 248:3 258:17 266:11 271:21 272:14 282:1 294:6 315:4 323:12 328:7 356:1 362:20 364:6 381:1	doj 219:16 224:9,18 239:1 239:20	
discussing 220:8 290:16	dissimulation 258:5		dollars 141:8,9	
discussion 5:15 7:3 10:13 25:14 27:13 29:7 63:14 119:11 124:17 124:18 145:6 155:4 197:13 213:4,6,11 215:7 234:4 235:13 268:12 297:5 353:20 383:8	dissonance 108:8		domestic 113:22 160:4 161:22 217:19,21 365:16	
discussions 131:22 153:20 165:11 235:19 338:20	distinction 266:3 336:6		dominant 144:16	
dishonorably 123:4	distinguish 380:9	doing 22:12 23:7 52:9 68:8 91:7 95:17 116:3 136:1 139:15 174:10 177:15,20 191:12 198:14 211:7 238:6,21 241:8,17 242:6 242:22 243:4 243:12,21 244:20 245:14 249:8 250:13 251:12,20 257:3 261:1,2 261:3 262:4 263:4 265:18	dont 11:17 13:22 15:14 17:8,11 21:8 22:10,13,17 23:7 25:22 26:3,16 43:14 44:9 47:20 48:6 49:22 51:12 53:5,10 55:7 56:16,22 58:5 59:16 64:8 68:2 70:13,19 73:12 78:2,13 79:14 82:12 83:6 101:1,19 102:18 104:13 106:15 107:16	
disincentive 292:12	distrust 349:8			
dismissed 353:14	distrusting 155:21			
disparate 96:17 121:11	disturbed 5:5			
	diverse 33:4			
	dividend 190:7			
	division 216:13 219:19 223:3 246:19 250:16			
	doable 140:17			
	doc 99:13			
	doctor 98:22 99:5,9,11,14 332:20			
	doctors 99:4			
	doctrine 13:21 72:5 97:13,13 97:22 151:6 168:17 197:13 353:15			
	document 272:4 324:17			
	documentation 249:10			

339:18 342:11 344:2,16 345:11 349:9 354:3 356:20 357:1 359:12 360:9,14 361:2 367:14 371:21 376:8 377:5,6 377:19 381:10 381:13,14 door 14:3 113:16 120:13 173:3 194:20 doortodoor 14:16 dossier 49:2 doubting 351:14 369:11 doubts 243:3 downsides 282:22 downstream 36:12 334:7 335:6 downtown 248:1 dozen 360:19 dr 160:1 189:10 drafters 53:13 64:21 dragnet 67:14 draw 184:2 280:10 drawer 306:15 drawing 255:20 drawn 259:18 draws 102:11 278:16 dream 303:21 drive 57:1 63:17 148:19 172:10 382:3 driven 188:6 229:16 336:16	driving 56:10,14 117:22 188:14 drones 15:6 369:16 dropped 16:20 duck 279:6 duckduckgo 198:13 dupree 7:15 286:15 dust 75:1 dusty 306:16 duties 205:14 dynamic 308:2 dynamically 348:20 <hr/> E e 229:22 230:1 e0 278:22 ear 164:20 earlier 57:15 79:2 101:21 129:15 142:22 144:21 161:2 179:22 194:8 194:19 199:19 200:4 203:10 226:16 246:1 310:5 365:8 early 143:18 easier 38:18 39:1 112:1 141:4 145:10 324:22 325:7 349:15 easily 75:1 162:4 easy 133:12 193:18 328:22 349:18 eat 86:15 eavesdropper 39:10,13,17	ecommerce 206:17 economic 138:17 economy 289:19 291:20 ed 2:12 33:11 75:12 77:11 87:10 101:11 105:10 115:21 182:4 edge 270:9 eds 86:10 education 225:9 311:10 356:15 357:2 educations 316:12 effect 26:6 34:19 35:14 36:14,18 66:10 79:2 80:12 168:5 169:2 315:17 325:9 330:3,19 360:22 379:12 effective 35:17 41:8 67:14 69:19 83:9 93:1 94:20 114:4,12 130:12 171:18 173:21,21 174:14 188:21 192:18 208:12 210:11 213:22 246:15 276:19 283:5 292:17 311:7 312:18 312:21,22 319:18 321:12 321:21 322:15 342:7 366:19 effectively 118:12 310:1	310:13 356:8 effectiveness 319:20 377:2 effects 36:12 37:2 291:8 312:22 366:14 effectuate 11:2 efficacy 213:20 380:6 efficient 294:21 356:19 effort 87:2 118:12 323:12 efforts 7:17 32:6 207:19 217:2,8 217:9 238:14 egaurdian 220:21 egovernment 240:21 eguardian 220:15 221:2 eight 288:11 either 21:5 61:4 62:6 66:11 67:1 72:21 77:13 98:13 103:5 115:9 183:15 245:3 261:14 264:7 264:22 281:6 282:3 283:20 291:22 294:6 328:8 351:14 364:16 elaborate 38:21 69:2 121:6 162:18 217:4 electronic 290:6 308:10 319:2 element 64:1 128:22 323:19 324:10 346:11 elements 231:17	345:20 elephant 201:14 eliminate 56:16 56:22 elisebeth 4:14 elizabeth 2:7 elses 51:18 elusive 235:2 email 132:12 188:21 343:17 343:19,22 embed 354:13 356:13 embedded 30:2 127:1 218:6 220:5 224:5 230:8 embodied 80:21 embrace 152:15 emergency 99:12 emerging 171:20 197:6 290:14 emitting 142:5 emphasis 100:16 101:12 300:3 emphasize 113:8 327:15 emphasizes 108:1,14 employ 326:22 employee 95:12 343:14,17,18 343:21 employees 95:17 107:14 126:8 172:13 employer 339:6 339:16 employment 37:13 59:17 60:4 293:1
--	---	--	--	--

enable 37:12 248:4	383:13	198:15	73:14 220:22 301:17	310:6
enabled 103:6 135:11	endangering 200:11	engineer 176:21 303:10 304:18	entirely 25:13 114:20 297:19	erosion 115:12
enables 27:16 35:11 129:2	endeavor 56:18	357:11,11,12	entities 24:4 39:8 42:19	errand 381:5
enabling 28:11 129:16	ends 108:16 361:18	engineering 26:4 305:6	43:22 44:9,17	error 31:6 55:9 56:7,17,19
enact 128:19	endurance 285:1	311:17	91:6,6 209:7	57:1,6,13
encompass 12:3 171:3	enduring 133:16	engineers 127:5 143:15 172:15	209:14,18	58:16 59:21
encompassed 42:8	enemies 44:14 55:18 115:10	249:4 304:22	221:3	84:16 87:5
encompasses 8:2 12:12	enemy 114:7 160:2	305:11 309:20	entity 102:15 106:8 230:1	174:15
152:5	energy 347:7	311:14,15,18	302:15 340:14	errors 56:11,14 87:1
encounter 362:9	enforce 135:12 155:5 158:4	356:16 374:19	entitys 102:14	escalation 127:3
encourage 115:15 118:6,7	enforceable 174:13	enhance 210:16 215:2 256:2	enumerate 138:1	especially 37:16 61:7 63:22
118:18 154:21	enforced 171:22	enhanced 86:13 195:17 298:16	environment 217:14 228:11	121:22 133:10
384:2	enforcement 38:22 69:10	enhancing 27:13 144:7	289:10 325:14	143:9 155:18
encouraged 7:1	132:10,22	348:15	329:11 330:6	180:9 192:6,10
encouraging 128:16	133:20 168:4	enjoy 133:11	331:3,4 353:4	280:5 290:15
encroach 362:3	169:1 189:16	enormous 117:22 293:8	353:5	310:15 322:14
encroached 364:20	191:6 217:3	320:19	environments 346:6	328:17 338:16
encroachment 317:9 365:19	219:18 220:18	enshrined 8:12	epic 375:4	349:16 357:9
encrypt 24:3 162:6 189:12	221:7 224:14	ensure 24:16 57:22 87:3	epicenter 124:13	essence 233:3
encrypted 190:14,20	282:3 304:6	93:9 114:1	epidemics 180:9	essentially 265:21
encryption 111:8 112:4,5	enforcing 140:15 342:6	126:4,5 133:4	equally 41:5	essential 25:16 31:14 59:10
112:13 115:16	engage 248:8 276:14 319:5	171:19 173:4	equate 13:17	64:2 111:8
131:10 159:4	363:15,18	173:11 192:15	equation 210:15 213:15 214:2	125:5 316:12
165:20 166:13	engages 218:12 281:17	205:9 216:4	267:6 382:3	346:13 374:7
185:12,13,20	engaging 52:8 72:15 199:3	226:20 232:15	equipment 228:15	essentially 25:17 74:17 90:3
185:22 186:12	engender 57:2	241:6,6 246:9	equipped 377:16	168:17,19
187:4 188:2,3	engine 198:13	ensuring 209:5 245:20 295:11	era 186:4,4 228:2 234:20	169:21 195:9
188:4,5 190:10		296:2	erika 3:13 215:10 225:8	314:11,16
190:11 191:2,3		enterprise 274:4	239:10 244:17	315:19,22
196:4,5 234:10		enterprises 125:10	245:8 255:17	316:7,9 324:3
		enterprize 273:20	264:6 280:20	324:15 325:2
		entire 13:10		326:2 335:16
				335:17 345:16
				345:21 360:22
				362:6,22
				365:11
				establish 146:8 206:18

established 210:8 313:13	76:3 77:4 85:4 98:18 137:6	160:8 161:21 170:9 173:18	exemption 14:13	152:21 157:16 166:19 191:22
establishing 135:9	241:22 270:5 274:1 289:20	174:6 175:15 180:18 195:12	exercise 15:9 192:19 207:19	197:7 198:7 334:11 362:4
establishment 89:10	304:3 320:17 321:8 353:19	196:3 210:7 212:6 218:9,20	210:5 276:15 328:12 340:14	363:7,10,20 364:3,18,21,22
esteemed 140:12	367:2,18	229:10 231:19 239:11 240:19	exercises 192:12 325:4	366:5,17 368:13,20
estimate 164:4	everyday 36:1	243:14 245:18 250:6 269:15	exercising 107:11 209:16	369:2,6,12,15 369:21 370:6
etcetera 19:8	everyones 147:18 195:4	270:5 271:17 281:17 290:4	exfiltration 343:12	expectations 47:18 147:9,11
54:5 64:9 91:10 153:4	285:1	301:3 320:7 329:3 343:9	exhaustive 380:16	149:13 150:9 151:19 167:3
169:7 178:11 188:5 254:12	evidence 67:12 221:19,20	349:18 351:17 353:12 369:5	exist 55:16 80:12 136:21	196:20 226:12 323:15 344:15
279:10 313:1 348:6	evidentiary 272:15	examples 35:19 35:20 36:3	167:10 309:8 existed 136:12	346:18 347:4 380:14
ethical 172:13 379:18	evolution 124:14	58:13 122:4 exante 70:18	309:6 existing 71:16	expected 47:14 148:7 212:14
ethicists 237:12	evolves 134:3 149:16 363:8	excellent 66:17 171:11 296:1	128:18 132:19 233:14 281:8	expecting 98:18
ethics 294:6 311:17	evolving 196:19 196:20 226:10	exception 14:8 99:10 168:18	exists 158:14 302:22 304:18	experience 98:17 154:18
ethnic 122:1	exact 275:6	exceptions 53:16 65:4,12	expand 115:19 149:4 167:11	216:11,11 242:17 243:5
ethos 335:12,14	exactly 57:4 66:10 77:9	65:15 71:21 295:3 344:1	198:9 282:8 368:12	244:16 314:15 317:16 321:4
europe 290:15 343:5	88:19 89:13 147:14 214:14	excessive 365:19 exciting 226:8	expanded 188:2 217:15 304:7	325:12 347:2 experiment
evaluate 23:6,12 24:21,22 225:2	307:7 308:11 308:13 310:11	exclusion 48:11 exclusive 309:11	306:7,10 expands 231:15	54:19 55:14 experiments
236:10	310:13 320:20 339:18	exclusively 131:22	expansions 217:16	250:1 expert 61:11
evaluates 73:4 216:1	examined 281:12	excuse 145:14 317:22	expect 5:14 36:2 40:7,8,8,9	225:14 256:7 380:11
evaluating 235:7 296:6,19	example 27:12 29:4 34:15	executive 117:4 127:9 193:1	119:22 148:19 148:22 149:10	expertise 126:22 184:8 244:15
332:1	35:7,19 37:4 38:18 39:8	212:22 227:9 229:18 279:1	149:12 166:22 167:9 191:13	249:20 experts 41:10
evaluation 263:16 332:10	52:11 59:1 82:5 86:22	301:5 exemplifies	366:15 368:14 expectation	110:16 178:12 237:12 249:14
333:8	99:8 113:22 126:11 145:12	301:12 exempt 222:13	74:17 147:6 148:14 149:4	374:22 376:15 378:7
event 7:17 137:17 208:8	145:15 148:2			expired 80:13
events 123:6 323:1				
eventually 379:14				
everybody 51:18 53:11				
64:7,16 67:18				

expires 385:18	245:17 260:11	118:16 119:1,7	246:5 305:17	feasible 84:3
explain 22:10,13	266:10 276:4	120:20 122:4	faith 256:20	92:11 115:13
147:13 160:7	302:4 340:18	133:2 143:10	fall 65:12 95:6	181:19,22,22
218:5 283:22	363:8 378:5	143:19 145:1	300:10 344:15	359:17
284:4 375:10	external 244:14	147:10,10	falls 43:5 180:20	feature 365:10
378:7,15	346:12	153:8 170:6	false 5:9 56:12	374:8
explained 248:6	externally	175:11,12	56:12,13 58:16	features 175:11
375:4	346:16	177:19,22	familiar 30:8	188:15
explicit 98:8	extra 87:4	184:10 190:13	304:2	federal 4:10
345:16	177:16 205:21	193:11 197:3	familiarity	30:8 122:11
explicitly 34:8	294:19	197:14 198:2	377:21	132:11 205:3
252:18	extract 91:11	199:6 212:18	families 122:9	216:12,14
exploited 378:1	extraordinarily	213:7 223:10	famous 35:7	220:19
exploiting 39:17	117:15	223:12 224:12	fan 190:11	feedback 183:20
exploits 111:20	extreme 108:12	243:10 258:2	far 9:6 28:13	211:12 352:18
166:9 170:7	115:8	279:14,19	29:11 75:17	feel 29:9 41:20
exploration 21:4	extremely	280:4,17 292:8	123:21 168:10	54:18 128:10
explore 7:21	108:20 161:1	292:18 315:9	218:4 278:14	177:22 207:11
339:8	197:12 204:5	318:2 332:7	288:14 291:2	240:8 243:1
exploring	207:14 276:21	346:19 352:2	317:19,20	260:20 293:10
285:15	361:6 378:2	373:18 376:13	fast 277:22	355:8,21
explosion 138:3	eye 105:5	factored 177:11	371:22	feeling 16:6
expose 49:12	eyes 364:19	factors 94:19	faster 117:18	54:20
171:2 228:22	370:22	250:9	138:10,11	feelings 51:11
exposed 47:20	F	facts 5:7 34:3	169:13	fellow 9:18
47:21	face 26:1 36:9	35:6 47:8 48:3	fathers 8:11	25:19 74:11
expost 70:17	100:19 268:15	factual 219:1,9	fathom 139:19	206:2 252:16
87:4	facebook 17:10	fading 150:10	favor 4:17	286:10
express 30:16	78:15 136:21	fail 37:22 38:9	384:11	fellowships
327:22	191:17 197:2	fails 299:16	favorites 136:6	311:11
expression 21:3	198:21 199:1	failure 38:5	fbi 81:4 112:9	felt 243:11,17
expressly 204:3	339:1 352:19	58:12	217:8,19 218:1	269:11 339:12
exquisite 380:8	facial 148:3	failures 38:3	218:12,19	377:11
extended 15:2	facilitates 129:2	58:6 95:15,19	223:3,15	felten 2:12
304:3	facing 344:6	fair 67:16 100:2	225:10 239:11	33:11,17 60:22
extensive 7:2	fact 13:22 14:14	100:17 125:20	239:16 240:2	61:19 63:2
74:1 230:4	19:22 24:15	134:6 149:7	240:13 241:3	67:21 79:6
extent 12:14	25:15 37:7	204:8 225:14	246:19 248:19	80:2,5,7 86:16
52:16,17 86:16	43:14 48:11,22	231:20 296:8	281:14 306:13	89:20 90:13
89:5 123:10	49:6,13 71:20	301:19 303:3	fbis 217:14	95:15 105:10
142:17 151:5	75:6 78:8,14	336:12	225:9 252:3	105:19 115:21
174:12 188:13	79:16 88:18	fairly 58:15	fear 28:13 56:2	169:17 200:4
196:19 213:21	98:19 99:2	152:10 240:21	382:14	fewer 320:22
213:22 222:14		244:21 245:9	feared 16:15	fiction 13:20

80:9,11,11	find 26:12 38:7	350:8 354:8	288:21 297:13	flick 348:16
field 61:13 64:3	117:19 161:6	370:3,7 381:11	300:2 313:12	flip 371:17
155:18,20	184:12 215:1	381:13,14	313:17 314:11	flipped 359:15
176:10 223:7	241:8 244:20	382:19 383:12	318:20 322:17	flow 105:13
249:14	257:5,6 267:21	fippslike 289:15	323:7 326:10	142:15 143:21
fifteen 149:6	271:1 311:6	316:3	333:12 344:22	143:22 156:4
fifth 131:14	318:11 319:16	fips 220:1 221:5	345:13 346:3	flowing 185:22
294:8	345:11 347:9	222:18 224:3	348:7 352:5	flows 40:16 68:6
fight 133:3	349:4 361:8	231:21 232:1,7	358:15,16	186:6 242:2
217:2	finding 116:11	233:13 260:17	361:13 364:5	308:11,11
fighting 111:9	fine 88:5 105:18	261:11 271:9	381:12	319:2
figure 62:10	159:6,7 182:18	271:15,16	fisa 129:8,17	fluid 237:8
84:22 123:20	367:2	272:3 273:1,15	130:4,11,14	flush 359:7
159:10 162:11	fingerprint	274:21 277:3	179:15,20	flushing 360:8
190:7,8 214:3	170:11,13,20	282:1	229:19 245:18	flying 194:2,3
261:22 262:1	171:1	fire 357:14	301:21 352:12	focal 238:11
313:21 316:9	fingers 172:21	firewall 179:5	358:18,22	277:12
316:16 340:4	finish 324:20	firm 124:22	373:7 376:21	focus 5:21 12:10
379:19	fipp 326:15,22	248:1 267:15	fisc 164:18	38:13 46:13
figured 191:11	327:3,10 328:7	first 5:21 7:18	165:3 353:13	94:19,20 95:14
254:16	328:14	13:3 18:7 34:1	374:10	111:6 120:3
figuring 191:13	fipps 25:21 26:5	34:5 36:6	fisma 320:17	131:22 150:3
191:15 312:21	80:21 81:7,8	55:10 61:20	fit 58:9 62:7	217:7,8 228:3
file 34:22 74:22	82:2,7,12 83:5	62:7,14 65:17	97:22 206:7	230:18 238:14
151:10 152:14	83:17,18,22	71:4 76:18	322:11	243:12 244:12
222:2 306:13	84:1,6,12 86:3	80:16 94:22	fits 50:1 101:19	244:14 256:2
306:19,22	86:17 87:20	99:22 102:9	261:10,11	258:21 264:9
307:5,7,8	88:3,20 99:22	110:11 111:7	five 4:12 18:6	268:18 289:16
filed 129:10	100:8 101:18	114:18 118:20	76:1 139:7	289:21 290:17
files 34:14,17,19	118:6,6 119:4	119:2 120:4,8	141:20 159:16	292:1 293:12
35:3	119:7,14	121:5 124:22	177:1 235:10	294:12 305:13
filings 375:12,12	152:17 162:17	128:7 142:1,9	278:9 286:10	323:18 361:15
fill 334:12	271:18 288:3,8	142:12 148:13	322:9	361:22 362:8
377:18	288:12,19	158:8 159:22	fix 57:12 305:2	382:2,6
filled 283:13	289:7,21 290:1	162:20 171:12	305:7	focused 31:5
filter 188:22	291:18 296:18	179:20 186:13	flannel 164:22	127:18,20
final 6:6 39:21	296:22 297:8	189:9 199:10	flashlight	128:11 131:15
134:14 285:3	297:16 299:17	206:21 226:6	350:15	131:17 177:3
339:19 372:16	299:20 300:4	228:1 231:19	flat 136:21	209:5 241:21
finally 7:13 95:5	326:8,14,16,19	235:14 242:1,7	flatirons 311:12	242:20 244:6
114:15 119:21	328:19 329:4,4	242:19 253:22	flaw 253:1	248:2 260:19
145:22	330:2 331:8,20	255:21 274:4	flawed 71:18	285:19 290:6
financial 304:9	332:3,8,15	276:1 281:19	flaws 83:5	292:14 293:7
336:21	333:4 335:13	285:13 287:13	flexibility 38:15	296:16 352:9

353:7,11,20	372:12	forward 41:14	293:13,14,18	22:20 27:13
focuses 12:15	forces 346:22	96:15 116:7,22	294:3,5 314:12	212:6 266:21
295:17 338:3	376:18	141:1,15 215:6	350:12 353:12	freedoms 133:9
focusing 211:6	forcible 120:20	269:20 270:10	353:14 368:22	freely 22:18
224:14 281:14	forcing 263:15	305:16 352:16	372:15 383:12	127:13
341:20 350:9	268:4	383:18	framed 229:20	frequently
350:10 382:20	forecasting	foster 29:7	366:1	228:13 238:2
foia 14:6,8	381:4	127:16 129:20	framers 313:19	238:22 248:16
folks 178:20,22	foreign 111:16	130:4	framework 46:1	288:14
193:19,21,22	115:3 179:15	fostering 27:9	82:13,17 100:8	friedman
196:22 203:10	212:10,21	fosters 27:1,17	100:9,12,20,21	136:19
205:19,21	227:6,7,16	found 88:15	132:17 154:9	friend 13:8,14
235:20 238:22	228:3,5,12,16	92:22 171:18	205:22 231:21	friends 17:11,12
251:14 255:3	229:18 232:6	173:20 235:1	232:1 274:3	70:1
269:3 283:15	256:12 301:5	246:22 256:9	296:10,19	frog 347:10,12
285:20	358:7 381:21	316:13 323:8	297:1 326:20	front 6:22 9:11
follow 65:8	foremost 313:17	foundation	327:12,17	14:2 85:21
126:8 173:17	322:17 344:22	135:9 137:20	332:1,15 333:5	109:22 145:6
189:13,13	346:9 361:13	foundational	333:6 338:12	203:17 207:6
205:21 211:18	364:5	54:9	368:21 369:7	241:10 254:10
211:22 212:14	forget 23:16	founded 23:4	369:12,21,22	286:3 303:21
213:8,9 232:8	form 195:17	25:20	370:4 372:5,7	365:20
298:6 299:17	225:4 233:1,19	founder 25:5	379:21	frontend 245:16
followed 9:17	236:16 242:9	33:13	frameworks	300:6,14 359:2
12:7	270:14	founders 304:16	204:8 231:16	359:3,16 371:9
following	format 9:9	founding 8:11	296:12 333:7	372:6
138:20 140:11	former 3:20	four 5:20 118:19	framing 265:14	fruit 305:17
185:15 211:20	211:21 313:6	236:21 313:15	framework	frustrated
212:18 213:5	373:4	317:14 357:15	211:18 237:1	373:13
242:22 260:15	formerly 25:7	fourth 12:20	frankly 56:11	frustrates 38:4
344:21 363:3	122:6 376:19	14:22 22:21	288:3 289:18	38:5
follows 36:19	forming 145:2	27:22 29:13	290:1 319:3	frustrating 86:7
43:10 98:12	forseeable	42:2,14 43:6	325:8 329:10	ftc 264:8
followup 245:7	221:22	52:9 53:7,14	franzen 8:3	fulfill 300:18
263:14 354:6	forth 268:17	64:13,22 71:15	fred 3:18 350:6	fulfilled 254:7
377:6	284:15 318:16	71:17,22 72:5	350:6	full 22:11 76:3
food 276:22	374:11	72:6,8,20	free 20:9,9 22:6	116:20 123:10
fools 381:5	forthcoming	80:19 81:8	22:6 41:21	156:3 168:21
footprint 246:6	108:21	82:1,2 103:18	54:19 172:3	205:6 209:6
footprints 240:2	fortunately	107:4,9 119:21	241:14 355:7	351:19
force 51:9 61:21	288:8	121:5 130:16	364:7	fulltime 244:12
89:21 90:3	forum 1:5,12	167:13,19	freedom 5:4,4,5	248:8 249:20
195:5 263:21	205:1 224:12	168:18 229:16	5:8,9,12 11:2	fully 38:1 84:12
forcefully	264:3	292:5,13	11:16 14:6	100:11 189:20

191:14 208:17 210:16 fun 275:9 function 17:2 207:4 254:6,17 259:2 functionally 14:3 functioning 245:21 functions 104:22 207:20 217:14 252:4 254:3 273:5 298:8 fundamental 132:2 226:21 272:18 287:18 334:8 fundamentally 69:7 232:22 234:2 297:22 further 34:21 35:15 86:20 91:15 127:4 132:15 225:20 266:10 282:13 354:3 362:10 385:9 future 57:17 128:20 138:8 143:6 181:18 221:22 227:4 233:15 262:22 293:21	gathered 22:4 48:4 49:15 78:7 gathering 20:15 20:20 47:3 71:10,13 72:16 75:1 180:6 381:22 gathers 22:2 gay 122:19 123:13 geiger 3:19 295:14,14,20 326:8,12 327:2 331:19 340:8,9 358:15 368:16 371:3 375:16 377:13,19 general 29:1 30:10 42:4 95:4 96:3 112:10 209:11 209:12 215:13 215:17 217:19 238:3,7,15 239:12 240:1 243:15,15 244:7,7 257:17 257:19 290:16 generalist 248:12 generalized 84:8 generally 19:18 69:6 90:10 238:15 265:15 299:12 360:2 generals 295:6 generated 182:18 generating 139:18 142:5 182:17 generation 156:14 157:14	158:15 191:11 191:21 generations 341:14 gentleman 9:11 gently 203:20 genuinely 259:15 geogretown 3:4 george 2:15 18:3 georgetown 1:12 4:7 117:5 georgia 3:3 110:14 143:10 german 343:17 germany 343:20 getting 44:4 45:1 52:8 82:18 110:22 143:1 184:21 187:10 347:10 gewercman 7:16 giant 343:13 give 9:11 33:14 58:13 71:5,6 105:16 120:14 143:13 154:19 170:8 180:18 229:13 274:21 308:5 333:16 333:17 335:2 344:17 364:7 given 5:14 23:17 90:7 111:11 114:22 119:10 120:2 179:4 205:20 233:4,4 246:6 250:7 253:7 265:7 273:1 274:11 297:10 319:17 334:8 358:11 373:16 383:16 gives 21:12	64:14 270:5 giving 87:11 97:14 249:12 347:20 glad 88:5 global 131:18 206:19 globally 200:15 globe 154:1 glove 322:19 go 8:10 17:9 22:10,13 28:22 43:9 48:20 51:2 54:5 57:12,18 67:19 75:20 79:19 87:15,17,19,22 88:8 103:8 105:10 109:15 109:17 141:16 142:8 146:21 148:18,19 149:2 152:18 159:17 168:9 168:19 173:3 176:15 178:7 181:8 184:12 184:16 185:4,6 186:21 196:13 201:21 202:2,6 202:8 207:5 220:21 223:7 238:1 245:17 261:3 262:13 263:17 269:20 274:1 278:10 285:6 286:17 286:20,22 287:19 298:9 312:8 320:18 331:18 335:9 346:19 347:18 350:6 353:16 357:15 372:11	373:20 374:3 380:20,21 goal 268:22 301:6 349:10 goals 86:20 114:17 god 355:3,5 goes 10:11 21:19 91:16 155:20 171:12 181:2 201:19 211:9 211:16 278:16 351:4 356:14 going 10:4 23:7 23:22 24:7,21 24:22 25:1 41:16,22 63:19 66:10 74:10 75:22 77:19,20 80:17 84:9,21 92:20 101:3 102:4,4,17 120:16 138:11 138:12,13,14 139:17 140:7 141:3,4 145:8 145:9,21,22 149:18 156:17 164:21 165:1 165:15 166:16 169:13,13 174:2,8 177:11 177:16 178:21 182:20 183:6 184:19 185:11 186:3 187:18 189:14,18,21 189:22 191:14 193:19 195:22 197:8 199:21 200:4 202:11 207:4 212:5 215:2 233:20 234:18 241:16
--	--	---	---	---

G

gained 288:8
gains 27:2
gap 156:14
324:17
gather 72:22
74:20 105:1
271:11,15

245:1 250:1,4	60:21 85:19	43:15,21 44:8	200:16 202:9	132:4,15 133:3
251:5,8,11	88:12 100:6	45:9 47:3 53:8	202:10,16,17	188:12 200:8
252:2 253:5	107:19 109:9	54:21 55:16	202:18 203:2,7	258:14 293:9
255:7 257:10	109:10 110:19	56:16,18 58:1	204:1,20	298:8 317:4
258:14 259:13	113:17,17	59:17 61:2	206:14 216:11	318:4 380:6
259:18 260:9	114:8 115:12	63:1,3 65:1	230:17 231:17	governmentwi...
260:10,13,17	116:22 117:9	69:8,19 70:2	233:13 241:13	209:16
261:6,20	129:20 155:8	70:10 72:15	258:15,17,19	gps 15:7
263:11,13	157:20 158:2	73:3 74:19	259:1 263:4	grabbed 93:10
265:21 269:13	159:11,21	75:7,8,14,18	264:20 266:22	gradations
270:2,9,16	160:3,5,9	77:21 78:8,11	267:18 272:2	308:1
272:7 276:14	162:3 165:20	78:17,20 79:19	273:7 285:17	grade 283:14
279:7,9 283:5	176:2 177:6	79:20,22 81:9	294:14,22	grand 54:7
283:19 286:21	182:11 194:20	81:20 85:5	295:18 296:10	grant 301:20
311:19,19,20	197:6 198:6	88:21 90:2	297:12,18	303:9,9,15
312:1,10	203:4 207:5	93:3,15 94:21	298:18 299:17	318:19 319:21
316:12 319:8	245:22 256:20	95:12 102:11	299:19 300:2,8	338:10,11
322:3 323:17	263:5 275:1	102:14 103:14	301:9 302:3,6	342:9,10 348:7
324:13 330:9	277:14,15	103:17 104:3	302:12,18	348:13 356:12
339:10 342:3	279:5 284:22	104:19,22	303:2 314:6,10	362:22 366:11
348:17 349:19	294:22 321:16	105:2 107:12	315:2,7 317:7	378:12
352:16 353:1	321:17 327:5	108:4,6,12	317:17,18,22	granted 55:20
355:11,22	360:15	111:18 116:11	318:1,2 322:15	221:15 322:18
356:6 357:7,8	google 43:16	117:13,14	325:12 327:20	323:5
357:13,14,20	77:19 78:14	118:1 122:11	334:16 337:6,7	granular 11:14
359:20 360:10	112:3 339:13	124:7 127:13	337:10,13,19	101:13 210:10
361:8 362:16	googles 108:7	127:15,19	337:20 338:6	307:16 309:1
363:19 370:7,8	gotten 37:15	128:5 129:5,11	339:14,15	342:19 348:10
371:22 372:1	322:22 337:17	129:16 130:6	341:21 342:8	grateful 313:13
378:21 379:13	gov 7:8,11 384:5	130:16 131:1,5	343:1 344:9	great 42:22 43:1
380:20,21	384:9	131:7,12,14,16	345:2,15	43:17 74:14
goitein 2:13	governing 221:1	150:13 153:16	360:17,22	75:8 105:15
10:6,9 42:13	government	157:2 167:16	361:4 366:15	116:17 143:5
44:2 51:1,3,19	3:10 6:3 8:21	167:20,22	368:7,8 376:10	155:14,15
53:3,5 63:22	11:1 13:15	175:12,14	379:19 380:15	160:12 180:8
64:19 78:3	14:8 15:6,18	176:4,4,6,15	382:15 383:9	234:12 238:9
80:18 81:14	15:20,22 16:2	176:18 178:1	governmental	239:7 250:4
82:19,22 87:9	20:14,19 21:21	178:15 179:1,6	12:6 85:3 86:5	313:8 334:14
97:9 102:10,17	21:21 22:2	179:10 180:14	94:17 97:7	344:13 368:4
103:10,22	23:5,6,12,19	181:1 186:10	107:11	369:5 380:12
golden 186:6	24:4,11 27:14	186:16,20	governmento...	382:18
good 4:2 18:5	27:21 28:1	187:3 189:5	228:14	greater 47:10
27:10 40:5	29:22 30:7,18	191:7 192:9	governments	62:4,5 83:13
49:6 53:9,11	39:7 42:15,16	199:16 200:1	45:1 57:21	84:5 86:19

87:2 104:3	253:22 256:6	199:19 318:11	harlan 18:2	17:7 18:11
130:5 204:15	257:12 271:21	322:19 385:12	harley 3:19	43:11 69:1,2
211:8 212:1	273:10,14	handle 64:15	295:14,14	150:6 201:1
213:6,14	279:8 326:16	127:8	337:9 358:1,8	heard 15:13
237:15 290:17	343:8 344:3	handling 37:15	358:11	83:15 96:11,18
300:3 301:10	354:4 358:13	231:11	harm 16:5 49:12	97:4,12 130:14
302:4 303:6	guessed 305:8	hands 151:17	50:20 54:6	139:1,16 140:7
337:11 376:20	guessing 156:8	156:8	55:5 59:7	166:19 199:11
greatly 176:19	guidance 159:8	hanging 305:17	237:2	235:19 269:11
greece 166:7	162:11 216:3	happen 15:11	harmful 49:7	280:2 348:1
green 9:12	218:1 312:7,13	105:8 224:18	121:15,22	383:9
207:5	guide 125:17	251:17 270:21	123:19 382:8	hearing 4:9,16
grind 45:3	226:20 276:7	300:11 348:17	382:11	4:17 207:9,18
grocery 148:18	282:2 293:20	happened 80:10	harmless 36:11	355:6 384:11
ground 28:11	guided 379:17	122:13 184:12	harmony 135:8	384:15
31:19,20 32:19	guidelines	311:1	harms 16:22	hearings 210:9
250:8 376:3	217:19 364:4	happening 24:1	50:5,7 52:6	hearsay 99:10
groundbased	gun 70:3	80:10 139:13	58:10 76:15	heart 208:7
369:17	guy 161:7	140:11 144:10	92:20,21 291:7	hearts 346:10
grounds 311:5	310:21	144:13 153:20	331:17,17	heavily 33:2
332:6	guys 139:5	154:6 175:1	336:9,20,21	182:22 375:3
group 3:20 25:6	171:10 188:10	241:18 252:20	340:17 350:17	hedge 380:14
116:1 161:15	244:9	255:2	harness 234:18	held 1:12 14:12
313:5	H	happens 49:14	hasnt 58:7 74:4	14:18 33:2
groups 41:10	habit 259:7	57:5 109:17	97:5	91:2 132:13
251:1 336:10	hack 130:17	119:1 166:12	hasten 32:4	267:9 318:1
growing 40:17	hackers 158:15	260:11 265:16	hate 291:22	325:10
62:15 147:12	187:5 188:10	happy 59:3	havent 87:18	hell 33:14
185:15 226:10	hacking 130:20	75:20 237:18	90:10 238:19	help 41:11 85:8
grown 104:21	131:2	278:10 326:8	283:21 381:20	105:1,1 116:1
growth 142:15	hadi 3:7 134:14	hard 197:10	hawk 183:22	128:5 133:3
142:20 143:3	134:17 142:2,9	246:8 249:6	haystack 257:4	160:12 161:6
guarantee 107:1	154:17 164:19	266:16 268:7	257:6	180:4 195:22
107:3 138:9,9	169:8 182:2	270:3 310:11	head 323:17	200:16 226:11
141:2	189:7	316:2 323:14	324:16	237:7 249:18
guarantees 42:9	hadnt 347:12	324:18 347:13	headed 240:3	271:3 289:21
138:7	half 124:13	371:21 381:5	headon 297:11	313:16 326:2
guard 261:7	137:15,16	harder 140:10	heads 215:22	335:17 340:4
guarding 291:6	139:10 163:13	195:20 314:3	headway 154:8	342:13 358:19
guess 61:8	284:3 368:1	317:11	health 37:13	377:3 378:14
161:18 165:21	halfway 108:9	hardwired	180:7,8 270:3	382:5,10,17
167:18 186:21	hand 58:18	308:18	healthcare	helped 129:20
189:6 194:18	68:19 110:9	hardwiring	332:18	206:18
195:1 224:1		308:14	hear 5:16 6:3	helpful 11:10

116:6 159:9 164:19 202:19 232:17 248:9 254:15 260:3 276:6 314:5 354:2 383:17 helping 147:22 162:11 251:17 helps 261:14,17 263:7 379:7 382:2,3 heres 267:17 hes 124:12 287:3 hesitate 80:2 heuristics 143:16 hew 162:21 hey 46:18 120:13 148:17 176:12 243:7 269:19 274:2 hide 18:11 19:6 166:2,6 hiding 18:8,15 high 29:16 70:12 106:2 119:16 134:16 163:5 170:16 193:7 196:1 289:14 305:14 306:1 higher 336:13 336:16 highest 29:12 33:2 152:20 highlight 96:10 highlighted 91:13 highlights 120:19 highly 183:17 hill 87:21 304:21	hindsight 123:5 hintze 3:6 124:11,15 134:9 149:5,12 151:4 152:3 153:18 168:3 168:22 171:17 172:5 174:12 179:22 180:13 180:22 181:4 185:21 188:1 198:18 201:6 hintzes 144:14 hipaa 99:19 145:17 229:12 332:21,22 historical 162:21 229:14 historically 122:3 229:15 233:18 history 44:12 58:3,8 137:18 231:20 284:2 326:6 354:3 hit 48:21 311:19 hits 259:11 hitting 118:4 hobby 271:8 hold 62:20 226:21 286:16 318:10 321:9 334:6 342:12 342:12 346:14 362:13 holder 37:5 holding 26:3 62:13 91:6 110:1 207:17 287:10 340:14 holdings 43:20 holds 237:1 286:4 holistic 233:1	home 14:22 42:2 113:17 141:11 195:4 homeland 25:8 100:5 104:6 226:2 290:4 303:12,13 homes 151:10 151:18 341:4 honest 107:7 honestly 87:18 342:14 honing 182:18 honor 259:9 313:9 honored 226:5 hoops 320:19 hope 9:19 41:4 88:16 126:8 143:3 172:21 193:9 199:11 213:3 225:19 284:9 343:3 hopefully 306:15,20 307:9 359:1 hoping 140:19 hops 91:9,10 horizontal 316:17 horrible 174:1 horse 271:8 host 69:19 224:10 hosting 226:5 hotel 1:13 4:7 hotter 347:11 hour 181:11 hours 139:20,21 140:2 house 170:2 369:18 housekeeping 203:12	houses 53:9 hr 127:7 huge 186:17 250:15,16 310:7,8 320:3 320:5 356:7 374:18 hugely 144:16 human 15:4 26:17 51:5,5,6 51:14,16,20 56:18 78:9 96:21 98:17 132:3 153:10 155:10 174:15 349:5 350:1 351:22 humandriven 348:21 humanly 56:15 hundred 43:3 56:4 93:17 139:20,20 140:2 141:9 159:13 198:15 379:1 hundreds 325:16 hurdle 282:11 hurt 160:21 hurts 112:18 hypothesis 56:3 hypothetical 55:15 173:19	106:1 116:9 144:21 145:5 165:16 179:8 208:6 227:1 229:11,13 233:15 272:22 313:15 318:18 318:19 322:13 326:7,10 330:17 333:16 354:10 idea 50:17 108:6 113:18 147:18 162:3 239:3 269:2,21 276:9 287:10 ideas 17:4 21:4 152:15 171:14 291:3 identical 355:12 identifiable 37:8 113:8 229:8 identification 46:4 48:22 161:1 237:6 identified 3:10 6:5 203:22 identifier 34:17 identifiers 34:11 39:9,11,18 identify 9:3 10:4 36:1 68:7 90:5 163:22 182:8 197:6 214:3 232:17 235:16 236:3,17 270:18 382:7 identifying 36:9 39:14 49:3 183:15 196:12 196:14 198:7 381:17 identity 34:20 35:2,3 39:20
---	--	--	---	--

59:22 113:21 216:14 ideological 10:22 ideology 44:10 ignore 48:2 ignored 352:2 ii 122:7,18 187:6 ill 17:22 41:17 49:18 58:13 67:18 74:12 76:5 79:6 102:5 106:16 107:22 109:16 119:10 121:18 134:9 142:8 175:22 176:1,3 185:4,5 187:20 189:8 198:8 217:7 250:10 257:18,18 276:11 279:6 279:11 280:2 280:20 287:10 304:2 316:11 364:1 378:12 illegal 294:5 illegally 292:8,9 illuminative 74:2 illustrative 380:19 illustrious 10:4 im 10:4,19 11:12 28:12 30:8 41:16,20,22 55:1 63:19 64:7 68:4 69:21 73:8 75:20 80:19 81:15,15 82:11 82:14,18 83:8 85:18 87:12 98:10,18 101:5	102:3,4 107:8 107:18 108:11 118:18 134:22 135:1 137:12 140:10,19,22 149:1 153:18 160:11 165:15 166:20 167:1,5 167:8 168:9 171:5 174:1 182:4 189:15 190:11 193:9 197:2,8 201:11 201:20 207:3 220:7 231:13 237:18,18 241:11,14 242:12 247:10 253:5 255:7 259:5,21 262:6 263:10 269:6 270:16 271:21 277:14,15 278:10 279:8 287:9 288:5 289:8,12 303:20 304:22 309:3,9 313:8 318:6,16 326:17 328:22 330:9 333:14 343:21 350:21 350:21 351:14 357:12,14 360:10 367:2 370:11 372:12 381:13 image 28:9 68:10 imagine 87:2 306:12 378:3 imagined 86:4 imbalance 357:17	immediate 352:18 immediately 266:8,8 impact 3:2 6:1 17:1 109:13 121:11 172:18 175:7 204:10 220:12 224:21 236:18 240:19 289:18,19 290:5 291:19 296:14 332:5 375:5 382:11 impacted 107:4 266:22 impacts 30:18 118:21 119:8 204:21 205:6 266:13 291:8 291:17 336:9 336:19 381:17 381:18 382:8,8 382:10 impediment 178:18 implement 145:4 146:1 206:19 342:13 implementation 346:12 implemented 84:13 92:12,16 100:10,11 215:19 345:21 implementing 379:22 implements 348:4 implicates 121:5 implication 37:14 39:6 107:20 implications	36:6 76:13 89:2,17 152:15 153:5 185:11 370:19 371:2 implicit 98:11 282:17 implies 219:9 imply 98:7 importance 11:15 115:22 180:8 214:16 242:15 279:13 350:9 important 11:18 12:12 20:22 28:14 38:17 49:21 68:1 69:13 71:11 73:5,10 96:10 96:13,14 100:1 120:5 124:17 136:15 143:6 147:3 153:5 161:12,17,19 161:20 162:5 178:10 192:7,9 196:4 207:9,21 216:9,17 224:21 227:20 239:4 240:8 242:4 243:7 257:11 258:1 259:2 260:20 264:1,16 272:11,12,13 276:21 277:2 285:4 296:9 312:5 313:14 329:22 331:15 335:12 336:6 340:16,21 341:10 346:22 359:4 372:10 374:7 379:5	impose 29:16 72:21 81:9 95:7 239:16 325:2 imposed 322:19 323:4 324:6 346:16 imposing 69:9 impossible 55:20 77:18 86:18 164:3 330:5 373:16 impoverish 17:2 impression 17:18 200:3 imprison 104:1 improperly 49:13 94:5 improve 114:16 165:9 200:10 224:20 240:18 357:2 improved 111:13 224:7 improvement 309:6 improving 349:19 impulse 85:19 inaccurate 60:18 inaccurately 294:17 inadequate 57:7 332:14 inadvertent 31:7 174:21 inappropriate 98:7 265:20 350:18 incentive 104:1 195:3 inception 119:11
--	---	--	--	---

inching 369:10	290:22 309:1,2	326:15,22	inevitable	47:19 48:3,4
inchoate 266:20	incremental	327:10,19	178:13,20	48:13,14,19
incident 127:2	67:3	328:6,14 329:9	179:1,3,10	64:1,8 66:7,9
220:16	inculcating 95:1	329:18 330:2	200:1	66:22 67:3
incidental	independence	331:8,10,14	inexorability	68:6 69:8 70:3
262:20 279:3	4:22	334:11 336:15	142:11	71:10 72:16,22
incidents 316:14	independent	337:14 340:19	inexorable	74:20 75:11,15
include 21:2	29:17 31:1	364:22	142:4	76:14 78:7,8
47:3 115:19	41:10 57:20	individualized	infer 34:3 35:6,9	78:15,16,17
231:15 234:8	59:9 60:3,10	84:2	37:1 59:8	79:9,10,16,22
324:3	73:2 92:2	individuals 8:15	79:15,16	81:19,20 84:3
included 51:16	315:14 325:21	20:7 83:12	inference 35:14	87:16 89:7,15
141:12	373:22 374:1,2	84:6 91:12	37:3,8	90:6,16 91:2
includes 126:21	374:9,16	121:2 204:21	inferences 35:13	91:19 93:9,10
127:2,9 302:6	index 110:7	205:16 253:8	35:16	93:21 97:14,16
327:14	indiana 3:18	281:22 291:19	inferred 35:11	98:1,4 99:3
including 13:10	287:3	298:12 299:5	40:21 152:9	100:2,13
61:1 112:6	indicated 364:2	302:19 327:7	inferring 35:18	102:21 103:8
125:22 165:6	indirect 115:11	333:2 336:10	infiltrate 112:1	103:15 106:6,9
206:20 216:5	indirectly 183:4	336:10 337:5	infiltrations	112:6 115:7,10
312:17 370:6	indispensable	337:10 340:12	16:18	118:2,15 120:9
incorporate	296:19 333:6	340:15 352:10	infinite 308:5	120:22 121:2
234:19 310:1	individual 8:1	363:15 371:14	influence 115:4	122:8,10
incorporated	9:4 19:14,16	individuuated	212:13 242:13	125:21 129:6
144:14	19:19 20:1,2,7	60:16	inform 5:18	129:13 131:5
incorrectly	20:8 44:7 49:2	industrial 20:18	226:11 261:14	133:5 134:6
73:11	49:7 54:15	industries 104:7	261:17 278:18	139:12 141:8
increase 50:15	59:5 60:8,15	industry 59:20	365:4	141:12 142:7
128:21 130:10	66:19 80:22	60:4,5 63:1,15	informant 13:16	142:16,20
141:3 169:15	81:3 82:3,8,15	104:21 117:13	information	143:20,22
increased 114:6	86:3 94:21	117:14 118:1	5:11 12:9,13	144:1 146:10
149:14 169:18	95:17 112:19	118:11 131:11	13:4,7,10 14:1	150:16 151:1,2
198:15	125:9 130:7	144:4 158:1	14:7,9,14,18	151:9 156:5
increasing 61:12	163:7 164:13	178:5,21 179:3	15:3,10,12	160:19 161:4
104:9 131:9	183:14 204:4	179:6 180:15	16:3 17:11,12	163:16 166:6
186:10,11	221:5,8 230:1	189:11 190:5	19:8 20:15	168:7 169:10
245:11	230:21 235:8	200:17 202:5,9	22:3,4,5 23:18	169:18 175:14
increasingly	236:11 268:14	383:10	24:20 33:14	176:12 186:8
104:20 108:5	270:15 271:18	ineffective	34:6,8,20 35:1	186:18 194:10
151:8 188:11	272:6,7 273:6	208:19	35:2,11 36:10	196:12,14
incredible	274:9 277:11	ineluctably	37:1,4 39:5,14	200:2 201:20
351:20	289:17 295:4	69:18	40:15,16 42:21	202:10 204:9
incredibly 17:10	295:10 296:21	inevitability	43:13,21 45:5	204:12,16
72:2 246:7	302:16,17	142:11	45:7 47:14,16	208:15 209:22

219:5,6 220:18	informing 145:7	211:9 239:5	insufficiently	175:4 316:15
221:2 222:4,11	informs 208:14	242:10 244:1	299:12	intentioned
222:14,19	infrastructure	325:9 334:16	intel 193:22	204:11
228:22,22	111:15 310:9	339:3	intellectual 5:3	intentions 38:6
229:8 231:11	312:4,6 342:18	insiders 115:3,6	intellectually	interact 98:6
231:20 232:3	ingenuity 143:4	insight 247:5	275:9	interacting
235:4,5,15,17	inglis 3:20 313:4	335:3	intelligence	139:13
235:22 236:7,8	313:8 322:13	insights 320:12	215:4	interaction
236:12,13	322:17 324:1	insist 62:19	intelligence 3:12	273:6
241:12 242:2	333:20 334:4	114:10	15:13 30:4,11	interactions
246:12 248:6	344:12 348:1	insofar 11:10	74:1 85:12	70:16
249:9,12	351:6 360:13	27:1,5 107:10	90:18,22	interactive
253:18,19	364:5 380:2	inspection 58:17	118:11 119:15	110:13
254:10 261:4	ingrained 118:5	inspections	163:3 179:16	interest 8:22 9:1
265:2,4,6,8,20	inherency 55:11	58:14	192:7 206:6,13	12:7 19:13
266:6,12,17,19	inherent 26:17	inspector 244:7	207:13,15	20:1,2 29:2
267:1,3,7	61:5 104:9,13	295:6	208:7,13,18,22	33:7 66:21
268:10,14,19	133:16 235:7	inspectors 30:10	210:11 211:10	67:2 73:17
268:21 280:4,8	279:21 339:22	95:4 209:12	212:11,14,21	91:22 97:15,15
281:18 283:10	inherently 20:18	instance 32:22	213:1 214:12	98:4 153:10
296:8 299:1	26:20 279:17	55:21 59:2	214:19 216:22	155:15 211:17
300:9 302:14	initatives 240:8	60:2 94:22	219:17 221:22	229:3 256:22
302:15,16,19	initial 9:14	145:18 160:15	226:13 227:6	279:12 280:19
303:3 307:7,8	218:7 232:13	161:9,14	227:16 228:3,5	361:21
307:13 310:21	235:9 251:2	164:18 255:22	228:12 229:19	interested 80:20
317:19,20	initially 9:10	256:9	231:6 232:6	89:20 137:12
320:9,11,20	90:15 271:12	instances 28:15	242:10,18	149:9 153:22
321:10,15	initiatives 212:7	29:9 71:22	243:7 244:2,8	154:16 160:1
334:13 337:11	215:19 216:2	159:7 161:9	245:1 253:15	220:10 272:22
338:7,8,21	247:6	195:15 378:1	254:4 255:19	367:6,8 372:12
339:2,7,22	inject 255:17,18	instill 357:18	256:12 258:2	385:11
340:1,12,14	injury 104:2	instilled 304:17	266:15,19	interesting 11:8
342:1,4 343:11	256:5	institute 66:17	267:8,10	88:15 107:21
348:9 349:21	innocent 256:13	institution 30:7	275:11 276:11	216:18 226:17
358:2,4,12	innocuous 268:15	institutions 61:1	298:5 301:5	239:18 268:8
359:7,11,14,16	innocuous 47:6	107:10 133:10	304:7 320:3	282:18 339:8
360:9 366:18	innovative 39:3	210:1	353:5 358:8	344:4 357:10
366:22 367:7	inoperable	instrument	381:22	357:16 365:8
368:2 370:15	101:7	146:8	intend 313:20	interests 2:10
370:17 371:14	input 211:11	instrumental	intended 217:15	3:2,10 5:21,22
377:1	237:9	26:20 54:2	intent 243:21	6:4 8:1,14 9:4
informative	inputs 143:14	97:1 98:20,20	intentional	9:8 12:12 21:1
383:8	inside 94:16	instrumenting	174:18	45:21 49:18
informed 66:3	176:15 197:4	165:8	intentionally	61:5 66:19

73:13,14,19 79:4 97:3 101:14,16,20 109:12 121:6 151:3 203:22 204:4 211:2,3 231:11,13 256:3 264:4,10 264:11 285:15 295:10 334:2 340:17 367:12 interface 349:20 internal 30:2,10 57:21 95:20 173:1 193:2 224:16 244:17 246:10 247:9 300:9 341:9 346:13,14 365:9 366:22 367:7 372:22 372:22 internally 268:2 280:2,16 338:20 international 51:10 113:2 132:16 154:3,8 206:18 internet 43:17 115:1 131:2 139:1 143:11 143:12 160:17 185:17 186:5 335:21 internment 122:17 interpretation 301:11 314:21 interpretations 71:17 315:1 325:19 interpretative 356:9	interpreted 301:15 355:20 interpreting 352:20 interrupt 259:4 intersection 110:16 intersections 135:14 interspersed 228:17 intervening 54:5 55:4 intervention 60:10,10 77:13 interview 329:20 intimate 151:16 introduce 109:16 201:17 235:11 introduced 137:5 intruder 113:18 intrusion 5:6 29:15 58:19,20 intrusions 112:14 intrusive 218:10 218:16 219:3 221:17 261:2 262:17 341:2 364:10 inured 147:18 invades 120:21 invest 188:16 312:6 347:7 invested 316:20 investigation 218:7 219:10 221:21 352:7,9 investigations 217:21 219:8 219:14 221:9	223:10 investigative 219:12 223:8 281:15 investment 127:11 invitation 303:16 invite 206:2 invited 6:14 9:21 224:17 inviting 10:12 207:8 216:8 295:22 involve 122:5 200:21 201:3 215:3 218:22 273:6 279:17 308:19,20 involved 58:11 116:8 145:2,6 146:5 184:13 199:16 362:1 374:13 involvement 10:15 involves 18:19 18:20,21 49:1 122:1 279:20 iot 139:1 iphone 137:4 ireland 132:14 ironic 337:16 351:5 ironically 361:14 irreconcilable 55:8 irrelevant 350:11,21 irs 69:10 isnt 18:18 19:22 23:14 49:10 54:15 75:8	116:4 246:18 252:8,8 304:12 362:7 367:10 368:14 378:16 isolated 36:14 228:13 263:20 isolation 36:11 issue 21:18 49:8 59:5,6 87:15 113:6 125:3 131:19 177:7 179:18 193:5 193:18 196:8 229:9 249:3 287:18 309:18 320:5,13 329:22,22 334:22 357:1 378:16,17 issued 162:22 217:18,21 issues 5:19 10:15 30:18 63:11 67:22 75:4,19 100:17 107:5 110:16 124:20 134:12 135:16 150:4,6 153:8 154:4 171:21 172:14 173:4 176:20 205:2 224:16 225:15 240:7 247:2,18,18 248:22 276:4 284:19 285:7 289:17 293:22 295:17 352:15 353:14 379:7 issuing 29:18 item 36:7,8,20 36:21 201:15 items 34:2 36:15 91:11	iteration 271:16 iterative 263:13 277:18 itll 269:6 346:10 ive 10:14 13:9 31:4 43:8 70:14 88:15 124:21 144:6 208:17 212:19 214:13 242:6 251:20 256:16 261:9 273:11 274:6 288:8 290:3 293:13 357:15 367:21 ivy 197:4 <hr/> J <hr/> jackpot 278:14 jail 44:18 58:22 james 2:6 4:14 january 132:7 japanese 122:7 122:16 jargon 290:21 jerusalem 140:19 jim 96:6 109:6 154:2 159:19 164:20,21,22 278:3 jims 107:18 job 12:10 27:10 42:22 43:1 59:19 95:13 156:21 171:14 177:6 224:18 226:17 240:15 243:12,16,18 244:12 267:5 280:14 283:2 304:18 305:5 319:15 324:21 325:6 349:15
--	--	--	---	--

357:15	270:20 274:22	147:15,17	176:15 178:17	148:17,20,21
jobs 244:4	judiciary 254:11	keep 7:1 19:1	187:7 212:9	149:1,13 152:3
joe 6:22 7:16	judicial 29:12	27:17,18 28:12	214:9 261:11	152:7,11
joel 3:11 206:4,8	42:7 60:9	76:1 94:3	261:12 280:4	153:12,19
207:1,7 241:11	70:22 73:3	102:7 105:5	325:19 328:12	154:15,17
241:19 247:15	85:21 106:22	109:20 113:17	339:4 346:4	155:22 157:5
253:15 257:18	130:9,12	133:1 151:9	347:1 361:3	157:13,14,19
257:21 258:8	168:13 221:13	162:4 200:1	362:4 369:8	158:3,10
259:6,9,12	282:8	255:6 282:14	372:16 373:2	160:11 161:11
260:1 262:6	judicialmade	306:6 322:8	373:20	163:11 168:9
264:14 275:22	369:3	323:16 359:11	kinds 45:15 46:2	170:1,2,3
279:5 310:5	judiciaries	362:16,19	64:10 73:17	172:5,6 175:4
john 18:2 303:9	32:20	keeping 18:19	90:21 103:15	176:8,18 180:8
315:9,10	judiciary 74:6	49:10 64:7	161:4,5 219:20	182:3,21
316:11 348:7	117:7 179:16	316:1 374:20	249:3 264:18	183:21 184:21
356:11 366:8	193:21 210:5	kelly 6:22 7:16	280:3,5 308:13	189:22,22
join 316:17	julian 66:16	kept 18:22,22	349:11	190:16 191:19
joined 242:19	jump 356:12	19:8 22:5	kinetic 298:12	193:13 196:1
joining 205:16	378:12	49:10 94:6	klatch 77:3	197:9,16,18
206:14 225:22	jumps 366:11	336:7 341:7	knew 17:21 77:1	201:7,14 209:5
joke 321:7	june 137:4	key 22:20 37:7	77:1 180:4	213:18,20
jonathan 8:3	jurisdictions	48:16 62:18	191:10 202:17	214:17 215:5
jones 76:8 369:7	220:20	74:8 83:11	356:6	217:12 218:4
journalists	jurisprudence	128:22 193:11	knocked 120:13	220:18 222:17
115:4	15:1 292:14	208:20 214:1	know 13:14 23:7	223:22 240:22
judge 7:19 10:9	jury 54:8	218:9 252:5	23:11 24:19	241:18,20,22
25:9 29:18	justice 2:13 3:13	265:12 266:3	28:6,6 43:2	242:8 247:7
80:18 179:12	133:13 209:15	kick 206:22	45:2 50:1,14	248:14 249:5
352:12 372:8	213:2 215:12	kid 196:1	56:21 60:15	251:6,7,9,18
373:4,15 374:5	222:7 246:7	kind 10:11	62:9 67:11	254:14 255:16
377:11	364:15 372:15	13:20 15:17	69:21 70:4,13	256:16 257:12
judged 54:21	justices 225:5	20:4 22:1 27:6	82:12 83:6	257:15 259:18
284:9	justification	30:16 46:1	87:14,20 88:2	260:1,17
judgement	63:12 72:22	50:22 54:9	88:12 93:12	261:10,15
25:15	justified 260:16	57:22 62:9	95:1,11 101:18	262:16 263:6
judgements	366:2	64:6,14 68:10	103:6,7,19	263:19 267:11
32:19	justify 22:8 63:5	68:14,18 72:7	104:14,16	268:5 269:3
judges 352:12	63:6 106:10,11	81:11 85:14	105:15 106:2	270:6 271:7
360:20 373:11	315:4 317:7	86:18 91:13,14	108:5,10 120:8	275:18,18
373:13,18	justin 368:3	101:13,18,19	120:15 121:4	276:17 277:19
377:20		108:7 145:1	122:13 138:7	278:14 279:18
judgment 26:19	K	152:17 159:6	139:17 142:21	280:16 281:11
27:1 33:6	kaplan 286:3	159:13 160:22	143:17 144:6	281:18 282:4
214:7 257:8	katz 74:16 75:17	165:7,7 176:12	147:16 148:7	286:5 289:21

290:2 291:2,6	labs 144:4	8:19 18:3,4	230:18 301:11	learning 35:10
292:5 293:3,17	lack 48:11 56:3	22:8 26:18	302:2 321:4	191:1,8 205:14
296:22 304:1	127:16,20	42:12 51:10	341:7 343:15	251:20
306:18,19	193:8 253:3	65:9 69:10	lawsuits 129:10	leave 156:8
309:19,20,21	291:4 310:3	70:16 72:6	lawyer 80:3	186:15 187:8
312:1 314:18	344:8	97:12 112:6,18	135:1,2 247:22	187:12 224:2
320:15 322:5,8	lacked 122:3	117:5,6,8	305:8	319:13
322:20 325:10	lacking 327:11	124:22 131:6	lawyers 165:2	leaves 277:4
329:14,18	lacks 179:17	132:10,22	187:12 249:6	leaving 256:4
330:14 332:18	248:15	133:20 145:3	305:11 309:19	led 274:5 290:2
332:20 337:15	lag 121:18 122:5	145:11 146:11	311:13,15	lee 3:13 215:10
339:18 342:17	laid 46:11 128:4	147:4 168:4	354:14 378:3	215:17 216:7
344:2 345:4,14	landscape	169:1 177:10	layer 192:12	239:17 245:22
348:14 350:14	227:21	177:14 189:16	layering 82:2	263:11 267:13
351:2 352:6,7	language 222:18	191:6 217:3	layers 209:9	277:16 281:9
352:19,20	249:6 375:11	219:17 220:18	212:22 223:21	left 4:22 9:20
353:13 354:9	languages	221:7 223:4	lazy 187:8	187:18 286:6
355:16 360:14	158:18	224:14 243:20	lead 38:2 47:19	347:6 370:2
361:2,7,13	languish 359:14	247:18 248:1	164:2 217:7	378:19
364:13 367:16	lapd 182:7	267:15 272:16	328:20 330:7	leftover 259:8
368:1 369:8	large 37:11 40:2	282:2 287:3	331:21 335:15	leg 345:9
371:13,19	40:17 50:17	292:5 298:22	leadership	legal 13:19 21:9
374:11 376:4,5	58:20 62:1	304:6 309:20	238:13	41:3,7 42:7
377:19 378:4	66:20 67:5,6	311:14,21	leading 110:16	63:16 80:3,9
378:16,18	117:17 125:10	315:1,5,11,18	206:4	98:14 129:11
379:6 380:11	171:19 178:4	327:8 341:8	leads 47:13	132:16 150:4
381:19 382:22	211:10 246:6	343:6 352:6	206:10	174:3,5 191:7
knowing 58:19	248:2 302:18	355:1,18,19	leagues 197:5	216:3 230:4
227:6 241:16	333:10 371:13	356:5,8 364:6	leak 115:9	238:16,17
251:7 272:22	largely 235:1	364:8,12 365:1	leaked 49:13	247:18 272:18
338:6	289:10 307:9	369:14	leaking 115:3	292:4 293:7,14
knowledge	315:8 380:2	lawabiding	leaks 198:12	293:19 316:18
47:19 50:18,19	larger 61:2,6,6	133:10	leaning 33:1	334:14 348:6
105:21 176:6	83:20 249:19	lawful 189:6	leaping 101:4	348:12 354:11
288:9	330:3	260:15,16	learn 47:8	355:2 377:7
known 36:3	lastly 140:22	261:21 262:16	147:22 149:16	legality 187:13
76:6 138:2	191:11 333:4	265:6	190:22 191:18	legally 8:6 68:3
166:9	latanya 195:12	lawfully 209:1	197:21 311:13	243:2
knows 77:11	latent 117:19	laws 9:6 24:10	311:14 334:22	legislation
156:19 306:21	latest 40:9 112:3	48:17 103:19	341:22 342:8	303:19 378:19
337:10 380:20	latitude 51:13	129:14 144:20	learned 3:17 6:6	legislative 212:7
	laud 255:16	145:7 146:8,14	10:14 92:3	legislators 8:21
	299:10	168:22 178:2	230:10 244:9	legislature
L	law 2:15 3:18	216:4 230:16	285:5 304:19	192:21 193:4
label 152:12				

legitimate 9:7 86:12 147:7 231:10 292:22	203:5 205:10 206:5,11 207:16 209:2 209:13,19 211:3 215:11 215:14,18,21 216:1 217:17 223:17,19 225:12,16,18 226:6,9 227:2 227:18 229:5 229:14 231:1,3 231:13,14,18 231:22 232:4 232:18,19 233:5,10 234:5 234:16 237:6,7 237:12 238:10 238:12 240:3 242:15,22 243:8,19 244:10,13,18 275:7 280:22 282:22 284:13 289:20 295:17 295:21 296:3 303:10 304:18 305:5 310:22 317:10 334:1 349:13 351:18 353:8 356:21 357:7 358:21 383:20	likehealth 235:22 likelihood 31:7 likeness 5:10 likes 140:19 limit 40:14,16 68:6 90:9 106:6 112:15 124:6 143:3,4 143:22 178:10 178:17 293:15 293:19 299:1 336:21 351:3 351:11 372:10 limitation 329:7 350:13 371:9 372:6 limitations 28:1 226:12 297:7 297:14 312:9 312:15 327:15 342:7 350:8 360:3,5 362:13 362:20 372:21 375:21 379:18 382:17 limited 77:1 118:6 120:2 182:5 271:20 306:19 319:8 343:2 352:22 373:7 376:5 limiting 39:2 54:4 142:15 256:3 299:7 300:14 301:3 limits 22:3 38:14,17,19,21 38:22 141:18 292:17 330:16 351:20 line 44:21 67:19 75:7,20 108:3 120:8 159:17	256:15 259:14 326:1 341:15 347:18 lines 132:10 162:16 173:7 270:7 link 15:18 34:12 39:11,19 161:4 linked 91:20 linkedin 137:1 141:11 339:1 linking 49:1 90:21 links 35:3 90:5 90:22 list 10:18 83:14 83:16 84:19 120:14 288:12 listed 51:6,7 299:15 listen 166:10 listing 311:9 lists 55:18 literally 119:11 353:6 literature 40:17 little 45:14 47:15 53:21 54:19 57:18 60:2 83:1 92:18 110:7,10 114:21 146:1 159:3 162:19 165:19 179:19 190:21 199:20 205:20 217:9 218:18 220:9 227:1 229:13 233:16 248:10 252:2 262:15 270:17 271:7 277:4 288:8 305:14,18 323:22 330:12	347:5,14 live 20:4 158:12 191:15 205:14 245:17 livelihood 59:11 lives 12:4 34:6 49:5 151:16 379:12 living 126:5 283:14 356:22 livingston 1:22 385:4,16 liza 2:13 10:6 41:22 70:8 74:15 103:22 108:2 loaded 255:12 local 220:19 location 114:1 148:3 168:7 232:6 locations 39:16 lock 194:20 locked 306:15 306:15 locks 113:16 log 306:20 310:12 logging 308:10 320:20 logistically 285:22 logs 320:7,17,18 321:1,6 long 22:4,7 32:9 55:22 62:2 94:3 118:2 123:9 126:2 138:16 202:6 229:6 284:2 300:18 309:7 319:16 362:13 362:16 longer 40:6 56:2
---	--	---	---	---

118:8 138:15	339:2 340:17	83:6,18 86:9	loyalty 37:5	malware 189:1
158:14 191:10	340:22 347:13	88:18 94:11	lunch 7:4	manage 139:19
282:19 289:1	363:19 364:2	95:3 96:11,18	lynn 7:15	140:4 237:2
362:19	366:16 368:14	120:9 123:8	286:15	307:18 308:6
longestablished	371:5,12 373:3	138:12,14,17	lynne 1:22 385:4	310:4,13
118:5	373:21,22	139:5,14,16	385:16	342:18 350:2
longstanding	382:9	143:8 144:19		management
332:12	looked 50:15	144:20 145:3	M	127:3 234:11
longterm 59:6	160:16 281:13	145:10,17	m 1:14 4:5	248:21 290:18
look 11:16 15:21	looking 68:11	147:4,6,7	machine 35:10	290:19,22
22:19 26:8	89:6 90:21	154:9 157:5	machines 349:2	291:3,13,21,22
30:14 41:13	105:6 141:1	176:18 183:1	magicmarker	304:4 305:19
43:14 48:7,8	142:10 196:19	187:2 191:12	307:12	307:15,16
50:3,13 52:13	197:11 220:2	191:16 192:22	mail 107:14,17	381:16 382:1
52:15 59:16	236:19 240:17	193:14,19	main 36:16	managing
61:18,20 66:18	240:18 252:9	197:13 212:1	184:5 242:5	124:19 306:2
75:3,10 76:9	263:6,18 269:2	245:10 247:1	305:10 371:8	310:7
76:11 78:6	269:22 270:15	251:19 252:12	mainstream	mandate 5:19
82:17 87:17,20	282:8 288:18	262:19 264:15	10:22 229:9	231:5
87:22 88:4	320:12 321:3	266:2,5 268:13	maintain 191:2	mandating
91:9 95:15	339:6 341:13	269:8,9 273:5	191:3 208:11	165:22
104:16 105:6	343:10 357:19	273:7 275:5,9	214:11 370:16	mandatory
116:22 120:10	366:6 367:3,4	278:7 283:13	maintained 57:6	172:12
120:16 141:15	368:9 371:18	284:6 290:6	226:22	manipulate
156:13 157:7	372:2	291:13 292:1	maintaining	228:20
170:4,5,5,6	looks 15:16,22	304:1 305:9	140:9 190:3	manipulated
177:1 178:15	73:3 236:16	307:15 308:3,9	214:17,17	336:15 378:11
178:16 197:2,3	loop 183:20	309:3,13	maintains	manner 103:18
198:22 199:1,3	loophole 300:12	317:16 320:8	265:12	298:4 378:8
215:3,6 223:10	loosen 327:6	328:4 333:1	major 241:20	manners 21:17
223:18 228:8	loosened 378:6	342:10,19	262:1 298:14	manuel 217:22
233:15 236:22	los 182:7	343:4,7 344:6	298:21 330:19	map 343:15
240:20 243:18	lose 97:14	344:13 348:8	majority 53:15	mapping 155:9
250:21 252:2	257:10 268:18	349:18,19	64:20 253:12	marcos 250:19
256:11 257:15	losing 95:13	368:2 370:1	makers 349:12	marginal 73:16
258:1 261:13	148:13 270:11	375:20 383:11	making 7:17	marked 222:2
261:19 269:7	loss 16:5	383:16	18:21,22 32:19	markers 242:3
269:19 270:17	lost 16:4 24:10	lotion 35:9 37:6	35:15 100:18	market 24:5
272:2 273:17	326:5	lots 86:1 103:19	140:13 142:2	42:21 63:16
275:3 276:15	lot 21:12,13 25:2	220:2 223:21	148:17 154:7	marketing
276:16 310:12	43:11 47:4,6	loudly 154:4	154:14 167:9	127:6 172:16
311:5 320:22	48:12,17 49:12	love 189:12	199:5 246:13	320:4
321:6 322:3,7	49:17 71:18,18	low 305:17	249:8 265:11	marriott 1:13
329:19 338:22	71:20,21 72:5	lowly 357:11	379:21	4:7 206:17

247:21 264:8	103:13 121:20	237:4 252:1	medical 98:21	32:5 41:17,19
marriotts	144:9 149:20	265:20 268:1	99:5	74:12 101:6
206:19,20	151:5,8 157:17	286:7 289:6	medicine 304:9	109:9 110:4,5
marshall 18:2	160:7 161:20	295:6 299:7	medieval 76:21	110:6 122:19
marvelous 26:2	168:3,22 169:3	332:21 339:10	medine 2:3 4:2	123:4,13
maryland 385:5	180:17 184:22	339:18 352:22	4:20 74:14	141:17,21
mass 60:16	188:1,7,17,18	355:12 356:2,2	79:21 80:4,6	154:12 159:15
301:7 310:15	190:16 191:17	356:3 360:6	80:13 107:2	181:9 185:7,8
317:2 365:17	195:11 202:10	meant 180:5	108:19,22	252:16 254:8
masses 43:17	210:18 214:20	334:2 352:9	109:5 116:14	254:18 256:1
massive 195:2,5	232:9 244:19	measure 119:8	116:18 165:14	278:5 286:10
289:13 320:6	248:14 273:4	123:22 141:6	165:15 166:18	286:14 295:20
massively	277:3 282:1	221:11,18	167:18 168:16	347:20 352:13
335:20	289:10 290:20	345:18	169:8 171:9	378:21 383:6
match 85:9 91:8	291:3 321:11	measured	194:6,14,18	383:21 384:3
matching 12:19	327:18 332:15	291:18,18	196:7 203:4	mention 147:1
material 324:15	336:20 340:9	measures 23:21	264:2 268:9	210:6 220:14
math 235:11	340:10 353:6	23:22 68:5	284:17,22	290:3
270:1 283:13	354:13,18	112:8 163:22	354:6 355:7	mentioned 70:9
283:15 284:6	355:20 356:1	213:22 225:19	356:11 357:22	99:22 115:21
mathematically	367:10 368:17	276:3 281:5	360:10 363:1	125:1 142:22
113:9	369:19 371:3,8	mechanicism	383:3 384:13	144:21 153:7
mathematics	371:21 377:11	31:1	meet 39:4 238:1	172:19 177:8
269:14	377:22	mechanism 33:4	314:11	182:5 190:17
matter 12:17	meaning 138:3	89:22 178:16	meeting 4:4,6	193:6 212:20
80:4,5,8 90:21	248:15 277:21	212:10 263:15	5:17 116:12	219:16,22
98:12 149:2	326:3	263:22 319:18	117:1 193:15	221:16 223:2,9
208:7 242:1	meaningful	322:16 346:17	193:18 203:6	239:21 243:14
253:22 294:18	145:19 190:19	mechanisms	295:22 347:4	246:1 249:22
315:9 338:4	232:16 247:4	29:19 30:12	meetings 224:11	250:1 280:21
358:11 379:11	263:18 282:2	31:6 55:10	253:20	293:13 319:10
matters 5:2	290:10 299:9	56:8 57:7,13	meg 139:10	mentioning
118:21 124:5	301:1 329:21	63:17 86:1	mellon 251:8	223:20
215:14 338:5	331:11	93:1,8,20 95:2	member 6:10,11	mentions 89:1
mature 126:21	meaningfully	101:15 173:22	41:18 102:6	mere 78:14
maximize 61:17	333:2	210:22 211:19	110:11 134:14	170:6
mean 9:13 11:7	meaningless	212:4,16	141:20 192:2	merely 232:21
13:9 23:9,10	328:12	244:22 306:4	203:8 226:8	371:18
30:13 44:11	means 11:20	308:8 316:3,4	255:2	merge 34:2
46:21,22 52:7	13:4 20:14	319:1,7,15,19	members 2:1	merged 34:17
61:14 64:5	28:22 72:14	321:1 335:13	4:12,13 6:11	34:19 36:21,22
69:12,17 78:6	79:3 124:1,2,4	342:5,15	6:13 7:9 9:18	merges 34:13
78:16 84:18	187:16 189:4	media 338:14,22	9:21 10:12	merging 34:18
87:10 102:19	202:3 221:17	340:3	25:10 26:13,14	34:21 35:2

37:3,16	346:3	181:17,21	267:4	modified 88:3
merit 362:2	midst 316:14	minister 166:12	misuses 266:22	modify 212:4
380:12	mike 124:11	minorities 122:2	mit 251:8	modifying 85:5
meritorious	134:8 144:13	minute 109:2	mitigate 46:15	moment 316:2,2
362:17 365:20	149:5 167:19	110:2 140:3,3	92:20 225:2	323:20 324:1
merits 113:5	185:21	159:16 201:9	232:17 261:8	325:10 347:11
mess 8:7	mikes 164:20	217:11 284:18	262:2	347:11 362:6
messages 136:8	military 122:21	353:18	mitigated 20:21	369:18 380:17
messy 117:17	123:2 227:16	minutes 9:10,12	66:9	momentum
metadata 37:10	228:4	9:16,17 41:16	mitigating 93:1	178:14
102:12 103:4	million 361:1	74:11 76:1	93:4 280:17	monday 224:18
152:1,4,11,12	mimic 353:3	109:21 139:7	mitigation 92:19	money 342:20
190:18,18	mind 56:5 82:20	141:19,20	mobile 135:21	monitor 122:16
metaphor 260:7	101:13 121:8	205:20 217:7	136:4	monitoring
method 106:12	145:13,16	278:10 286:1,5	mode 58:12	343:21
160:8 218:11	180:22 201:4	286:9,10	model 35:21,22	monitors 22:12
267:11	306:6 318:15	misbehavior	83:5 115:12	months 95:14
methodologies	336:7 346:9	27:21	118:14,19	311:20 379:11
237:5	366:12	misconception	121:9,11,13	moot 78:14
methodology	mindful 146:14	119:3	135:10 155:7	moral 121:18
59:4	182:4	misconduct	155:19 157:22	122:5
methods 35:5,10	minds 148:15	31:15 192:15	modeling	morality 27:18
40:18 62:16	mine 199:15	misinterpreted	111:14 114:15	morning 4:2
89:8 91:21	259:7 271:8	22:16	114:19 115:19	18:5,6 109:9
92:6 182:21	minimization	mismatch	182:9 183:3	109:10 110:19
214:18 218:16	272:12	351:13	199:20	117:9 184:17
219:3 267:2	minimization	mismatched	models 114:19	202:22 203:13
metric 165:7	118:7 126:1	346:18	182:19,22	203:19 204:7
mic 318:16	221:16 233:8	misplaced 13:18	183:2 261:11	234:1 245:11
323:21	297:7,16 300:4	missed 173:5	261:12	255:21 268:12
michael 3:6	300:5,6 301:18	184:12	moderate 193:7	285:13 287:14
190:16	327:14 328:1	mission 216:20	moderated 6:9	mortal 313:20
micro 28:22	329:9 358:9,14	227:5,22	7:19 203:8	mosaic 36:13,18
microphone	359:3,4 372:4	298:13 304:13	moderating	47:11 75:13
203:15,18	376:2	383:18	109:6 285:8	76:7 77:9 78:5
375:15	minimize 106:5	missions 215:15	moderator 6:17	80:11 89:1,2
microsoft 3:6	204:20 361:13	298:7	9:16 286:8	89:10,12,18
124:12 125:2,3	382:10	mistake 55:19	modern 32:11	97:5 383:14
144:14 149:7	minimized	93:16 316:15	97:21 186:4	mosiac 268:13
149:10 150:17	358:3,5	mistakes 173:11	329:11	mother 13:8,12
150:17,20,22	minimizing	174:17 213:9	modest 58:19,21	motivated 99:12
151:1,2	62:14	misuse 56:21	91:4	motivations
mics 318:17	minimum 62:20	86:6 94:18	modifications	44:9
middle 92:18	mining 47:9	misused 55:17	85:14 374:12	motive 44:17

mount 141:5 170:13,20	201:13 202:15 naïl 150:12	257:1,10 280:1 285:7 294:10	208:21 259:17 290:11 300:18	312:5,7,9,12 312:13 316:5,6
move 19:10 96:6 116:6 236:16	naïve 166:17 naivete 355:15	296:3 297:20 297:22 298:8	301:22 317:8 345:5,6 370:16	317:13 319:6 319:13 320:13
270:9 301:6 383:18 384:10	name 5:10 237:13 306:20	298:18 299:8 302:5,7 310:19	necessities 86:7 necessity 54:17	320:14 321:17 331:5 345:15
movements 15:2 148:8	names 175:13 194:9	327:11 330:19 331:3,12	204:11 208:9 317:6 345:3	347:7 348:2,3 348:5,5 349:5
movie 160:17	nara 222:5	335:11 367:9 375:19 381:21	362:14 366:3	349:12,15 354:7 355:17
moving 89:21 94:15 96:15	narrow 18:15 19:10 53:15	383:19	necesssarily 218:21	355:21 359:12 360:8,9 373:2
219:7 305:16 318:15 369:10	65:4 72:3 365:12	nationality 231:9	need 23:11 24:20 26:6	377:18 needed 40:21
370:13	narrower 360:1	nations 111:22 112:19 325:20	28:22 29:6 32:1 46:2 47:1	118:14 217:14 243:18 282:21
multifaceted 173:14	narrowing 300:14	365:18	47:21 52:13,15 53:14,16 62:10	300:15,20 307:4 359:7
multihop 90:22	narrowly 31:5 45:18 366:1	natural 26:18 106:15	63:4 66:7 67:1 67:4 68:16	needing 95:22 needle 257:5,7
multilaterally 153:13	nation 23:4 111:2 115:2	naturally 378:21	83:10 89:11 90:3,4 93:17	needs 39:4 54:16 66:2,3
multilayered 173:15 358:20	116:13 189:19 209:3 226:11	nature 32:15 58:11,22	93:20 94:3,10 105:4 113:22	67:15 85:9 90:17 116:13
multinational 343:13	226:21 227:11 228:4,6,9	188:19 226:14 229:1 230:19	109:18 127:21 130:10 132:8	128:2 133:8 134:1 167:17
multiple 308:20 308:20 360:19	234:20 302:2 national 3:11,14	333:18 336:1 379:6	133:6 134:3 143:15 146:13	179:18 193:1 195:9 204:5
370:5	8:17 10:8 46:2 53:22 64:6	naval 313:10 navigate 335:17	146:19 155:4,7 168:12 170:9	236:17 254:2 259:1,10
multivaried 32:15	66:13,18,20 67:4,5,6,9	near 308:5 nearly 124:21	170:17 172:7 174:18 175:2	273:20 281:6 311:3 374:8
music 135:8	69:10 81:1,12 84:13 85:9	necessarily 24:15 98:12	176:12 183:1 187:11 190:9	nefarious 112:2 negative 20:10
muslim 16:18	89:9,13 104:10 111:15 112:18	155:4 168:21 182:8 184:8	193:16 194:4 198:8 200:13	35:19 175:7 204:20 291:8
muster 332:4	123:22 129:14 129:18 133:20	190:9,15 218:20 275:15	210:16 214:8 214:21 234:17	291:17 312:22 381:17 382:8
mutually 155:21 296:22	162:16 176:13 181:15 200:11	279:2 284:7 305:9 315:4	245:5 254:18 257:4 261:21	negatives 56:12 negligent 95:10
mysterious 369:9	204:5 206:6,12 218:15 219:19	333:13 338:11 365:4 376:8	265:2 267:4 270:19,19	neighborhood 183:12 184:20
mythical 331:7	222:6 223:2,3 223:4 225:11	necessary 31:7 40:20 55:3	283:15,16 294:11 309:21	neighbors 148:22
	225:22 226:15 246:19 256:21	57:22 161:13 178:11 192:8	310:3,8,9	
N				
n 1:13				
nahari 3:7 134:15,20				
154:17 155:1 158:11 169:22				
182:3 189:9				

neither 44:17	84:19	89:21 99:1	nsas 15:14 23:14	obligation 86:20
nervous 80:8	noncontent	155:16 156:10	225:17,20	240:13
355:8	152:1	167:11 190:17	226:6 227:2,5	obligations 38:9
netflix 160:15	nonexistent	201:17 289:15	227:18 229:14	obscure 14:20
161:10 195:11	307:6	363:6 370:20	229:17,20	15:5
network 197:16	nonintelligence	374:1	231:1,15	obscurity 5:3
199:7 369:16	231:17	notions 196:20	314:20 351:18	15:8 74:19
369:16	nonpregnant	197:6	nuance 29:1	76:19,22 77:5
networks	35:21	notwithstandi...	348:21	observation
131:10 197:22	nonstate 228:7	369:8	nuanced 307:20	15:4 27:14
neutral 374:2,16	nonstatutory	novelist 8:3	368:5	30:1 78:9
380:4	300:9	november 1:7	nuclear 60:4	observations
never 55:16,16	nontechnologist	4:5	227:12	176:10 257:19
55:18,19	137:7	novo 53:6	nudge 39:2	287:22
120:16 164:1	nonu 132:9	nowadays 40:7	number 17:13	observe 293:20
303:17 326:5	282:9 301:8	nsa 3:20 13:11	37:5 66:4	observed 5:5
351:7 354:1	302:11	81:4 82:5	141:6 149:19	79:10 337:15
nevertheless	noon 7:5	84:11 103:8	153:21 164:5,7	obtain 81:20
131:11	normal 15:4	104:7 130:20	164:9 172:8,9	131:2 221:8
new 25:15 47:8	78:9	164:3 165:3	172:11 173:6	227:5
50:18,18 76:14	normative 167:4	172:2,4 177:3	189:19 198:13	obtained 223:11
78:18 118:14	notable 234:8	177:9 225:15	200:17 287:4	266:19 280:11
118:19 132:16	notarial 385:12	227:14,22	320:19 363:4	352:4
132:17 140:9	notary 385:4,17	228:1,8,10	numbers 91:12	obtaining 261:4
143:4 145:18	note 6:21 28:14	230:3,10,14	91:19 175:15	262:19 265:8
157:14 158:15	75:22 78:3	231:20 232:4	175:15 194:9	266:6
172:2,3 177:8	116:1 179:13	233:3,6 234:2	229:10	obvious 11:19
190:9 191:9,11	noted 81:2	238:10,13	numerous 88:22	39:22 42:14
209:20 225:13	358:1	248:17 250:14	nuts 96:1 354:12	348:11
230:4 231:4	notes 61:9	251:1,17,22,22	nvidia 3:7	obviously 28:2
241:9,9,10	nothings 173:13	269:13 270:16	134:16	43:5 63:16
250:1 260:13	notice 83:8 84:2	275:12 276:8	nypds 16:18	81:7 89:2 95:3
260:13 271:22	84:17 272:5	283:13 284:1,6		99:17,18
273:2 330:18	289:11 290:6	301:13,15	O	102:20 150:13
364:9	290:10 312:14	313:6 314:14	oath 244:4	154:15 163:7
newer 340:5	328:6 329:5	316:13 319:14	obama 132:7	176:9 194:14
newly 209:12,18	332:13,19,21	320:8 323:1	obfuscate 68:7	194:21 204:2
news 16:17	343:4	325:16 330:11	objected 339:5	221:6 223:18
163:19	noticed 203:13	333:21 351:6	objection	241:15 272:7
nice 225:9	326:12	351:15 357:4	339:14	272:16 273:9
235:12 325:8	notified 84:6	360:16,21	objective 86:5	276:20 297:5
nodding 97:10	notion 8:2 55:4	364:2,13,19	219:2 223:12	311:8 341:22
98:2 107:18	69:7 80:17,20	365:9,14	objectives 27:5	342:11 350:11
nofly 83:14	81:11 82:3	380:16	obligated 309:9	367:11,12

occasion 148:5	223:8 244:5,8	364:8	228:2,11,14	opposition
occur 37:3	244:11 264:5	older 322:10	operates 130:4	69:18
occurred 228:21	358:22	omg 354:8	operating	option 197:18
occurring	official 224:10	357:20 358:19	210:21	328:10
185:18 187:22	239:22	359:21	operation	options 39:22
240:16	officials 3:10 6:4	once 29:16	204:12 374:14	90:8,12 308:3
occurs 110:8	8:21 15:13	157:19 186:3	operational	308:4,6
184:1	23:7 66:5	191:1 258:22	28:20 32:2	oral 120:3
october 4:10	204:1 205:5	293:8 300:8	85:9 86:7	318:21 326:18
odd 294:11	215:21 232:10	321:1 351:1,2	218:19 315:18	order 4:16
odds 69:7	383:9	ones 5:2,6,10	operations	68:10 70:12
315:12	oftentimes 48:1	13:4 42:2,10	215:15 217:20	90:5,18 109:18
odni 239:1	218:21 358:5	51:11 57:17	217:22 225:9	130:4 159:17
244:20,21	oh 136:9,11	83:19 85:8	227:16 313:11	196:13 208:12
249:15	187:8 189:11	94:20 163:7	355:17 373:9	217:13 221:8
odnis 206:10	199:6 201:11	210:3 252:17	operators 239:6	221:14 229:18
oecd 329:4	207:3 262:6	272:10 273:17	316:18 334:15	238:14 254:2
offensive 111:1	305:2 355:3	279:16	334:16	254:18 257:5
offer 32:14	ohm 195:12	ongoing 142:19	opine 253:6	259:1 265:2
33:18 38:14	ohms 311:11	263:16,16,22	opinion 80:3	279:1 301:5
63:11 86:22	okay 18:1 33:8	online 16:10	148:6 199:12	323:9 324:14
257:19 287:21	41:15 42:13	34:9,10 39:12	368:19 369:9	orders 128:9,9
offers 39:21	45:10 52:4	39:19 69:1	375:2 380:5	128:20 129:18
291:13 357:15	67:17,21 82:21	125:8 151:10	opinions 301:22	129:22 169:3
office 3:11 206:6	83:3 87:7	152:9,13	374:10	301:22 325:18
206:11 215:16	88:11,13 102:1	160:16 161:10	opportunities	ordinary 128:13
215:22 238:3,4	102:2 103:21	onset 177:17	91:8 226:19	228:17
238:5,7,10	105:9 106:14	ontological	opportunity	organic 326:3
240:1,6 243:14	106:17 108:16	26:15	6:12 25:11	organization
243:15 244:6,7	134:11 159:14	onus 63:5	33:17 96:5	115:13 234:3
245:4 246:5,19	161:8,9 163:1	open 54:16 55:3	110:20 117:10	244:21 252:4
351:18 354:20	164:14 167:18	107:14,16	124:16 134:20	264:21 265:7
officer 4:11	179:22 180:16	219:10 286:11	230:22 237:14	268:3 308:12
120:12 171:18	194:14 201:4,8	318:6	237:18	320:8 357:17
172:3,4 206:5	207:7 255:8	opening 4:17	opposed 43:22	357:19
206:21 215:11	257:18 259:6	109:15,20	44:19 54:8	organizations
223:18 225:13	267:13 274:7	157:22 172:6	70:22 192:19	34:7 38:7
226:7 239:12	275:20 277:7,8	237:21 340:10	251:6 263:19	106:19 107:6
officers 56:20	305:2 354:14	openly 122:20	277:9 287:22	232:2 264:19
203:2 243:7	357:15 369:14	123:12	318:5 338:8	304:13 310:8
264:18 265:10	369:20 383:1	operate 95:22	355:22	320:16
349:12,14	old 106:21	126:10,18	opposite 11:21	organizing 63:8
offices 209:11	117:20 137:22	208:9 346:8	214:14 243:10	orient 217:1
209:11,13	247:12 259:7	operated 204:19	355:20	orientation

216:15 oriented 114:18 originally 175:13 ought 42:11 63:15 75:18 229:7 344:17 359:6 outcome 385:11 outcomes 291:10 outcry 298:15 outdated 25:21 outlined 101:21 outputs 143:14 outset 332:14 outside 10:21 13:17 29:18 31:4 43:5 57:20 59:4 94:16 95:4 116:19 194:1 209:13 230:14 353:7 355:13 369:18 373:3 373:20,21,21 overall 112:19 114:5 200:8 261:13 262:3 263:2 301:6 overarching 23:3 49:21 overcome 68:20 overlapping 296:22 overlook 331:13 375:7 overlooked 173:5 overly 353:11 overrepresent... 184:2 override 65:2 overriding 12:6	oversaw 303:13 overseas 229:22 oversee 41:4 254:18 oversees 215:17 oversight 1:3 4:3 21:19 24:12,17 30:11 31:19 38:4,22 41:7 42:7 52:12,16 71:12 72:19 73:2,18 73:19 94:11 95:21 96:5 130:9 157:2 165:10 169:4 174:17 177:5 178:1 179:15 192:4,6,14,18 193:2 194:5 203:5 207:13 209:6,7,17,19 210:1,6,7,10 210:12,14 211:1,18 212:16 219:15 219:16,20 223:2 225:17 238:22 239:19 241:17 244:8 246:1,3,17,18 247:4 252:18 253:2,10,14,15 253:21 254:3,6 254:22 276:16 276:19,21 277:17,21 295:21 306:4 307:5,15 308:8 318:19 319:5,7 319:9,12,15,18 319:22 321:12 321:14,19 322:16 324:21	338:1 342:21 349:12,13 375:18 376:2 383:13 oversights 30:10 56:8 overtime 327:12 overusing 190:17 overweighing 73:13 overwhelming 144:17 319:4 ownership 70:3 <hr/> P pace 341:8 page 241:10 pages 119:13 163:1 220:8 paint 36:15 pairing 173:22 paladin 3:20 313:5 palantir 303:10 304:2,4,11,20 305:19 309:9 309:11 311:10 320:15 338:19 349:4 367:8 palm 136:11 panel 6:6,9,19 7:18,20 10:2 26:14 31:14 32:5 41:17 69:22 85:21 88:16,18 96:10 102:6 108:17 108:22 109:3,7 109:10,11 110:8,12 119:3 134:14 135:6 142:22 155:3 164:21 171:11	171:13 179:9 181:10 185:10 199:10 200:5 202:22 203:1 203:21 204:22 255:21 256:1 269:11 276:20 278:5,10,17 285:3,4,13,16 285:17,17,18 287:14 288:3 288:18 310:5 319:11 333:12 333:13 341:17 347:20 363:6 363:22 383:4 panelist 9:9 165:16 252:22 286:1 295:14 303:9 313:4 panelists 6:17 6:18 7:1 9:3 10:4 25:19 64:17 79:7 88:7 105:11 154:13 185:10 203:7 206:3 275:21 285:10 286:2 313:12 318:10,14 384:3 panels 5:20 116:5 140:7 178:12 179:9 199:10 206:16 286:13 313:18 383:4 paper 271:13 276:18 306:13 319:1 papers 12:21,22 42:3 paperwork 192:12	paradoxically 361:15 paralyze 379:3 pardon 119:19 parentage 303:20 parents 303:21 parker 7:15 286:15 parking 137:1 part 11:20 49:9 55:11 65:16 67:13 82:10 83:22 86:3 87:10 107:22 108:17 120:10 137:11 155:9 172:1 178:15 207:15 210:14 212:8,15,19 214:1 215:16 216:20 224:22 225:4 227:5 232:19 233:6 240:15 241:2 243:18 244:4 247:8 250:5,12 262:20 274:20 277:3 280:22 289:8 291:5 298:12 320:13 339:2 346:4 372:5,7 partial 71:6 participate 10:13 124:17 299:6 participated 360:17 participates 362:18 participation 19:3 80:22 82:3,9,16 86:3
---	--	---	--	--

163:8 221:5	94:13,15	10:2,17 11:22	252:19 255:20	70:10
271:18 272:8	230:17 233:12	15:20,21 16:4	260:4 262:19	perception
274:9 326:15	250:17 273:15	16:7 17:3,7,8,9	263:5,17	253:4
326:22 327:10	360:13 371:19	17:13,19 18:9	264:18 266:18	perceptively 8:4
327:19 328:14	372:19	18:10 19:1,2	267:2,19	perfect 111:11
329:9,18	party 150:16	20:9 21:5,22	278:19 283:13	114:4,7,12
particular 9:8	151:6 168:17	22:6,17 23:5	284:5 294:18	115:18 133:18
21:15 29:2	361:22,22	23:17,20,21	294:20 303:17	160:2,5,10
37:8 40:19,22	pass 187:20	24:3,6,7,7,9,16	304:2 309:21	161:21 162:3
41:18 49:2	286:19 332:4	34:4,7 35:6	310:3 312:9,11	173:13 194:21
65:10 66:21	364:7	37:1,21 43:2	319:13 321:15	213:8 241:12
67:2,2 86:17	passed 145:8	44:10,13,18	321:15,17	perfectly 70:4
94:1 102:6	230:16	47:19 48:11,17	322:1,4 328:18	100:10 354:11
121:22 129:5	pat 255:7	49:12 54:17	329:14 330:15	perform 38:10
181:1 192:1	path 276:11	56:1 58:1,16	332:18 338:16	104:22 254:3
204:13 208:4	paths 91:9	58:20 59:18	339:10,20	254:22
211:15 214:4,9	patricia 2:5 4:15	64:2 65:22	342:22 345:11	performance
216:13 220:14	patriot 103:5	68:1,5,8 69:20	346:14 352:4,8	134:17
225:10 240:12	301:12	70:1 71:5,6,9	354:22 355:1	performed
241:3 245:2,19	patternbased	74:8,18 76:15	357:20 361:1	233:11
248:17 249:14	181:16,20	79:3 81:18	363:17 368:3	performing
280:9 281:16	paul 2:14 25:4	83:6 95:8 98:6	379:17 381:2	254:17
286:16 315:14	64:12 68:15	99:3 104:2	peoples 12:4	period 138:17
323:19 328:1	69:4 98:2	113:14 120:12	18:19 21:3,4	196:11 206:2
333:20 335:9	100:18 106:14	120:18 122:2	23:16,17 42:20	periodically
particularly	195:12 311:11	123:8 132:1	45:5 47:18	241:8
278:9	pauls 40:4	133:9 146:9	53:9 57:2,5	periods 15:2
particularly	pausing 81:15	147:21,22	59:10 128:13	93:2
47:5 109:10	pay 243:8 286:6	148:5,17,21	148:15 150:9	permanently
124:7 151:13	287:12 336:16	149:16,18,20	151:16,18	196:16
168:2 203:14	paying 157:4,5	151:8 152:20	153:3 198:17	permissible
210:8 240:22	pays 190:7	153:8 160:18	209:2 373:10	238:17
244:6 245:8	pbgc 106:20	163:18 166:22	379:12	permission
246:3 285:19	pclob 110:6	172:16,17,20	perceived 213:6	348:10
289:16 294:10	114:9 116:2	173:7 178:5	315:13 317:19	permit 29:10
334:16 342:7	159:9 279:18	180:7 183:15	percent 16:9	299:9
parties 42:17	295:6 303:1,19	184:13 197:3,4	39:18 43:3	permitted 130:2
63:13 91:3	318:8 353:6	197:15,18	56:4 70:12	222:16 243:2
151:18 153:22	355:6,10	198:14,20	93:17 157:10	294:3 314:22
375:9 376:21	358:22 361:6	199:5,22	157:10 159:13	permitting 6:16
385:10	382:21 384:9	200:19 214:7	163:19 196:22	perpetrators
parting 108:18	penalties 222:22	242:11,20	198:16 363:13	183:16
partner 313:5	pension 107:2,3	243:11 247:1	379:1	persecute 44:10
parts 47:11	people 6:15 9:22	249:11 251:7	percentage	persecution

55:18	33:19 94:15	phones 112:3	335:16,20	70:7 78:13,14
person 12:20,21	97:7,8 124:19	135:22 139:5	345:11 352:5	79:4,8 81:22
15:9 34:15	135:7 137:12	363:17	357:10,10	91:10,10 93:6
79:12 97:14	184:6 208:8	phrase 363:4	361:8 364:19	96:19 100:22
98:9 103:6	216:17 219:6	366:9	placed 39:17	101:5 102:12
120:14 150:15	220:7 229:14	phrasing 260:21	376:20	108:2 120:4
230:2 238:19	244:14 251:5	physical 336:21	places 5:8 29:15	123:15,17
240:6 256:13	254:15 265:17	physically	108:8 149:1	142:2 144:14
256:15 269:5	266:16 270:12	170:10	305:4 311:12	146:22 147:15
278:22 279:3	270:13 273:14	physicians	planning 159:22	159:15 162:21
289:20 294:16	277:17 280:1	122:22	platform 220:17	179:12 183:2
311:1 376:8	280:15 334:10	pick 106:16	304:5	189:2,10
personal 5:1,11	338:14 360:16	297:3 326:20	platonic 49:22	192:13 238:11
14:10 17:10	360:21	picking 203:18	72:2	245:3 246:1
20:13 27:18	perspectives	picture 36:16	play 73:21 74:7	256:19 257:2,9
43:12,21 51:11	232:9	123:7 156:16	74:7,9 83:12	257:9,22 258:6
118:21 127:8	pertain 315:6	156:20 170:18	172:17 272:21	260:3 275:15
133:9 136:9	317:4	249:13 261:13	373:8 375:18	277:12 286:8
228:18 229:1	pertaining	piece 64:8	377:1	290:8,13 292:1
231:11 232:3	225:16	203:12 222:3	players 209:9	300:7 305:22
235:4,14,17	pervasive 30:22	256:13 324:2	playing 73:21	307:17,19,19
236:7,7,11,13	341:2	371:5	239:1	308:8 310:14
242:17 254:15	pervasiveness	pieces 47:5,15	plays 12:4	310:14 315:8
265:8 368:19	30:19 186:10	76:12 263:20	315:16	316:22 319:11
personalities	pessimistic 8:8	306:13	plcob 7:8	323:14 324:13
54:18	peter 6:14 7:16	pierce 15:7	pleasantly	335:9 350:7,9
personality	ph 110:14	pike 341:1	242:19	354:7 356:15
37:13	145:19 284:6	pilot 249:22	please 4:17	361:14 367:12
personally	phase 78:22	pioneers 205:8	110:18 134:19	371:8 377:6
85:18 160:21	218:7 258:1	pipeline 34:1,13	154:14 201:12	pointed 64:12
178:3 229:8	346:1,21	35:4	286:6	75:12 195:11
243:5 247:16	phases 37:17,17	place 42:18 96:2	plenty 16:4	252:18,22
249:10	255:19	137:1 144:20	78:21	pointing 306:5
personnel	phenomenon	178:5 180:4	pllc 2:14	points 18:6 71:4
126:22 127:6	142:10	209:22 232:3	pockets 139:6	76:18 77:13
persons 15:1	phishing 339:3	233:14 242:3	point 15:12 16:2	118:20 252:12
29:15 66:21	phone 37:10	245:19 252:8	16:3 18:7	277:21 307:13
67:2 78:10	90:15 91:3,12	267:3 269:5	19:12 20:12	309:4 346:1,21
113:21 118:22	91:18 135:21	270:22 272:7	22:21 23:19	police 56:20
131:18 132:1	136:1,4,5	273:11 275:3	35:15 39:21	57:3,5 120:12
164:5 231:7,10	166:8 170:12	275:14 288:22	49:21 51:21	183:10 185:2
279:3,21 282:9	194:8,12	300:2 323:7	57:19 60:9,14	policies 38:8
301:8 302:11	278:19 301:14	330:10,22	60:17,20 66:12	83:7 95:20
perspective	301:16	331:7 333:1	66:17 69:5	119:9 125:15

125:16 129:3 144:20 145:8 214:15 215:4 216:5 230:18 234:14 338:21 348:5,12 367:1 policy 25:8 33:14 41:3,7 80:4,5,8 110:17 113:4 113:12 115:5 142:13 145:2,3 174:13 175:5 240:12 251:4 257:8,14 259:22 282:10 315:5 322:6,11 327:6 329:17 339:3 342:3 349:11 350:4,5 352:21 360:15 362:6,8 380:6 polishing 182:19 political 44:14 45:3 122:3 politically 44:19 327:5 poll 16:8 197:1 363:12 pollution 20:19 pool 46:10 pop 269:19 population 36:4 371:10 portion 250:15 portrait 47:11 pose 6:12,17 41:16,18 159:15 181:14 185:5 255:22 368:16 poses 6:11 position 70:4	169:6 206:21 216:18 238:13 239:18 positions 242:12 264:11 268:1 positive 27:2 35:18 128:1 129:4 229:6 291:10,16 293:22 354:19 positives 56:12 56:14 58:16 positoin 273:8 possess 305:9 possessing 302:15 possession 202:18 possibilities 169:19 possibility 56:17 56:19 87:5 110:4 141:21 142:18 345:15 365:21 possible 7:17 56:10 57:1 118:2,3,15 143:14 156:19 157:1 174:16 235:6,16 236:3 236:6,8 348:18 349:16 378:8 possibly 102:7 186:9 343:1 377:8 post 70:22 130:19 197:1 363:12 postal 106:20 107:13 postchurch 85:13 postcollection	87:14 118:17 121:10 posted 384:8 postindustrial 76:19 posting 191:16 posture 111:22 potential 30:18 115:7 142:14 144:7 169:17 174:15 234:18 265:4 268:20 291:17 348:8 381:17 382:7 potentially 222:20 253:1 370:17 power 21:12 36:18 44:7 122:3 302:14 302:16,21 306:7 337:5,12 337:22 357:17 powerful 117:15 124:5 163:10 167:6 337:13 337:14 357:11 powers 15:4 78:9 111:16 314:7 375:9 378:5 ppd28 231:5 practicable 162:7 practical 12:17 74:18 76:18,22 77:5 92:10 106:5 113:13 113:19 115:16 159:4 171:15 235:7 292:20 358:11,14 practically 14:19 15:5	242:6 373:16 practice 38:1,16 63:15 100:2 106:6 114:10 146:7 204:9 205:8 287:19 296:9 303:3 314:4 315:18 354:9 364:12 practices 33:20 33:22 39:7 62:8 63:6 108:13 111:21 112:12 125:21 193:1 197:22 231:21 296:20 299:11 practicing 267:15 practitioners 316:18 pre 70:22 pre2007 137:22 precedent 150:14 precise 34:19 35:2 168:7 307:11 precisely 99:10 182:13 307:19 precision 34:21 38:15 predicated 219:8,14 221:21 223:9 predication 219:1,10 predict 36:8 37:20 145:20 183:3,21 184:19 prediction 182:11 predictions	37:12 183:13 predictive 35:5 35:17,21,22 182:9 183:3,13 184:9,15 preerror 95:2 preferences 33:5 pregnancy 35:9 pregnant 35:20 37:9 prem 286:16 premise 96:21 96:22 98:16 158:8 186:13 186:14 282:18 283:1,3,7,9,12 313:18 premised 98:22 premises 81:16 prepared 7:7 63:10 preprocessing 62:14 prescribed 362:21 prescriptive 221:18 present 4:12 68:10 227:3 268:16 336:22 presentation 380:18 presented 249:9 president 60:12 128:17 132:7 presidents 23:15 50:14 231:5 presiding 4:11 press 31:9 131:12 pressured 13:15 presuppose 283:19
---	---	---	---	---

pretend 197:8	297:8,16 300:4	24:14 25:2,14	126:15,17,21	217:5 218:5
pretext 44:18	328:1 332:16	25:20 26:6,7	126:22 127:10	220:12 221:1
pretty 77:2	principled	26:11,15,19	127:11 129:1	221:10 222:12
90:20 113:17	237:5 268:3	27:3,8,13,20	130:7 131:17	223:17,19
159:11 162:3	principles 61:9	27:22 28:2,6	132:2 133:14	224:10,12,15
193:3 194:20	61:10 64:10	28:11,16,17,19	133:16,19	224:21 225:2,6
195:17 199:4	84:12 86:17	29:3,10,20	134:1 135:10	225:12,16,21
343:22 381:16	100:2 134:4,6	32:15,16,20	142:18 143:13	226:2,7,9
prevent 126:14	164:12 180:1	33:16,21 36:6	143:17 144:7,8	227:2,19 229:5
131:8 174:17	192:18 204:9	36:17 40:13	144:15 147:5,6	229:15 230:12
175:1	231:21 234:22	42:1,5 43:3,19	147:9,12 148:1	230:13,16
prevention 85:3	272:1,17,20	45:8,13,16,16	148:14 149:4,9	231:2,3,10,13
previously 229:2	273:3 274:18	46:8,12 47:18	149:11,14,20	231:14,18,22
previous 119:10	276:10 288:12	48:1,5,17 49:9	150:1,3,9,15	232:5,9,18,20
155:3 171:13	296:9,21 303:4	50:1 52:7,15	150:21 151:3	233:5,10,11,17
179:9,13	317:3 332:9	52:20 53:22	151:19 152:15	233:18 234:6,7
252:22 276:20	principles 220:5	54:9,13 55:2	152:21 153:5,9	234:9,14,16,18
278:17 286:13	prior 45:14	58:2 59:14	153:22 154:18	234:22,22
287:4 319:11	184:3 199:15	61:5,12,17	154:20,21	235:8,13,18,21
363:6	206:14 225:22	65:2 67:7 69:1	155:5,11,16,16	236:18 237:6,8
previously 90:5	264:11	69:17,18 72:2	156:11 157:16	237:11 238:10
117:6,17,20	priorities 227:8	72:11 73:6,8	166:19,22	238:12 239:12
148:5 228:2,11	priority 200:7	74:16,17 75:4	167:3,9,12,21	239:22 240:2,3
303:11	201:15 227:10	75:10,18 79:3	171:18,21,22	240:8,19
price 336:13,16	prison 104:6	79:4 83:7	172:2,4,10,18	242:16,21
pride 303:19	137:1	86:13 87:21	173:4,9 174:4	243:9,19
primarily 111:6	privacy 1:3,5	96:21 97:6,15	176:7,20	244:11,13,18
119:4 121:9	2:10 3:2,4,10	98:1 99:2	177:17 190:4	246:12,14
202:8 229:16	3:10 4:3,4,21	101:15,20	191:20 196:20	247:3,6,18,22
326:17	5:14,19,21,22	106:19 107:6	197:7,15 198:7	250:5,7 252:1
primary 94:18	6:4,4 7:22 8:2	109:11 111:4	198:20 199:2,6	255:18 256:2,5
256:2 324:19	8:4,10,13,19	111:13 112:19	199:8,17,20	256:8 257:1,11
346:9	8:22 9:5 10:15	113:7 114:5,18	200:8,10,14,14	258:12,18
prime 166:12	10:16,19,22	114:21 115:15	203:2,5,6,22	259:16 261:12
princeton 2:12	11:5,9,15 12:9	115:19 116:10	204:1,4,8,10	264:4,9,18
33:12,13	12:11,13,15,16	116:12 117:4,7	204:21 205:2,6	265:10 267:16
principal 94:18	13:3 14:4,7,10	117:12 118:5	205:10 206:11	267:20 269:5
215:12	15:10,11,19	118:12,13,16	206:16,19,21	269:22 270:4
principally	16:22 17:6,8	118:22 119:5,8	207:16 208:2,3	270:11 274:3
56:13 59:3	18:7,9,13,14	119:18,22	209:2,13,19	275:7 276:4
principle 23:3	18:14,15,17,18	120:12 121:1,9	211:2 215:10	277:6,7,15
61:20 62:7,18	18:19 19:9,11	121:14 124:2,6	215:13,18,20	281:1,4,10,11
86:21 202:14	19:13,15,16,22	124:11,14,19	215:22 216:4,5	282:6 284:13
221:6 254:1	20:3,6 22:22	125:4,4,6,19	216:13,16	285:5,14,15

287:5,18 289:6	224:13 225:18	proactive	51:17 72:17	procurement
290:5,7 291:1	private 3:17 5:2	218:22 267:22	76:15 103:3	250:5,9,11,12
291:3 293:22	5:7 6:7 14:17	proactively	104:12,15,18	252:7
295:1,20 296:2	27:17,19 42:17	205:9 322:2	104:19 105:4,5	procurement
296:6,12,19	42:19 43:5,16	probable 29:16	105:6,7 143:7	251:16
297:4 298:16	43:22 44:6,8,8	53:17 65:3,14	189:15 193:3	produce 164:4
298:16 299:3	44:16 45:7	73:1 81:21	203:19 256:19	246:11
299:13 302:14	63:1,13 102:11	169:5 362:3	311:9 344:7	produced 74:2
304:15 305:1	102:14,15	probably 27:14	376:16	produces 16:5,6
306:3,10	103:22 104:4	58:15 101:5	procedural 28:1	product 26:17
310:11 311:18	104:18,21	120:16 137:6	procedures	35:8 126:14
312:2,4 313:20	124:20 125:12	191:17 276:12	114:5 177:13	150:22
317:10,11	125:13 127:16	306:13,18	300:5 314:22	products 111:19
330:1 332:2,4	127:17 133:19	307:10 317:16	376:2	113:2 125:10
332:7,21 333:1	133:21 141:7	318:17 337:1	proceed 4:20	125:18 131:20
333:3,17,18,19	151:16 152:20	342:22 343:2	134:19	150:18 154:20
333:22 334:2	186:9,18	344:13 360:10	proceedings 4:1	professional
334:12,22	216:10 229:7	probe 11:17	130:11 385:6,8	140:17 242:16
335:19 336:1,8	231:16 233:12	probing 41:3,5	process 56:9	247:20
337:2 338:17	234:12 250:3	problem 13:14	117:18 130:13	professionals
339:20,22	264:7,8,19	21:11 27:7	146:5 174:9	190:12
340:5,11,17,17	267:15 284:19	47:17,22 48:8	191:8 218:8	professor 18:1,3
340:18 341:2	285:4,20	48:10 49:20	223:7 231:14	33:11 45:10
341:12 342:2	287:20 288:14	51:18 62:17	232:15,17,20	54:8 89:19
343:6,7,15,18	290:14 291:14	92:1,7 117:12	233:6 236:9,10	110:12 142:8
344:5 345:9	293:3 294:14	117:13 118:4	240:18 250:6	169:17 186:22
348:15,17	296:10 297:6	120:11 121:17	251:16 274:2	194:7 286:21
349:9 352:21	297:14,17,19	137:11 146:18	277:5 283:14	287:2,2,6
353:7 356:21	297:21 298:2,7	171:8 264:21	308:18 316:8	296:14 305:22
357:6 358:21	298:10,14	274:20 277:3	330:20 344:16	326:9 328:2
362:4 363:7,11	299:10,16,21	305:2 309:14	344:18,21	335:22 341:17
363:20 364:3	302:13 303:5	316:21 320:1	345:20 346:11	374:4 375:17
364:20 365:3	314:5 317:15	335:6 346:5	347:8 356:9	381:9
365:19 366:18	317:21 327:21	353:13,15	382:22	professors 92:17
368:13,20	328:7 329:11	356:7 371:11	processes 29:21	195:12
369:2,7,12,15	331:4 336:5,8	371:16	57:21 96:2	profile 75:14
369:21 370:7	341:20,22	problematic	117:21 126:9	148:9 268:16
370:18 371:2	342:5 343:12	361:12	127:3 132:18	profiles 159:10
375:2 376:1,3	345:2 352:17	problems 20:16	173:22 215:4	162:12
376:11,12	354:9 356:13	20:20,21 21:2	224:6 252:13	profound
383:19	357:4 367:17	46:12,13,15,16	330:22	151:20
privacypreser...	379:18	46:17,20 47:1	processing 46:4	program 7:6
40:18 106:12	privilege 287:15	47:2 48:7,8	323:2 324:11	10:8 25:5
privacyrelated	325:4	50:5,5 51:17	325:5	30:17 31:3

56:18 84:14	prohibited	101:17 111:2	52:17 85:10	129:22 181:2
90:1,9 92:4	122:20	113:21 116:11	86:13 111:3	202:1
103:4 120:7	prohibitions	118:16 121:14	132:8 163:5	provides 100:9
126:21 127:2,8	128:19	124:6,8 133:6	166:1 204:19	113:13 216:2
128:16,18	project 311:12	167:14 199:5	208:2 221:1	221:11 225:14
129:1 158:18	prominent	204:11 208:3	225:17,21	226:18
163:17 174:3	122:4	228:9 230:16	229:15 232:2	providing 24:2
175:10 180:20	promise 99:4	233:9 237:7	233:7,14	83:8 85:10
180:20 181:1	122:10	258:12 264:10	234:17 280:22	104:8 111:3
182:6 202:11	promised	264:12 289:5	281:1 282:8	115:10 135:8
204:13 206:20	156:16	330:1,22 333:2	296:16 333:1	207:12 209:6
214:9 224:22	promote 154:21	333:22 334:3	341:9	210:12 211:8
225:6 229:21	234:9	369:1 376:11	protective	227:15 249:12
230:7 245:2,19	proof 225:1	protected 31:10	299:12 332:7	266:7 272:5
251:22 252:2	proper 23:14	42:11 114:1	protects 12:5	280:4
257:15 260:14	48:18 74:15	126:4 133:17	20:7 125:18	provisions
261:21 275:7	210:3 315:3	150:8 167:17	167:15 207:16	122:14 365:6
311:2,17 332:4	proportion	191:14 211:4	209:2 217:5	proxy 274:10
332:6,11	317:13	222:11 264:5	304:15 348:17	pseudoprivate
359:18 360:18	proportionality	protecting 28:16	protocols 51:8	107:15
365:9,22	317:6 345:4	52:7 61:11	proud 28:12	psychologists
366:14 372:1	362:14 366:3	129:1 133:19	prove 113:9	122:22
programs 30:15	proposal 212:9	142:18 234:5	proved 134:5	public 1:12 4:4
32:2,7 46:3	proposals	242:21 284:13	proven 235:2	5:4,7 7:10 14:1
56:16 58:14	358:17	287:19 289:5	366:18	14:4 15:2
64:6 81:6,18	proposed	306:3 341:12	provenance	33:12 48:4
128:7 129:3,7	354:11	341:14 367:7,9	326:4,5 365:17	66:2,2,5 67:16
130:5 168:14	proposes 358:8	protection 42:4	provide 24:12	74:2 75:2,4
180:14 199:18	proposition	46:2 113:14	84:16 105:13	84:8 96:14
200:21 201:2	96:15 233:2	114:5 154:3	112:17 130:16	115:5,11 120:1
204:15,18	proscribed	168:20,21	135:5,20	129:2 130:22
205:4,7,12	334:20 365:11	169:4 194:20	168:20 169:2,3	148:14 163:14
213:21 214:5	proscriptions	194:22 200:9	210:9 211:11	180:7,8 197:17
215:18 216:2	324:8	200:11 206:5	211:22 213:14	207:8 211:10
227:3,19 241:9	prosecute 16:1	216:14 229:20	214:1,15 218:1	213:3,6 255:5
241:9 242:14	prosecutor	258:16 290:7	239:15 276:2	278:21 284:8
245:16 247:14	70:15	290:11,12,17	294:19 295:5	287:20 288:15
262:13 296:4	prospect 95:12	296:2,7,20	301:9 302:3	291:14 292:18
310:2 311:7	prospective	297:4 299:4	305:18 370:8	298:15 317:20
331:21 333:9	267:19	306:10 332:2	provided 43:4	328:5 329:12
375:19	protect 9:1 20:2	349:14 362:10	175:13 219:5	330:5 336:5,18
progress 153:13	20:3,6 24:3	376:12	provider 182:16	337:2 339:21
154:7,14	28:20 29:4,20	protections	188:4,20 189:5	340:1 381:7
234:21 284:8	29:22 31:11	24:14 43:4	providers	385:4,17

publically 219:4	pursued 260:20	170:1 171:12	91:16 100:9,20	337:8
publicity 5:8	260:21 280:3	174:1 175:9,19	100:22 101:1	quorum 4:13
publicly 14:19	pursuing 213:18	179:5,13	102:3 109:1	quote 8:7
15:3 75:11	push 96:5	181:12,20	110:5 133:22	136:20
92:3 208:12	201:22 235:20	182:13 183:8	134:13 141:1	
339:1,13	269:3,13	185:4,5 186:14	141:15,21	R
publish 129:17	put 7:7 17:4	192:2,5 195:1	150:7 159:16	race 68:18
published 82:5	27:6 39:8	196:18 197:9	165:5 175:21	rachel 2:4 4:13
publishing	52:20 58:22	197:10 199:9	181:9,14 185:8	80:14 159:18
271:13	83:2 93:22	199:15 200:6	194:6 206:1,3	271:4 285:7
pull 203:17	144:12 150:3	212:16 238:9	215:6 230:6	racial 122:1
316:7 323:21	150:12 152:11	238:16 239:11	232:5,7,10,15	radically 148:9
345:21	160:15 163:6	239:18 241:5	237:19 238:11	raise 110:9
pulled 60:16	167:1 169:9	241:12 252:15	238:20 239:3,9	276:4 305:4
pulling 58:16	172:22 201:15	255:13,22	248:5 255:2,4	357:7
purchased 37:6	229:11 242:3	257:2 258:11	260:15 262:12	raised 74:15
purchases 35:8	269:14,18	262:9 267:14	262:14 263:2	326:9
purporting	280:5,8 370:21	274:12 276:13	274:5,15,19	raises 357:1
271:9	377:15	276:15 279:5	275:10 277:9	ramification
purpose 69:9	puts 25:18 38:20	281:3 282:17	278:3,6,8,12	17:5 140:12
94:9 97:18	245:18	283:4 286:18	278:15 280:3	ramifications
118:9 256:12	putting 60:6	289:4 293:5	282:20 284:16	13:2 137:12
260:17,18,19	151:8 268:5	313:16 318:10	286:9,11,12,14	139:14 202:4
261:1 265:1,1		318:12,15,20	312:11 318:6	range 11:10
272:11 275:2	Q	321:20 326:10	322:5 343:16	101:20 152:7
288:21 289:2	quantify 164:8	334:9 335:18	357:7 368:9	172:13 253:8
296:16 300:16	196:21	344:11 348:7	381:7 383:6	319:1 383:11
300:18,21,22	quasifederal	357:22 358:10	quick 66:12	ranging 237:10
329:6,7 359:19	106:19	358:16 360:14	71:3 76:17	rank 319:19
359:20 360:1	queries 164:10	361:11 363:5	78:3 175:9	rap 14:13,15,17
362:16 366:19	querying 60:13	363:22 367:14	179:12 183:19	rapid 226:15
purposeful	question 9:15	368:16 370:11	198:18 203:12	rapidly 190:6
178:11	10:1 26:9	372:19 373:5	313:15	rare 12:5 295:3
purposes 79:20	31:16 43:9	374:3 379:4	quickly 51:4	rarely 133:12
93:13 112:2	55:7,8,11 61:8	questionable	53:3 146:6	rat 13:13
186:19 273:5	63:19 66:19	112:22	175:22 198:11	rate 57:1 58:16
281:20 299:9	74:15 75:3	questioning	200:12 267:14	315:21
318:4 352:22	76:9 82:20	74:11 110:3	277:14 354:7	rates 315:22
365:15	90:16 96:2	141:17	quite 12:19 17:7	ratings 184:17
pursuade 243:6	98:11 102:18	questions 6:11	70:11 74:4	ravaged 137:19
pursuant	105:19 107:21	6:12,14,16	87:12 151:20	reach 91:11
204:18 278:20	110:8 142:1	9:17,20 10:2	224:3 240:5	249:17
pursue 57:14	154:16 155:14	41:1,3,6,14,17	246:10 249:16	reaching 33:6
221:9	159:22 165:16	81:16 88:8,10	252:8 318:3	reaction 353:2

reactions 360:11	157:20 158:13	reasonable 23:1	recognition 42:7	175:12 203:3
reactive 267:19	158:13 159:21	60:12 65:10	55:2 148:3	284:21 306:21
read 31:4 45:19	161:13,17	70:4 111:11	362:7	385:8
58:7 83:6	163:10 170:3	147:5 148:13	recognizable	recorded 7:6
181:13 339:10	177:3,3,6,15	157:20 162:7	54:10	34:9 163:20
351:17	177:16 178:5	169:4 198:7	recognize 8:22	330:10 385:7
readily 75:5	187:3,4,5,6	292:17 334:11	54:11 64:11	recording
160:19 273:22	190:1 195:21	362:2 363:7,10	68:1 75:18	329:15
reading 103:4	196:4,4 197:4	363:19 364:2	123:6,18 125:7	recordings
162:22 220:9	197:5,10,10	366:15,17	131:18 153:9	34:11
241:9 301:19	200:13 220:5	368:12,13,20	155:3 231:5	records 14:11
339:15,16	225:4 239:4	369:2,6,11,15	270:16 284:5	14:16 15:16,16
reads 324:15	248:11 250:7	369:20 370:6	327:18	98:21 99:5
real 77:10 97:6	251:16 252:7,8	reasonableness	recognized	120:7 163:3,17
97:6,7 113:13	256:21 259:1	65:16 70:17	42:11 65:5	168:1 221:12
132:3 184:4	259:10,17	377:8	133:13 151:13	221:14 222:6
252:21 257:1	263:3,22 270:3	reasonably 59:2	217:12	278:19 301:14
266:21 292:3	271:10,18	69:20 106:4	recommend	301:17
328:21 331:2	272:4,8 275:9	155:2 177:18	61:11 93:13	red 2:14 17:21
379:12,22	277:12 282:1,2	182:11	303:1	22:14 25:5
realistic 221:7	282:21 287:16	reasoned 327:9	recommendat...	110:2 207:6
realities 99:15	287:17,21	reasons 79:1	92:15 213:19	286:4,6 354:4
reality 77:10	288:15 289:3,6	264:2 268:4	240:12 373:9	redacting
84:15 97:21	291:4 292:15	292:20 299:15	recommendat...	307:12
realize 33:1	294:18 307:6	319:6	92:11 128:15	redactions
121:21 148:12	308:9 312:12	reassert 68:2	171:16 239:15	220:11
156:22 167:9	313:14 316:2	reassociate	279:19 288:1	redefine 118:12
357:1	323:14 326:14	196:14	300:1	redress 83:15
realized 12:16	328:7,8 329:13	reassurance	recommended	282:9 294:11
210:16 347:12	330:19 332:21	211:11	163:22	294:15 295:4,9
really 13:20	336:6 346:13	reassure 120:17	recommends	reduce 40:11
25:13 27:9	357:16 360:14	267:2	93:16	174:15
32:6 47:6 48:7	373:6 374:16	reassures 56:9	recommit 303:2	reduced 174:22
53:9,10 55:4	378:20 381:5	rebecca 3:14	reconcile 55:1	reducing 211:7
58:10 67:9	reason 15:17	recall 70:21	157:13	redweld 306:14
68:18 71:3	25:17 53:9,11	321:5	reconciled	307:1
72:20 76:10	69:14 82:4	receive 5:18	315:13 316:1	reevaluate
84:3 88:21	121:8 155:9	88:6 136:7	reconstruct	134:3
89:20 93:6	175:6 247:8	332:19	39:18 184:10	refer 355:5
107:21 116:3,6	291:5,12 292:1	received 128:9	reconstructing	reference 75:6
120:16 143:3,5	292:15,22	129:13,19,22	179:5	referenced
143:6 145:7,20	293:1,2,2,3,4	139:10	reconvene 203:1	74:16
148:22 150:4	339:7 349:3	receptacle 8:14	record 59:20,21	referendum
155:22 157:1	362:5,17 372:3	recipient 139:22	97:9 109:4	361:1

referred 126:17 186:4 192:3	regulates 103:1	releasing 14:9 164:9 201:20	remedies 281:10	177:4 206:11 253:20 302:13
referring 68:4 185:21 326:17	regulating 24:11 38:14	relevant 28:3	remedy 282:6	repository 21:14 49:16
refers 97:12	regulation 42:19 43:7 102:13,19	100:12 125:22 134:7 203:14	remember 106:21 119:18	represent 45:15 197:14
refine 232:15	103:11,12,14	206:15 289:1	135:21 136:3	representation 364:16 380:7
reflect 97:9 170:21 355:15	103:19 108:6,7	301:4 307:4	remind 88:9 109:19	representative 32:21 253:12
reflected 174:10 229:17	108:12 290:17	352:7,8 370:16	reminded 203:20 214:21	represents 155:7
reflects 29:13 382:5	regulations 7:11 384:5	relied 375:6	reminder 255:3 318:7	republican 69:22
reform 127:22 130:15 168:5	regulatory 372:18	relies 121:9	reminders 214:16	repurpose 382:15
179:21 212:3 380:16	rehash 354:3 360:15	religion 11:3,16 11:17,19,21	reminds 159:2	repurposing 322:21
reforms 130:3	reidentified 113:11 114:2	12:2,3 26:16 44:10	remotely 197:14	requested 365:15
refrained 16:14	reidentify 160:18	relocate 122:16	render 214:7	requests 167:21 168:14 302:5,8
regard 33:3 126:1 128:1	reigning 44:15	rely 74:18 124:3 190:9 194:1	renee 7:15 109:22	320:22
132:6 219:8	reinforcing 184:3	246:10	renting 321:7	require 30:22 59:4 168:5
220:8 221:19	reiterate 341:9	remain 45:8 119:7 122:12	repealed 123:12	218:22 219:1
222:9 246:4,13	relate 47:2 183:4 285:5	125:12,21 228:6	repeat 198:8	219:14 228:8
281:22 285:6	related 49:9 124:20 128:13	remaining 86:8 101:12 154:15	repeatable 232:16	370:21 371:4
294:15 317:17	232:7 241:4	223:22 274:18	repeatedly 298:15	required 102:13 168:10 172:12
regarding 5:2 6:4 87:4	295:17 344:7,8	remains 44:5	replace 101:9 350:5	208:3 272:16
204:12 213:20	relation 21:21	remark 278:17 340:10	report 50:14 74:3 82:5	298:22 346:21
272:6 278:21	relations 115:11	remarkable 375:9	84:11 119:12	requirement 29:17 71:21
301:10	relationship 63:17 167:16	remarkably 383:7	162:22 179:20	202:5 311:16
regardless 118:22 168:6	239:14 302:20	remarked 8:4 373:15	184:17 213:20	314:10
231:8 303:5	337:22,22	remarks 7:2 45:14 109:20	223:14,15	requirements 174:4,5 227:8
365:1	338:1	140:22 141:14	256:9 279:19	239:16 272:19
regards 220:14	relationships 54:20 153:3	157:22 172:6	351:17,19	327:6 343:7
regime 230:11	242:10 263:18	217:1 237:21	358:1 362:19	requires 31:18 52:11 91:4
register 4:10	265:13	281:12,14	reported 1:22 130:20	130:12 131:4
regnant 86:8	relatively 76:2 225:13 298:3	284:15 286:2	reporting 130:2 220:16 240:10	188:19 219:9
regular 224:11 240:17 373:19	release 155:20	remedial 281:5 281:8	302:6 336:12	
regularly 133:22	released 157:8 222:15		346:21	
regulate 46:19 78:22 211:16			reports 31:5 57:16 163:19	

requiring 111:18 112:17 370:14 371:12	70:8 127:3 227:7 253:22 262:9 305:2 355:4 357:21	retailer 35:7 retain 62:1 118:2	202:14 revoke 201:22 202:16,18	161:7 173:9 175:3 176:17 178:7 181:7
research 18:3 39:15 92:2 144:4 234:5 250:15 251:10 251:14 252:10 349:19	responses 165:17 responsibilities 245:10 responsibility 240:13 244:1	retained 126:2 221:4 222:4 300:17 retaining 134:5 263:20 retention 40:20 90:4 93:2 256:10 257:22 258:4 259:3 322:6,11 351:9 351:10 371:8	rewriting 366:22 rhetoric 294:2 richards 3:14 225:11 226:4 238:9 250:10 262:10 268:22 271:11 272:9 273:10 277:1 283:6 354:20	186:14,21 195:21 196:2 197:9 200:18 201:19 202:15 203:21 220:7 241:19 242:22 243:1 247:15 248:5 251:2,3 251:13 252:8 253:5 258:8 259:12 261:18
researchers 144:3 160:16	responsible 18:20 19:1 209:15 236:22	retrospective 347:1 return 195:6 returned 222:1 returns 192:13 319:12 reveal 76:14 151:15 153:2 revelation 47:13 revelations 128:6 131:15 reverse 159:17 194:15 review 30:9 31:1 57:20 59:9 60:3 65:19 71:1 74:1 116:1 130:12 168:13 221:11 221:13 223:6,8 223:17 251:2 253:18 281:20 371:1	rid 52:8 ridiculous 197:19 rifle 307:2 rigged 200:15 right 4:21 5:1 17:22 19:16,17 26:17 48:14,17 51:5,5,14,16 51:20 53:2 54:4,10,15,15 57:11 60:5 65:2 66:22 72:10,12,18 76:6 77:9 82:8 82:12 83:14 84:5 85:16 87:1 88:20 90:15 96:21 97:1,17,18 99:20 107:18 117:12 118:10 118:22 124:9 129:12 132:3 134:1 136:4 138:10 139:7 140:16 146:9 146:10,11,20 147:14 153:1,1 153:10 157:4 158:17 160:13	259:12 261:18 262:7 263:12 263:17 268:6 275:10 285:9 293:16 310:19 314:2 315:3,6 326:3 333:19 335:15 338:15 344:16 345:12 347:6 350:19 350:20 361:19 362:1 364:16 364:21 365:10 365:20 367:14 378:9 379:13 380:5 rights 8:12 11:2 19:2 51:7 83:15 84:20 99:2 130:8 131:17,22 150:15,21 157:6 191:22 202:1 226:21 234:11 295:9 329:19 378:10
reservation 321:8,9	responsive 298:19 rest 88:16 190:6 293:16 327:12 327:16 restore 128:5 restrain 29:22 restraining 27:20 restraints 300:9 restricions 245:20 restricted 300:13 restriction 42:16,17 121:13 122:12 245:19 301:2 376:20 restrictions 81:10 118:17 121:10 124:3 245:18 341:18 result 176:9 187:19 228:21 266:18 315:20 379:3 results 177:4 290:2 330:8 resume 109:3,6 284:18	reviewed 358:3 reviewing 30:5 reviews 30:3 173:4 216:1 223:5 281:16 revocation 201:18 202:3	risky 294:2 225:11 226:4 238:9 250:10 262:10 268:22 271:11 272:9 273:10 277:1 283:6 354:20 rid 52:8 ridiculous 197:19 rifle 307:2 rigged 200:15 right 4:21 5:1 17:22 19:16,17 26:17 48:14,17 51:5,5,14,16 51:20 53:2 54:4,10,15,15 57:11 60:5 65:2 66:22 72:10,12,18 76:6 77:9 82:8 82:12 83:14 84:5 85:16 87:1 88:20 90:15 96:21 97:1,17,18 99:20 107:18 117:12 118:10 118:22 124:9 129:12 132:3 134:1 136:4 138:10 139:7 140:16 146:9 146:10,11,20 147:14 153:1,1 153:10 157:4 158:17 160:13	259:12 261:18 262:7 263:12 263:17 268:6 275:10 285:9 293:16 310:19 314:2 315:3,6 326:3 333:19 335:15 338:15 344:16 345:12 347:6 350:19 350:20 361:19 362:1 364:16 364:21 365:10 365:20 367:14 378:9 379:13 380:5 rights 8:12 11:2 19:2 51:7 83:15 84:20 99:2 130:8 131:17,22 150:15,21 157:6 191:22 202:1 226:21 234:11 295:9 329:19 378:10 riley 133:14 151:13 ripe 59:21 rise 114:22 risk 13:17 40:11
reshapes 226:11 reside 231:9 resides 156:2 resilient 111:16 resist 118:18 121:9 resisting 377:4 resolution 170:15,17 resources 68:17 150:2 160:19 194:4 245:13 248:7 294:22 310:3,8 319:8 343:2 respect 45:3 90:13 97:17 115:11 179:6 193:2 198:2 231:8 334:10 361:11 365:21 380:3,5 respectful 189:15 respond 158:22 348:19 351:12 responded 298:15 respondents 16:10 response 57:9				

49:15 60:18	73:21,21 74:6	rubber 259:11	132:12 133:2	353:14,17
62:5 92:19	74:7,9 83:13	rubric 9:5	164:5 230:2	354:14 381:13
93:1 106:6	116:20 207:12	rule 38:19 99:10	278:22 279:2,3	says 72:9,12
111:12 114:14	225:13 239:2,5	126:7 131:6	279:21 282:9	96:4 163:1
115:12 119:16	239:18 247:3	135:2 159:16	284:6 289:9	314:16 332:21
159:6,10	305:10 317:1,2	315:5 371:22	292:4 301:8,8	342:3 347:1
162:12 163:4	372:13 373:7	375:12	302:10,11	349:9 352:21
183:20 235:8	374:6,8,9	ruleladen	343:17 369:7	353:8 357:12
235:17 236:9	375:18 376:22	325:14	sadly 57:4	357:14 362:8
236:10 258:18	377:18 378:14	rules 28:6 38:11	safe 133:1	381:10
259:16 262:3	379:5 380:3,10	95:1,8 113:7	safeguards 87:4	scale 50:17
263:2 275:6	rolebased 127:5	132:19 135:4,9	safer 40:10	52:20 73:15
280:5 290:18	172:14	135:12 140:15	safety 40:6	152:18 169:2
290:18,18,22	roles 12:3 127:1	157:21 158:2,3	133:7,8	248:2 260:5
291:3,12,21,22	127:7 172:17	158:5,9,16	sake 20:7,8 27:3	261:6 302:18
330:21,22	246:2 355:12	159:11,13	192:14	318:3,5,5
331:16 334:6	roll 288:11	168:12 169:11	sales 127:6	334:8 344:7
337:11 350:10	room 22:11 60:9	169:15,21,21	172:16	349:17
381:15 382:1	78:22 115:22	171:6,21	salient 27:15	scared 373:5
risks 43:19	116:4 137:7	172:20 174:10	salt 27:6	scenarios 86:11
45:16 49:11	144:22 165:12	190:8 192:16	sam 286:2	167:10
58:2 61:5 93:4	193:14 201:14	210:22 211:17	sample 184:2	schedule 222:5
104:2,9 162:13	304:21 329:14	211:20,22	samples 135:20	schemes 281:8
225:2 231:22	rosenzweig 2:14	212:1,4,13,18	sampling 164:4	scholar 115:15
232:18,22	25:4,9 33:9	213:5,8,9,12	sanchez 66:16	scholars 113:4,8
233:5 236:1	50:8,11 53:20	213:13,13	sanctions 95:7	113:12
237:7 256:8	55:6 58:5 69:5	238:18 335:13	sand 300:10	scholarship
258:10 261:5,7	76:17 84:10	343:18 344:9	sat 136:20	36:17
261:8 262:1,2	94:14 98:5	348:6,12 356:6	satisfied 210:2	school 3:18 18:4
266:21 275:4	99:7,18 100:21	rulings 130:12	satisfied 43:3	110:13 117:6
291:6 343:12	101:11 106:17	run 37:22 55:22	177:19 187:15	161:12 196:1
risky 235:21	107:7	126:19 188:21	satisfy 157:21	287:3 292:5
270:4	rough 163:15	336:2 360:10	316:5	science 33:12
road 259:11	round 110:3	running 130:21	saw 164:1 278:7	77:11 110:15
roberts 133:13	141:17 146:12	182:7 200:8	300:11 375:1	233:17 234:7
robust 84:20	route 245:5	343:10	saying 47:6	234:17 261:15
125:15 210:5	routine 222:15	russians 189:13	150:20 160:2	313:11 316:8
211:2 252:20	222:17		163:19 167:1,5	335:15,16
253:14 297:4	routinely 123:1	S	167:8 178:20	sciences 181:16
303:2	229:10	s 3:13 36:4	178:22 187:8	scientific 235:1
robustly 299:16	row 9:11 109:17	127:19,20	260:8 284:2	236:9,15 237:5
rogue 346:19	109:22 116:16	128:4 129:10	298:10 310:20	scientist 33:19
365:18	185:5,6 186:21	129:14 131:15	310:22 348:2	134:18
role 32:14 65:20	207:6 286:3,20	131:17 132:1,9	350:10 351:15	scientists 237:11

237:13	76:11 105:21	304:9 310:20	133:20 134:15	145:5 148:20
scifs 253:18	secrecy 32:1	314:5 317:16	135:7,9,13,14	148:21,22
scool 2:15	192:8 208:10	317:21 327:21	140:9,16,18	150:2 155:14
scope 164:1,8	208:21 210:21	328:8 329:12	143:13 155:19	160:17 177:2,9
301:3 302:4	373:8	329:12 330:6	156:21 162:17	183:22 190:20
334:8	secret 66:4	331:4 336:5,6	166:13 176:13	198:1,9 199:4
scratch 53:19	98:18 214:18	336:8,18 337:2	176:19 188:8,9	223:10 236:22
65:8	302:2 355:17	341:20 343:12	188:11,15	245:5 249:10
screen 174:9	355:18	345:2 352:17	190:3,12	256:12 266:11
screening 59:16	secretary 25:7	356:13 357:4	200:11 204:5	280:16 290:15
84:19	secretly 301:15	367:17,17	218:16 219:19	294:13 307:1,3
scrutiny 29:12	secrets 18:8	379:18	223:2,4,5	307:7 308:6,12
60:16	19:7 32:10	sectors 284:19	225:3,12,22	320:14,16
seal 385:12	115:3 208:11	287:20 342:6	226:3,15	341:1,3 342:10
search 42:3 52:9	214:11,17	secure 12:21,22	229:10 246:19	372:11 376:20
65:10 198:13	267:9	18:20 49:10,11	256:21 257:1	seeing 57:8
198:14 300:12	section 90:1,9	72:10,12 94:7	257:10 272:12	158:18,18,19
searched 91:20	90:14 92:3	113:2 138:4	280:1 285:7	188:2 290:14
searches 52:10	103:5 119:13	143:21 155:16	290:4 291:2	297:8 338:16
53:8,18 70:10	128:16 175:10	209:21 253:17	293:2 294:10	370:12 376:16
72:10,13,15	278:20 301:4	secured 256:17	294:19 296:3	seek 125:14
198:14 290:5	301:11,15	security 3:7,14	297:20,22	131:2,5,20
314:20 369:1,4	330:11 351:17	8:18 10:8	298:8,18 299:8	222:8 365:5,6
searching	369:5	14:11 19:15,17	302:5,7 303:12	seeking 132:12
192:22	sector 3:17 6:7	19:21 23:1	303:14 310:20	241:14
second 5:22	43:5 104:18,21	24:15 25:3,8	313:20 321:15	seemingly 35:12
13:22 19:12	124:20 127:16	29:14 42:2	327:11 330:20	36:14 89:5
34:2,13 37:14	127:17 133:20	46:3 49:8 54:1	331:3,12 333:9	seen 19:16,17
70:1 109:10	133:21 174:4	61:18 64:6	335:12,19	44:12,13 95:18
111:10 115:2	186:9,19	66:8,13,18,20	338:21 339:7	109:22 129:4
116:16 117:2	200:16 216:10	67:4,5,6,9	343:11 345:8	337:4 374:21
119:2 128:21	230:18 231:16	69:11 73:6,12	367:1,7,9	sees 18:15
199:10 202:22	233:12 234:12	73:13,14,17,18	375:19 381:21	segment 198:3,4
238:1 269:11	250:4 264:7,8	81:1,12 83:18	382:13 383:19	segments 198:2
285:16 290:13	264:19 267:15	84:13 85:10	see 6:6 19:9 24:1	segue 159:21
297:18 301:9	285:4,20	89:9,13 100:5	24:2 27:12,21	seinfeld 321:7
324:14 332:12	288:15 290:15	104:6,10	49:8 50:1,21	seized 290:9
334:21 346:11	291:14 293:3	111:20,22	55:7,8 56:6	292:8,10
364:18 381:15	294:14 296:11	112:12,18,20	57:4 59:14	seizure 42:3
secondary 46:4	297:6,15,17,19	112:21 114:20	69:14 76:7	seizures 72:11
58:17 84:18	297:21 298:2,7	115:20 116:13	86:8 95:16	72:13 369:2,4
secondly 186:15	298:10,14	123:22 126:4	104:20 116:6	select 174:7
319:10 373:4	299:10,16,21	129:14,18	135:13 142:14	selected 226:6
seconds 32:13	302:13 303:5	132:22 133:7	144:10,13,22	selfcorrecting

158:20	separately 62:13	203:7	shes 70:8	sign 126:15
selfevident	sequential	set 108:10	shift 371:2	167:1
335:3	235:10	113:10 125:15	shifting 213:4	signal 355:21
selfhelp 23:22	serendipitous	163:2 222:5	213:11 251:21	signals 231:6
68:5,19	50:18	231:12 232:10	259:3 330:1	320:2
sell 131:20	series 8:20	264:21 271:22	shipping 126:14	signant 227:22
semiclear	29:20 198:1	299:22 316:21	shocking 163:13	signed 51:9,14
158:11	206:1	322:9,10	shoes 361:9	354:15,16
senate 117:7	serious 193:3	374:10	shop 238:8	significance
164:1 179:16	194:5	sets 117:16,19	239:13	54:12 98:13,14
303:11	seriously 171:21	167:15 323:16	short 86:1	185:13
senators 193:8	177:20	325:17 335:1,4	117:21 137:18	significant
193:12	serve 361:10	359:21	344:15 361:1	20:15 43:19
send 9:21 136:7	served 204:15	setting 69:18	shortcuts 350:1	58:15 59:11
193:14,17	206:16 288:21	86:19 294:14	shot 67:18 99:13	216:19 218:1
sends 343:17	303:11	settings 114:3	shouldnt 18:10	223:6 228:21
senior 25:6	server 156:2	197:17	55:4 67:9	234:21 240:1
224:10 226:1	serves 12:13	settle 379:14	95:18 171:8	253:1,11 309:5
238:13 239:22	67:7	seven 9:10	180:2 311:22	314:16 338:4
295:15	service 26:21	109:20 137:14	361:16 375:7	361:3 367:13
sense 28:5 31:10	106:20 107:13	137:16 286:1	show 65:2 267:6	significantly
83:18,19	112:15 122:19	severely 377:2	267:6 283:15	240:5 248:18
105:19 151:6,7	123:4,13	shame 28:11	283:16	248:19 306:9
161:18 163:15	126:14 127:7	shannon 7:14	showing 16:9,13	silicon 135:1
166:21 221:11	129:22 139:22	shape 20:4	shown 37:12	311:12
244:1 246:6	150:22 152:9	226:20	177:5	silly 290:2
248:11 251:4	181:2 182:15	share 13:7,9	shows 11:10	silver 172:7
271:22 273:8	188:3,19 189:4	17:10,12,13,14	39:15 67:13	332:9 370:7
274:8 317:18	202:1 208:13	105:2 198:3	shredder 307:10	simialar 268:7
320:11 322:6	208:18 299:6	220:17 264:20	shut 283:2	similar 29:14
338:2 344:13	328:11	375:14	side 19:20,21	122:18 212:7
365:14	services 34:10	shared 221:2	58:14 66:11	239:10 264:20
sensitive 35:11	125:8,11,18	222:20 283:3	68:20 73:13	266:3 267:17
35:12 115:6	126:19 127:17	shares 13:5	130:13 142:12	278:21 302:13
120:20 168:8	131:10,21	sharing 17:16	142:13,13	320:5 344:6
268:11,16,19	140:1 150:18	119:20 123:11	155:6 170:2	355:12
sensitivity 152:2	151:11,17	142:5 149:17	216:16 219:17	similarities
172:10	155:12 158:4	241:12 325:19	219:18 221:16	264:12,15
sensor 17:3	188:19 199:3	sharon 7:14	222:10 261:6	similarity
sent 137:2	228:5 299:2	sharply 112:8	261:15 264:17	264:17
139:10 326:13	serving 122:20	sheer 37:19	267:5 277:22	similarly 37:10
sentence 105:17	123:12	228:19	371:17	simone 7:15
separate 8:1	session 2:9 3:1,9	sheet 14:13,15	sides 213:15	simple 136:17
167:6	3:16 202:22	14:17	256:21 382:2	137:9 329:1

135:20 141:4 155:13 simplest 124:5 simply 28:10 62:18 84:12 106:1 113:1 115:8 143:15 156:20 175:14 314:7 322:21 323:12 345:8 364:10 370:17 simultaneously 187:22 single 40:2 62:1 98:9 121:8 140:3,3 168:11 168:11 270:17 sit 126:22 272:18 316:16 sites 39:12 sits 108:7 sitting 6:22 22:11 69:21 174:7 286:3 306:14 situated 205:2 situation 99:12 situations 8:20 259:19 348:20 six 16:13 45:16 177:2 273:16 274:18 sixteen 45:15 48:20 124:12 149:6 sixteenplus 125:1 size 58:9 101:19 152:14 skeptical 100:18 skew 73:12 skews 19:20 skill 305:10 skin 35:8 37:6	skipping 309:3 sky 136:22 skype 137:3 sliding 169:2 slight 199:13 slightly 21:7 269:16 316:20 sloppy 362:7 slow 121:21 123:18 379:20 small 51:21 59:7 66:4 242:9 244:21 245:9 246:5 299:22 310:6,6 371:7 371:10 374:11 smaller 44:4 138:12,12 228:8 smarter 110:22 187:11,11 smartphones 139:6 smile 8:6 smorgasbord 297:2 326:19 smudges 171:1 snapchat 156:15 157:11 snooping 24:4 snowden 16:9 16:14 57:9 120:6 163:14 198:12 social 14:11 17:3 19:17 27:2,8 37:12 197:16,22 199:7 229:10 237:11 338:14 338:22 340:3 sociatal 227:21 societal 8:1 9:4 19:13 20:2	26:21 33:6 155:10 289:18 296:14 society 8:15 11:4 17:2 19:18,20 20:3 20:4,9 22:6 27:4 47:20 50:19 54:13,16 54:22 55:3 56:10 57:7 67:7 70:6 121:21 123:17 137:21 147:17 167:15 191:8 229:4 291:19 302:22 312:5 societys 20:8 societywide 17:1 software 111:20 126:12 156:5 165:8 172:15 173:2 176:21 177:12 sold 24:6 solely 124:2 solid 380:7 solitude 5:6 solove 2:15 18:2 18:5 45:11 46:7 51:21 52:1 71:3 76:5 83:4 93:5 104:11 soloves 54:8 solution 315:14 316:10 358:21 solutions 115:18 285:19,20 311:8,9 316:7 341:21 solve 143:6 146:18 somebody 47:7	47:8,12 54:4 55:5 60:3 61:16 175:4 186:4 201:10 245:4 249:17 353:17 someones 156:2 268:16 someplace 275:16 292:11 somewhat 25:21 33:15 100:18 158:20 173:18 183:12 230:13 240:10 255:12 256:3 sophicated 280:7 sophisticated 41:9 111:1 112:22 142:4 199:4 sorry 51:1 193:16 194:17 201:11 207:3 255:8 259:5 262:6 263:10 287:13 318:16 sort 26:11 30:21 55:13 57:8 60:3,11,19 76:19 81:15 87:12,13 93:6 104:13 105:20 106:2 150:12 152:19 159:17 172:19 175:20 180:10 192:14 210:14 218:5 225:1 243:10 246:2,17 250:20 251:21 252:3 255:13 259:20 260:17	261:6 262:19 263:1,3,6,14 268:3 269:5,10 269:12 270:14 271:2 273:11 274:2 275:1,17 277:9 283:12 284:1 289:15 290:2,21 294:16 306:1 307:22 329:4 330:20 333:18 335:14 338:12 338:20 340:3 340:22 352:2 366:13 368:12 369:10 378:3 379:3,20 sorts 91:21 soul 192:22 sound 136:22 177:18 328:22 329:1 sounds 88:2 197:20 source 323:13 sources 89:7 214:18 323:13 soybeans 193:15 space 5:2 138:3 304:7 338:15 349:22 spam 188:22 spare 304:2 speak 10:5 20:10 25:11 117:10 124:16 151:22 249:5,7 295:22 303:16 speaker 110:11 speakers 383:4 speaking 14:4 24:5 238:15 265:15 284:7
--	---	--	---	--

360:2	sphere 56:7 85:5	198:9 222:18	374:3	steps 128:1
special 358:18	208:9,21	233:7 354:8	starts 47:11	131:8 132:6
359:1 376:7,13	210:21 211:1,7	358:19 359:22	283:7 379:12	172:12
376:18	spillway 351:2	367:10	stat 157:8	stewards 19:2
specialist 248:3	spoke 164:20,22	standards	state 26:4,5	stick 237:22
specialized	spoken 120:14	111:21 125:16	115:3 138:2,4	353:10
233:9	sponsors 311:11	125:16,20	157:20 187:16	stimulating
specific 36:15	spread 227:12	126:7 153:14	189:17 190:1	275:9
45:21 62:8	springing	163:2 196:19	220:19 302:20	stingrays 15:7
90:11 92:7,14	333:14	200:14,15	348:11 385:5	stockpiling
128:11 168:14	square 142:19	314:11	stated 262:21	111:19
172:15,16,17	squared 32:1	standarized	273:12	stolen 382:12
173:18 182:8	staff 7:14 110:6	232:14	statement	stood 278:8
214:4 220:15	116:21 193:20	standing 327:6	109:14 138:2	stool 345:10
234:15 244:15	242:9 248:7	start 10:6 23:22	276:10 277:6,7	stop 17:22 49:18
262:8 280:12	249:19 250:19	27:11 41:22	318:21,22	77:18,19 105:5
287:22 300:16	253:3,13,16	42:13 49:22	319:3 326:13	207:4,6 263:4
300:21 312:13	254:2,5,8,13	55:4 67:19	326:18 329:17	291:15
336:19 352:7,9	254:17,21	74:12 89:19	statements 99:9	storage 152:13
352:10 359:18	286:14,18	93:4 96:20,22	109:15 136:3	152:13
361:11	303:11 310:6,6	148:12 166:8	224:4	store 148:18,21
specifically	staffer 193:8,13	174:2 191:1	states 51:8	stored 19:8
42:11 68:4	193:16,17,19	192:11 207:5	127:22 193:8	103:13 221:3
98:22 153:19	303:18	250:10 255:7	228:4,6 343:22	storehouse
180:13 182:3	staffers 193:14	257:18 269:10	statistical 164:4	293:9
208:1 240:6,7	254:11 318:8	269:13,17	status 35:18	stories 16:17
247:3 280:11	staffs 245:9	273:13 274:17	37:12 229:22	story 69:2
281:19 311:6	stage 34:1,5,13	275:16,17,18	statutory 265:1	122:18 351:1
314:21 315:1	35:4 92:21	286:1,14,21	statute 301:19	straight 109:15
specification	174:9 372:20	287:6 306:5	statutorily	323:16
272:11 329:6	stages 57:18	312:2,20	281:7 282:11	strange 197:20
specificity 382:3	218:6	318:18 324:20	statutory 5:19	361:17
specifics 279:9	stake 59:10,12	338:13 343:21	122:10 204:17	strangest 59:13
specified 300:22	101:14	347:17 364:1	207:19 240:13	strategic 68:8
329:8	stakeholders	started 139:7	375:21	68:19 69:3
spectrum 205:6	308:21 361:9	198:14 210:19	stenographica...	streamlined
speech 11:3	stand 153:11	242:7 250:11	385:7	132:17
355:7	194:13 233:19	304:6	step 46:18 76:16	street 148:19
speeches 9:15	286:15,16	starting 53:18	129:20 156:1	streets 311:20
spend 30:4	361:9 378:22	54:16 65:7	163:12 177:16	strength 376:12
233:16 239:7	standard 55:21	76:8 96:19	323:4 347:13	strengthen
275:5 313:9	70:17,18 74:16	100:22 159:18	354:19 369:18	225:20 281:7
spent 68:17	75:16 81:5	171:17 219:4	stepping 217:11	strengthening
333:21	82:17 167:4	274:15 283:8	354:13	131:9

stress 246:17	174:21 180:10	55:5	132:19 354:8	242:11 246:14
stretched 346:4	214:11 334:14	suffice 304:3	support 56:5	247:12,13
strict 6:22	348:15 367:19	sufficient 23:18	57:11 104:8	248:5 249:8
114:11 299:20	370:1	195:10 281:4	130:3 150:14	251:9,21
strides 234:8	subcommittee	300:5 341:10	187:3 237:5	252:11 254:21
strike 169:20	117:7	sufficiently	244:4 254:20	256:17 259:13
strikes 30:21	subject 130:8	253:14	312:6 350:4	265:11,18
77:12	137:13 141:18	suggest 132:20	354:20 366:13	267:3 278:13
striking 133:22	219:15 221:14	195:8 200:9	supported 56:1	289:8,12
134:5 337:8	222:15,17,21	236:16 276:14	126:20	303:20 311:13
strive 299:19	281:20 301:1	285:21 311:8	supporting	320:19 340:9
strong 24:14	333:12	381:11	269:21	356:11 379:1
29:17 31:1	submissions	suggested 58:3	supports 227:15	surgical 317:5
111:3,7 115:16	88:6	199:14 381:15	231:4 234:14	365:12
125:6 126:3	submit 6:14,16	suggesting	suppose 42:14	surgically 366:1
196:5 230:6	206:3 255:4	166:21 183:5	107:7 371:3,17	surpassing
235:1 268:5	384:4	288:5 350:21	supposed	111:2
280:18 299:3	submitted 7:10	350:22	272:18 285:18	surprised
369:19 378:22	110:5 318:22	suggestion	320:21 368:22	165:19 179:8
stronger 191:3	383:6	373:10	supposedly	241:11 242:20
195:10	subscriber	suggestions	302:22	290:3 301:13
strongly 29:9	169:7 175:14	165:5 305:6,15	supreme 14:12	surprises 38:2
128:10	subsequent	suggests 28:18	65:5,8 71:16	surprising
struck 53:7,13	131:16	57:10 108:10	76:8 150:14	301:14 330:8
88:22 89:17	substance 8:5	339:20	292:13 369:9	surrender 98:3
253:5 352:3	substantial	suit 298:6	374:1 375:1	surrendered
structure 21:20	36:12 68:13,22	299:17 327:7	sure 10:19 13:12	99:2 150:21
62:11 211:1	253:16	sum 15:1 105:20	18:21,22 41:20	surrendering
240:11	substantially	126:16 148:7	42:13 48:15,18	147:19
structured	302:1	summaries	50:10 61:19	surrenders
228:4 285:12	substitute	301:22	71:3 73:2 76:3	97:16 150:15
structures 258:3	348:12	summary	83:8 93:21	surround 348:5
struggle 197:5	substitutes	105:17	94:4,6 96:3	surrounding
struggling 87:11	288:19	summer 120:7	98:10 102:3	238:11
student 16:18	success 36:2	375:2	107:8 146:2,9	surveillance
145:19 229:11	237:9	super 134:11	157:3,6 159:2	5:12 16:16
students 157:9	successful	174:14	162:20 168:9	20:14,17,19
157:10	267:10,12	superb 287:15	173:7,15 175:3	21:12 23:12,14
studied 181:16	304:12	superbrief 76:5	175:17 185:3	23:21 24:11,18
studies 160:14	sudden 347:11	supervisory	203:13,15,18	32:7 44:14
study 145:1	suddenly 148:9	223:11	208:21 209:21	46:3 52:9,11
176:10	suffer 60:18	supervisory	210:22 211:2	67:13,14 72:16
stuff 120:17	suffered 292:5	219:11	211:19 232:20	81:1,6,18
152:20 154:9	suffering 54:6	supplement	237:18 240:16	84:14 85:5

87:15 127:22	62:11,20 77:3	47:4 52:5 61:9	218:3 219:22	target 35:8,20
128:11 129:7	85:10 112:13	63:20 64:16,17	225:20 238:2	62:6 141:11
130:5,8 148:10	135:8,17 138:4	68:16 72:6	268:13 272:19	174:7 228:16
148:17 153:15	140:20 155:21	75:21 104:5	276:17 326:14	256:14 262:20
167:2 168:13	156:11 157:18	109:2 156:1,13	326:16 330:15	targeted 44:13
180:14 186:6	158:19 170:5	156:16,20	341:12 348:14	67:13 82:6
212:11,21	174:11 183:9	157:7 163:12	382:13,16	181:3,4 230:1
229:19 249:1	187:14 188:21	163:17 170:4,4	talkative 139:4	271:13 301:7
295:18 297:12	190:2,3 191:2	170:5,6 172:7	talked 46:5,8	303:6
297:20 298:1	191:7,19 209:7	177:16 190:7	53:21 54:3,14	targeting 279:2
300:13 301:11	209:8 220:15	225:3 227:1	60:22 63:22	targets 128:12
302:7,9 306:8	220:16,16	231:6 236:5	77:4 142:17	228:9,13 232:6
327:1 363:16	269:18 270:18	239:2 240:22	147:10 154:17	task 204:6
373:21 375:19	270:22 292:4	243:22 247:8	161:2 166:18	tax 13:14 69:9
surveilled 81:4	293:7 295:11	257:17 265:22	167:20 169:9	taxonomy 46:11
surveillance	325:1,9 326:6	268:20 269:1	169:11,17	49:9,20
272:1	346:15,18	272:7 273:15	176:1 178:9,13	teach 311:18
survey 16:12	370:18	276:11 284:7	179:19,22	teaching 313:10
17:19	systemic 316:6	297:18 298:11	180:7 240:19	team 305:6
surveyed 367:1	324:19	303:19 316:8	245:10 256:7	322:1
survive 25:22	systems 37:15	317:17 321:8	268:9 282:1	tease 262:12
suspect 15:17	37:19,22 38:9	323:11 335:1	288:18 310:4	tech 3:3 110:14
329:19	95:19 112:1	347:13 362:10	319:1 326:13	143:10 250:21
suspended	134:17 135:3	362:11 379:13	348:8 373:1,17	technical 36:5
95:13	135:11,18	takeaways	376:7 381:20	36:17 40:22
suspicion 60:13	136:17 140:4	224:2	talking 21:22	41:5,9,10
suspicious 22:19	140:14 142:22	taken 4:19 69:6	29:3 68:15	62:15,17,19
sustainment	146:2,6,9	93:21 126:16	84:18 87:13	63:6,11 68:5
317:11 360:18	157:21 158:3	131:8 132:20	92:10 94:17	69:3 90:21
swath 324:15	158:17,20	169:5 170:18	100:1 101:16	91:5,16 92:1,7
swaths 282:19	170:22 173:1	172:9 205:10	119:13 137:14	95:19 104:8
sweeney 195:13	182:9 183:5	355:2 384:12	152:6 159:3	106:12,12
switch 348:16	185:1 201:16	takes 123:20	165:2 180:13	111:3 237:4,15
switches 39:16	214:15 230:9	171:21 176:21	185:9 203:16	249:14,20
synchronized	245:14,16	342:20 379:6	210:19 216:21	250:18 270:12
316:1	247:14 312:8	talismanically	233:16 271:16	279:13 305:10
synergy 39:6	312:17 315:17	288:11	272:5,17 275:5	309:19 351:22
synthesis 335:6	346:8,8 372:14	talk 9:10 54:20	329:5,6,7	360:4 376:15
347:1	372:18	64:15 67:11	340:2 341:18	378:7,21
synthesized		92:18 99:11	353:18 366:13	technically 91:1
323:10	T	108:1 119:6,17	talks 147:17	114:11 278:9
synthesizes	tagging 348:9	139:5 147:2	374:2	354:15,15
324:16	tailored 260:22	152:5 166:21	tangible 54:6	techniques
system 61:16	take 23:22 37:2	203:17 216:8	55:5 225:1	111:1 113:6

114:19 177:13 232:7 321:13 373:1 technological 25:15,22 40:1 61:21 86:13 90:8 101:2 199:17 227:21 245:11,13 278:1 308:10 340:6 350:1 353:21 379:2 technologies 40:6,14 78:19 105:13 106:4 115:17 143:4 230:8 249:1,2 250:2 303:10 309:11 310:1 318:3 341:3 375:10 381:3 technologist 112:11 115:14 116:2,4,16,18 134:22 160:11 165:4 179:17 193:5 247:17 248:8 technologists 115:22 116:5,7 116:20 137:6,8 144:22 145:6 146:4 154:19 162:10,12 164:18 176:3,7 176:8,11,16,19 237:11 239:6 249:5 316:17 349:11 356:16 357:3 383:10 technology 3:2,5 3:19 6:2 15:7 33:14 39:21 40:9,10 61:12	96:1,3 109:3 109:13 110:17 111:7,8 113:4 113:8 117:5,8 124:14 134:2 135:5,15 137:13 142:12 142:13,18 144:8 146:15 147:8,11,22 148:3,4 149:3 149:16 155:1,6 156:18 158:1 162:2 165:3,11 167:8,11 170:2 174:13,22 201:16 206:16 226:16,18 228:10,22 234:2,9,14,19 234:22 247:17 247:19 248:2,4 248:11,14 250:14,16 251:5 252:10 269:21 277:19 285:16 295:16 296:8 304:12 305:14 306:2,7 307:14 309:20 311:13,19 314:4 315:11 315:18,19 320:10 325:2 326:1 334:5 340:20 344:14 344:15,19,19 348:2,3 349:8 357:9 364:6,9 364:9 373:14 373:17 374:18 374:20 375:5,5 377:10,21,22 378:9,15	379:10,20 380:8,11,13,17 380:19,22 381:1 383:14 technologys 380:21 teenager 68:22 telephone 15:15 102:12,21 103:16 120:7 163:17 television 22:12 tell 98:17,18 123:2 166:20 180:6 184:18 261:15,19 262:3 274:20 274:22 294:6 312:9 314:14 321:5 335:11 343:20 367:3,4 telling 15:13,18 99:13 293:21 303:17 tells 294:4 template 232:14 ten 94:9 167:10 181:22 205:20 288:6 tenants 218:10 tend 66:20 77:16 267:19 tendency 61:1 tends 233:18 310:19 tenet 304:11 tension 161:7 tenth 314:12,15 334:17 terabytes 349:21 term 95:13 97:2 152:4 222:2 260:2,3	termed 54:1 terminology 180:3 terms 34:1 58:2 62:8 78:4 92:14 106:3 143:20 153:2 153:14 154:7,8 157:18 159:9 160:3 161:19 164:17 168:16 184:15 185:22 218:18 223:1 245:15 248:20 252:9 261:3 266:5 277:13 280:8 284:12 291:18,18 315:6 319:19 336:9 339:19 342:11 344:5 348:9 356:17 358:5 359:2,16 361:4 373:8,14 terrible 368:21 terribly 289:9 territorial 220:19 terrorism 111:9 133:6 181:21 182:4 183:4 217:2 296:3 365:16 371:15 terrorismrelat... 220:17 terrorist 15:18 161:16 181:18 349:4 terrorists 36:1,4 110:22 111:17 113:1 166:2,15 tesla 26:6 105:11 106:2 test 147:15	198:6 369:15 testify 33:18 110:20 134:21 303:21 testimony 83:2 116:15 118:19 119:6,17 120:3 121:7 147:1 342:15 testing 231:13 252:13 tests 66:13 text 12:19 136:7 136:7 thank 6:18 7:13 7:20 10:11 18:1 25:3,9,10 33:9 41:13,15 55:6 67:17 74:10,14 80:15 80:15 87:6 88:14 96:8,8 102:1 108:19 109:5,8 116:9 116:13,14 117:1,2,9,10 124:9,10,15,15 134:9 141:15 141:16 142:21 159:14,19 165:13 171:9 171:10 172:5 196:7 202:20 207:1,2,7,17 215:8 216:5,7 216:7 225:8 226:4,4 237:17 237:20 263:9 271:4,5 278:2 278:4,4 284:14 285:9,10 287:8 293:16 295:12 295:13,19,21 296:1 303:7,8
--	---	---	--	---

303:15,16	143:9,10	338:2 348:11	153:19 154:9	199:2 224:22
313:3,8 318:7	147:14 151:17	349:1 350:3	156:15 164:7	251:3,12
322:13 326:7	151:21 152:8	353:5,6 354:2	171:1 172:7	267:17 283:16
328:16 347:16	159:8,21 161:7	354:5,21 356:7	173:6,10 175:6	283:16 287:1
347:19,19	161:10,11,12	357:13,20	177:6 183:9	310:7 311:18
363:1 374:5	161:17 162:1,2	358:13 360:15	184:19 185:19	312:1 315:13
381:6 383:1	166:12 167:6	363:4 366:16	192:22 193:3	326:19 328:9
384:14	169:6,22	366:21 368:11	193:13 197:12	332:19 334:17
thankfully	172:12,15,15	369:8 379:22	198:12,16	334:18 342:3
193:21	172:16 174:14	theme 211:15	207:4 211:5	343:2,14,16
thanks 10:9	174:16 177:11	theoretical	220:2 221:18	344:6 357:6,7
33:17 67:21	177:12 178:4	285:14	253:9 258:4,5	357:8 363:15
107:19 108:22	179:18 181:6	theoretically	258:11 273:19	367:6 370:8
110:19 134:11	184:5,14 185:1	115:18	281:16 292:1	379:1
134:20 159:19	187:2 188:6,14	theory 38:15	292:21,22	theyve 24:10
169:8 284:20	189:6,14,19	76:7 78:5 89:1	293:1,2,2	33:20 106:10
284:22 303:14	195:22 198:4	89:3,11,12,18	308:3 317:1,2	149:14 177:5,7
313:2,6 383:3	199:6 200:17	97:5 250:12	324:13 328:4	289:8,10 367:2
thatd 160:12	206:9 210:14	268:13 368:5	329:1 332:12	371:6
thats 8:7 11:18	218:12 221:6	383:14	337:1 339:22	thin 79:12
12:2 13:20	222:9,15,20	thered 306:18	344:13 346:16	thing 10:14 14:3
14:5 15:10	223:6 224:19	theres 10:14	349:18 351:13	18:18 21:11
18:14 27:14,15	238:9 240:3	12:6 13:12,13	353:15 357:16	46:9 51:4 57:9
27:16,18 29:8	241:2 245:22	14:7 21:13	363:6 364:5	57:15 71:8,11
33:1 46:18	247:8 248:14	23:3 40:17	371:21	78:12 82:16
48:6,16 49:10	250:12 251:18	42:18 43:18	theyll 48:2	91:14 93:6
55:20 60:11,14	252:12 253:3	44:2 48:5,8,17	88:10	94:12 141:2
60:17 63:13	254:13 255:13	58:9 62:15	theyre 8:16 17:1	152:13 156:1,7
64:21 65:16	256:6 258:2,16	64:4,13 71:12	19:18 22:12	156:10,13
66:4,22 70:4	258:20 259:11	75:6 78:21	24:18 30:2,6	166:16 176:15
70:13 71:11	259:20 262:7	79:11 83:21	41:8 45:17,17	198:19 201:13
72:4,20 76:16	265:15 272:6	84:5,8 90:16	54:21 63:6,7	201:15 213:17
78:7 80:21	274:14 275:1,2	91:15,22 96:4	77:18 88:11	242:22 259:16
82:13,18 85:4	275:14 277:10	98:19,20 100:3	100:10,11	261:18 262:3
85:19 87:14	279:5 281:20	103:10,11,17	107:15 126:11	262:10 268:6
88:5,12 91:13	283:8 292:18	103:18 104:13	138:12,13,21	270:17 274:10
99:7,8 102:16	293:15 304:16	108:14 118:11	141:4 147:18	276:19 305:1
103:20 104:2	306:4 307:16	119:3 121:17	158:9 168:2	311:1 321:14
105:8 106:22	311:19 314:2	128:2 130:22	174:8,10,11	322:20 331:1
107:19 113:18	315:3 320:8	133:18 137:17	177:19 182:10	343:4 351:5
118:4,8 121:1	321:11,14	144:19 147:6	187:10 188:8	354:16 355:19
127:21 128:6	322:19,20	149:17 150:13	188:10 191:12	366:11
132:13 137:11	326:21 330:10	151:14,14	191:13,15,16	things 10:17,19
138:19 140:14	334:14 336:11	152:2,7 153:4	191:18 199:1,2	11:21 18:16,19

19:5 21:8,13	334:9 335:3,13	83:13,14,17,19	196:15 197:11	292:1,15,18
25:1 28:12	336:4 339:4,16	83:20 85:2	197:15,20	293:11,13,18
29:15 30:14	349:14 351:16	86:8,9 87:9	198:8,15	294:1,11 295:1
32:17 42:22	356:17,18	88:18 89:10,16	199:14,19	295:2 305:16
43:1 44:11	357:5 359:5	90:1,20 92:8	200:2,13,17	306:6 309:16
46:5 49:17	361:15 379:3,8	93:5 94:12	205:1 206:15	311:10 313:14
50:3 52:3 53:6	381:19	96:4,6,9,13,20	207:20 208:6	314:2,4 315:3
59:13,15 68:9	thingsternet	97:1,11 98:15	210:15,18,20	317:14 319:6
68:9,13 71:6	139:2	99:11,22 100:6	211:14,17,21	319:21,22
84:4 86:9 93:7	think 7:21 10:3	101:1,5,13,19	212:3 213:3,5	321:11,21,22
94:10 95:18	10:21 11:8,8	102:18,20	213:14 220:1,6	327:9,21
104:13,14	14:10 17:16	103:3,21	222:9 225:13	328:19,21
105:3 115:1	19:9,19 20:10	104:12,13,16	225:14 227:20	329:3 330:4,17
128:4 136:18	21:18 25:19	105:3,4,8,9,11	233:20,22	331:5,9,14
138:1,8,9,10	26:3,5,10,12	106:3,15	235:20 236:1	332:8,10 333:5
138:11 139:1,1	26:15,16 28:19	107:20 108:11	241:1,19	333:6 334:2,4
139:16 143:11	28:19 29:6	108:13 119:3	244:11,12,19	334:15,18,21
143:18 144:2	30:9,14 32:3	119:21 120:4	245:15,22	335:5,8 336:5
152:11,12,22	32:11,16,18	120:12,17,19	247:4 248:8,9	336:7,8,11,15
154:14 155:2	33:21,22 36:20	141:19 142:2,8	249:19 250:20	336:18,19
156:19 157:4,6	40:4 42:10,18	143:21 144:13	251:17 252:14	337:1,3 338:4
164:8 170:10	43:18 44:2,3,4	144:19 147:2,7	253:9,10 254:4	338:12,13,15
170:21 171:2,7	44:21 45:19	147:21 148:1,2	254:8,14	340:2,16,21
173:6,16 183:4	47:17,21 48:6	148:11 149:3,7	257:21 258:20	341:3,13 344:4
184:11 185:17	48:6,16 49:20	149:12,13	260:3,4,6,12	344:6 345:3,21
186:3,5 189:21	49:21 50:3	150:12 152:5	261:19,21	346:2,6 347:16
190:22 191:9	51:12 52:1,3	155:9 157:3,8	263:2,15	348:7,16 350:3
191:16 199:12	52:21,22 54:1	159:5 160:20	264:14,17	351:13 352:3
202:6,17	55:7 57:8,12	162:1,2,9	265:15 266:3	352:15 353:9
247:16 250:13	57:17,19 58:20	163:8,11,12,18	266:15 267:4,5	353:11 354:18
251:6,15	59:9,13 60:1,7	164:11 166:5	268:6,6 269:12	354:21 355:10
252:19 257:10	61:3,15,19	166:15,16	270:3,10 274:3	355:14,16
263:4 266:2	62:8 63:14,21	167:11,13,22	274:12,16	356:1,2,7,16
267:21 270:18	64:20 65:9	175:8,21 177:1	275:14 276:6	358:18,20
271:1 272:15	67:8,12,21	177:4,8,9	276:12 277:1,3	359:10,14,17
274:13 279:15	68:14 69:5	178:19,22	277:10,18	360:2 361:7
290:13 303:13	70:2 71:15,18	179:2,4,17,19	278:13 281:6,9	363:9 364:19
304:19 305:4	71:20 72:8,14	181:6 182:21	282:4,11,12,17	364:21 366:7,9
308:15,18	73:5,8,9,20	184:15 185:6	283:2,4,5,6,11	366:14 367:13
309:8,18,21	74:5,6,7,8,12	187:4,7 188:18	283:21 287:1,9	367:18 368:6,7
312:3,15 315:7	76:6,11 77:9	190:2,7,11,18	287:17 288:3	368:8 369:22
316:4 319:2	77:16 79:3,14	191:6,6,7,7,12	288:10 289:5	370:1,10
321:16 324:4	81:2,14 82:20	192:21 193:2,9	290:1,10,12	371:21 372:3,9
329:8 330:9	83:1,5,10,11	195:19 196:3,5	291:9,12,20	372:10,13,22

373:4,6 374:6 374:7,9,14,15 374:20 375:6 375:19,22 376:9,13 377:5 377:7,11,16,17 378:4,6,8,13 379:4,22 380:3 380:4,10,12 381:9,14 382:18 383:7 383:17 thinking 26:6,10 67:22 69:22 81:15 86:11 101:14 143:17 143:18 210:19 229:6 250:4 292:16 295:8 308:9 312:2,15 320:1 331:5 333:22 338:13 352:16 355:1 thinks 179:9,9 229:4 thinner 45:1,1 third 15:11 20:12 34:3 35:4 39:6 91:2 111:13 119:17 130:3 150:16 151:5,17 168:16 229:4 283:14 285:17 291:22 302:3 315:15 345:9 thirdly 97:11 thirdparty 13:21 72:4 97:13 197:13 353:15 thirty 32:13 thomas 136:19 thorough	111:12 thought 32:14 51:4 54:3 55:14 83:4 84:10 87:18 90:7 164:15,16 165:6 184:4 199:16 202:11 216:22 229:11 256:1 261:10 273:2 276:22 319:17 330:17 336:1 344:10 351:7,8 365:10 thoughtful 383:8 thoughts 82:22 87:8 153:4 183:7,18 187:21 189:7 192:17,21 227:4 235:9 257:13 259:22 268:17 322:14 328:3,13,17 366:10 threads 316:6 threat 66:8 67:3 94:17 111:13 114:15,19 115:12,19 199:20 217:13 218:15 226:14 227:20 228:1 threatens 302:19 threats 115:8 133:4,7 227:11 228:6 three 34:1 91:10 111:6 123:14 141:7 205:16 205:19 236:14 263:1 315:2,8	322:10 331:19 346:20 360:16 360:19 threshold 276:15 322:22 thresholds 272:15,15,19 335:7 throw 44:18 63:20 275:17 throwaway 138:18 throwing 307:11 thunderbird 26:2 40:5 tight 159:12 tightly 267:9 time 6:16 9:13 9:20 15:2 17:6 17:7 18:11 30:4 33:3 41:13 49:14,18 60:7 72:14 76:4 80:13 84:2 87:21 113:15 116:21 120:2 123:7,9 135:22 136:16 137:18 138:17 139:6 141:18 144:9 146:1,11 148:13 164:1 164:21 168:1 175:9 190:8 192:11 196:11 205:21 206:2 214:22 215:1 218:4 220:21 223:22 226:8 227:1 231:19 233:16 239:7 242:9 252:15 255:7 275:5	276:13 280:6 286:7 287:9 297:10 310:20 310:22 313:9 319:14 320:15 322:14,20 325:3 333:22 334:5 335:10 336:3 342:20 344:17 346:3,7 347:7,15,17,21 348:4 360:11 360:18 362:12 362:20 363:9 364:7 367:20 368:1,18 370:11 373:19 379:6 380:17 381:7 timekeeper 6:22 109:21 times 39:12 71:18 83:6 110:2 145:3 149:2 159:5 190:16 241:10 257:4 273:12 295:8 343:7 363:5 timewise 75:22 tinker 196:2 tiny 120:10 tipping 256:19 260:2 tips 260:8,9 tire 303:17 title 109:11 219:9 247:3 today 5:17,20 6:19 9:3 25:12 26:3,7 33:18 59:14 61:4 92:10 98:6 105:12 111:6	117:11 123:5 124:16 125:22 134:7,21 151:7 181:22 205:1 205:16 216:21 227:1 234:7 235:20 264:3 269:8 283:10 285:3 295:22 303:16 305:13 306:8 307:14 307:14 309:8 309:14 333:12 347:21 363:5 today's 5:15 7:6 7:17 10:13 33:22 35:10 123:21 340:20 383:22 toes 255:6 token 143:8 184:16 204:14 told 172:20 257:4 ton 178:1,1 tool 195:14 289:2 291:1 339:11 381:16 tools 117:15,16 126:12 133:5 143:16 173:8 175:1 177:13 190:12 233:9 234:9 314:7 320:11 349:11 382:9 top 81:7 82:2 150:4,5 162:7 181:11 272:18 296:13 349:5,6 topic 207:22 216:9 341:17 topics 16:15 383:11
--	---	---	---	--

total 15:1 71:5 148:7	248:2	345:9,10 356:5	trusted 242:10	109:16 203:17
totally 17:18 52:2 298:9 350:7,8	transborder 153:8,15,15 154:16	transparent 89:5 208:18 214:6 298:19	trustworthy 155:17 234:11	252:15 284:10 284:10 326:7
touch 127:8 252:11	transcript 7:7 384:7 385:8	transperancy 212:1	truth 32:8 99:13 361:17	turned 82:8 122:21 202:12 205:18 321:2
touched 170:10 288:2	transferred 90:17	transportation 59:20,22 60:5	try 45:10 56:22 61:20 62:7,19 68:2,6,6	turning 215:9 turns 250:14 252:7 322:8
touching 139:9 139:11	transiting 255:1 transition 60:20 88:20 107:22	trash 307:11	105:21 160:17 165:15 173:14	tweeted 339:9,9
touchstone 69:17 363:20	transitions 101:2	treat 121:18	175:1 178:16 249:19 262:12	twentyfirst 337:17
toughest 327:2	translate 88:19 305:11 340:18	treated 150:8 231:7	269:13 316:9 323:16 340:21	twice 70:9
touted 183:11 183:17	translating 171:14	treaties 51:8,13	348:13 361:13 378:15	twist 337:16
town 296:5	translator 378:14	tremendous 142:19	trying 27:10 68:14 72:21	twitter 136:21 367:22
track 71:16 280:6	transmitted 139:9	tremendously 288:4	82:14 84:22 159:9 161:16	twitters 368:4
tracking 306:19	transparant 208:13	trend 142:4 185:15,19	171:5 175:5 191:18 196:1	two 9:12 30:15 34:14 43:22 58:13 76:17 91:9 105:9,17 110:1 114:17 116:20 119:13 122:4 124:21 140:7 186:2 187:22 194:6 199:10 211:15 217:22 250:17 274:4 276:1 278:8,11 279:11 286:5 306:1 309:5 314:6 326:10 334:9 336:4 345:13 361:2 361:18 362:1 371:4 372:19 380:9
tracks 222:18	transparency 23:2,10 28:5	trends 144:16 186:7 187:22	199:17 213:7,9 239:8 242:3 243:6 247:10	type 31:16 129:21 168:11 239:5 248:18 251:10 262:17 302:10 331:16 370:19
trade 216:12,15 314:1	31:13,14,17,18 31:20,22 32:4 32:9 84:5 85:8 85:15 86:2 89:4 125:22 128:22,22 130:11 152:16 163:8 164:17 165:10 204:16 207:12 209:6 210:17 211:9 213:15 214:2 214:13 215:2 220:7 271:19 272:3 274:8 280:14 298:16 301:10 302:1,4 303:7 327:16 337:18,19	tribal 220:19	251:14 256:2 263:15,21 264:10,12 275:3 289:3,5 291:15 313:21 315:17 316:19 320:2,3 328:22 334:3 342:12 343:14 344:5 345:7 376:11 378:18	
tradecraft 187:17	tribe 36:1 85:12 137:19	tried 36:1 85:12 137:19	345:7 376:11 378:18	
traditional 204:9 232:4 274:8	trigger 60:13	trillion 141:7	tsa 58:14 59:16 83:13	
traffic 39:10	troops 227:15	troubling 80:12	tssi 193:8,15,16 193:22 201:6	
trail 276:18	true 17:9 48:6 99:7 130:13 151:21 336:19	truly 40:20,21	tuning 182:18	
trails 93:3 94:4 319:2	trump 66:14 67:9	trust 24:10 58:1 58:4 85:15 115:12 125:7 125:11,12,14 127:12,17,20 128:5 135:16 247:12 249:11 265:13 266:13 300:7	turn 7:18 28:18 34:21 36:22 37:7 61:22	
train 174:5 214:15	trust 24:10 58:1 58:4 85:15 115:12 125:7 125:11,12,14 127:12,17,20 128:5 135:16 247:12 249:11 265:13 266:13 300:7			
training 94:22 127:5 172:12 172:14 173:20 215:3 244:15 378:4				
transaction 331:7				
transactional 152:1 320:4				
transactions				

types 45:21 46:12 56:11 85:7 103:11 169:7 219:12 230:5,5 235:17 235:21 236:4 236:11 268:10	unanimity 97:12 unanimous 133:15 unavoidable 360:7 unbelievably 291:1 unbiased 378:15 unclear 291:7 uncomfortable 269:4 363:13 363:16 378:22 unconcerned 45:6 undercut 377:2 underlie 55:22 285:15 underlies 28:16 underlying 28:21 56:6 57:11 84:22 85:3 101:14 243:20 333:18 undermined 127:12 underneath 270:1 underpinning 274:14 underpinnings 285:14 understand 29:1 36:19 37:20 38:1 89:11,12,13 157:12 158:2 165:21,22 178:6 183:14 195:22 235:3 242:14 245:5 245:14 247:14 249:11,17,18 252:11 279:12 279:13 294:9	328:10 353:8 355:2 360:4 367:21 368:2,4 379:7 380:13 understandable 375:11 understanding 107:9 129:21 239:7 242:2 244:22 249:1,2 251:10 264:4 279:1 291:4 340:4 344:8 377:9 380:8 understands 328:8 understood 196:10 underwent 30:20 undesirable 40:16 undue 362:8 unduly 8:8 14:10 unencrypted 162:4 unfolded 122:19 unfortunately 44:13 62:16 unfortunatly 205:17 unique 34:10,16 39:9 234:10 uniquely 205:1 unit 240:3 281:15 united 51:8 127:22 193:8 343:22 units 228:5 universal 51:6 98:7 universe 298:4	universities 144:4 university 2:12 2:15 3:3,18 110:14 117:5 287:3 unjust 310:22 unknown 90:5 unlocks 37:7 unpleasant 38:2 unpopular 140:18 268:1 unreasonable 42:3 64:13 72:10,13,17 369:1,4 unremarkable 36:14 unrestrained 298:3 unscientific 17:19 unsolicited 358:15 unsurprising 315:20 untenable 32:11 unusual 186:3 unwilling 108:11 update 168:12 updates 374:12 upfront 358:9 uphill 243:6 uploaded 139:21 140:2 upset 265:22 upsets 302:21 urge 124:8 128:17,19 130:14 377:3 urges 303:1 usa 212:6 usable 138:16	usage 38:21 322:12 use 18:20 27:15 38:14,14 39:10 40:13,15 46:5 52:3 55:13 61:12 63:4,10 68:5 69:1 77:14 78:19 82:17 86:11 87:20 91:17 94:8 106:5,9 106:11 113:1 115:16 118:17 121:10,13,22 122:12 123:2 123:19 124:3 125:10 126:1,3 126:9 131:9 145:19 150:22 152:9 155:12 157:11 162:6 169:21 170:12 170:13 171:3 174:11,13 184:10 188:2 198:21 222:9 222:15 226:20 231:18 236:4 236:11 237:1 248:16 257:22 267:10 274:17 276:7 288:10 288:13 290:20 291:10 292:2,6 292:17 294:21 298:11 300:10 305:22 306:3 308:15 309:22 310:12 312:8 312:15 315:19 320:10 321:9 321:12 323:12 323:13 324:14
<hr/>				
U				
u 3:13 36:4 127:19,20 128:4 129:10 129:14 131:15 131:17 132:1 132:12 133:2 164:5 230:2 278:22 279:2,3 279:21 289:9 292:4 301:8 302:10 343:17 369:7 uavs 78:20,21 ubiquitous 50:18 147:19 148:16 186:5 379:10 ultimately 23:13 74:8 226:19 240:10 316:13 316:20 323:8,9 372:15,18 umbrella 97:2 unabated 364:11 unable 370:20 unacceptable 271:1				

324:19 329:7 338:3,5,6 341:9,18 342:1 342:6,14 344:16 350:10 351:10 363:17 364:8 365:11 365:15 372:12 372:21 380:22 381:2,20 382:16,16 383:12 useful 62:1 114:6 115:10 118:8 119:4 134:5 195:14 195:16 259:14 259:15 273:21 274:1 276:3 288:4 289:22 293:20 296:15 296:17 332:1 332:10 333:5 344:22 366:16 367:4 368:15 381:16 user 39:15,19 79:17 201:21 users 39:11,16 39:20 112:16 156:8 157:7 237:1 uses 15:6 35:4 71:9 121:15 214:19 222:17 234:15 236:7 236:12,13 262:21,22 294:13 322:9 362:7 usp 164:10 usually 39:19 147:16 229:22 utilitarian 26:22	29:14 50:22 51:4 68:15 72:9 utility 367:11 utilizes 204:20 uttered 66:14 <hr/> V <hr/> v 133:14 vaguely 269:16 vagueness 157:17 valid 97:20 260:19 validated 227:8 valley 135:1 136:13 valuable 27:5 93:8 195:6 197:12 198:5 207:14 291:1 361:6 value 9:2 11:4,6 15:19 17:20 26:11,16,20,22 28:15,21 29:14 50:19 51:5 54:9 55:12 64:4 69:13 77:6,7 85:3 98:21 116:19 117:19,22,22 125:5 132:21 133:16 144:8 214:1,4 222:1 233:1 244:11 265:19 266:6 266:10,17,20 270:10,11 284:11 291:13 312:5 331:2 358:8 381:20 values 8:5,15,17 26:21 27:8,22	55:22 56:1,6 57:12 67:6,11 84:22 97:3 118:5 209:3 234:19 331:17 357:18 varied 9:4 180:3 variety 50:16 230:16 237:10 246:2 247:15 304:8 308:5 various 46:12 76:12 104:14 105:3 163:22 241:7 255:19 325:18,20 346:1,21 373:1 vary 95:8 varying 8:16 196:11 vast 21:14 53:14 64:20 vehicle 40:7 velocity 50:16 venture 313:5 venue 313:13 verify 247:13 verizon 293:3 version 75:17 88:3 100:3,4 326:17 versus 114:11 336:5 369:7 vetting 263:16 263:22 viable 327:5 victims 113:22 183:15 video 139:20,21 140:2 167:2 329:16 view 13:21 32:10,11 33:15 63:2 81:12	98:1,1 132:2 151:22 171:14 192:6 210:12 212:12 214:1 241:1 296:18 299:11 322:15 324:20 339:21 340:10,11 342:9 351:6 376:8 viewing 338:17 370:1 views 19:11 54:8 96:17 231:15 284:19 333:17 vigorously 154:4 339:5 village 76:21 violated 29:10 violation 15:10 281:4,19 violations 15:11 16:22 281:10 281:11 327:7 violaton 222:20 violence 160:4 161:22 270:6 virtually 30:6 virtue 14:2,15 visavis 11:1 45:8 188:10,12 vital 214:20 379:5 vivid 36:15 vocal 127:21 voice 10:11 243:3 244:17 284:4 void 51:14 volume 37:11 50:15 129:21 228:19 280:9 289:14 volumonous	269:9 voluntarily 219:5 voluntary 273:6 volunteered 122:8,9 vote 4:19 384:12 voyeurism 31:21 vulnerabilities 49:11 vulnerability 16:6 vulnerable 121:12 123:19 <hr/> W <hr/> w 1:13 wade 257:20 wait 115:18 201:9 353:18 372:11 waived 122:14 wald 2:5 4:15 7:19,20 10:10 18:1 25:4,9 33:8,11 41:15 43:8 45:10 50:10 51:2,15 51:22 53:2,4 53:20 57:14 60:21 62:22 63:19 67:17 69:4 71:2 74:10 75:21 80:14,18 87:7 88:5 96:6 102:2 103:9,21 105:9 106:14 106:18 107:3 108:16,20 175:20 177:18 178:7 179:12 179:19 180:16
---	---	---	---	---

181:3,6 199:9	279:6,8 283:19	197:1 363:12	307:20 309:7	111:20
200:19 201:1,4	287:16,21	wasnt 65:11	327:4 328:22	weakens 166:1
201:9 202:8,20	297:3,11 306:5	181:18 199:22	329:21 330:4,5	weakness 292:3
255:8,12 258:7	309:4 333:13	307:3 358:3,3	332:5 334:21	weaknesses
259:4,7,10,13	335:9 344:1	358:5,6	335:2,8 336:11	342:16
372:8,9 374:6	354:3 356:18	wasted 68:18	336:14 337:12	weapon 111:5
377:5,14	360:14 367:22	watch 183:22	338:7 345:3	weapons 56:22
walk 304:21	368:2,4 374:4	198:16 369:17	347:22 348:3	227:13 365:17
379:20	374:16 379:15	watched 280:12	351:7,14	wearables
walking 14:2	380:15 382:4,9	watchers 21:13	352:20 353:20	185:17
273:21	wanted 46:13	wave 287:11	354:21 355:10	wearing 164:22
want 6:18,21	47:15 61:16	way 8:10 11:16	355:22 356:9	web 220:10
7:13 20:3,4,4,9	87:14 89:19	17:1 19:3	358:14 359:9	website 7:8 39:9
21:9 22:7 24:6	102:10 142:1	21:16 28:2,19	364:9 373:22	384:8
46:15,18 47:20	180:16 201:10	31:10 32:9	374:4 377:12	wed 146:5,6
47:20 48:7	218:3 220:14	41:2 56:5,9	377:15 378:15	176:13 318:4
51:3 53:8	237:22 262:9	57:11 61:14	380:5 381:16	330:20
63:21 64:8	263:12 273:13	62:12 63:7	382:5,19	weeds 218:5
69:20 76:16	305:13	64:21 67:8	385:10	week 7:8 120:15
83:1,12 86:15	wanting 329:20	78:6 97:22	ways 16:21 21:5	157:8,9 224:13
87:17,19,22	wants 63:3 73:3	98:1,6 113:9	21:17 24:3	373:19
88:4,9 91:1	75:21 106:8	115:4 121:18	26:9 49:19	weekly 184:20
93:14 98:15	264:22 367:18	124:6 125:18	68:1,16 69:16	weigh 52:5,22
99:3 104:16	379:19	144:12 145:4	74:18,21 89:6	53:6 66:18,20
108:1 115:2	war 122:6,7,15	145:10 150:11	99:15 116:11	67:1,5
120:3,13 133:4	122:18 187:6	164:17 172:22	147:16 148:11	weighing 33:5
143:21 146:21	228:2	173:2,11 175:6	149:14 163:9	232:22
147:1 156:9	warning 110:2	175:22 183:6	164:11 165:9	welcome 4:2
158:22 160:4	warrant 29:18	190:2 191:20	184:16 191:15	7:10 134:18
169:9 181:14	53:10,16 54:7	192:4 197:6	199:5 214:3	162:11 181:13
185:10 189:9	65:11,13 70:18	198:16 200:4	215:2 240:17	203:9,10 225:7
192:5 194:2	71:21 73:1	200:16 201:17	240:18 244:20	237:14 375:22
198:3 202:2	81:21 132:11	201:21 202:6	258:4 261:2	376:1
206:22 207:1,7	167:22 168:6	202:13 209:1	265:14,20	welldefined
207:17 215:5	168:10,21	210:21 211:5	277:20 279:7	155:2 158:13
235:20 239:2	169:5	224:19 229:6	280:17 295:7	wellunderstood
243:22 248:11	warranted	230:12 242:5	307:22 319:5	14:6
250:7 257:12	366:2	258:12 260:6	334:6 337:17	wellwritten
263:4 265:5,18	warrants 42:4	260:12 261:3,9	339:3 350:12	351:19
267:11 269:3	70:11	265:12 271:20	371:4 373:13	went 45:13
269:18 270:17	wartime 123:11	276:7 283:20	374:21 379:20	80:19 160:16
270:21 271:8	washington	285:12 287:11	weak 24:11	161:11 175:3
273:15 275:16	1:13 2:15 4:7,8	289:7,22	weaken 111:21	175:12 304:20
275:21 278:6	18:4 130:19	294:22 304:14	weakening	315:2 374:11

westend 4:6	292:7	women 35:21	328:14 329:14	312:16 331:8
weve 15:12 32:9	wherewithal	270:6	349:19 356:17	331:12 335:19
51:13 58:6	195:3	won 278:14	356:18 371:20	339:11 356:22
92:3 95:18	whispers 164:19	wonderful 99:8	373:19	361:17,19
126:16 127:4	wholesale	143:6 167:6	worked 127:12	363:18
127:12,21	108:12	wondering 55:1	136:5 156:18	worried 178:3
128:4 129:4,13	wholl 367:20	82:11 259:21	176:17 226:1	258:13 266:18
129:18 131:7	wholly 315:10	271:21	289:9 303:18	304:22
132:11,15	316:11	wont 15:20,21	worker 59:22	worry 15:14
150:3 154:17	whos 60:4 175:4	105:21 191:17	workforce 45:4	18:10 22:17,18
168:4 169:5	196:1 220:10	366:15,19	171:19,20	43:15 68:11
172:9 173:6	250:19 256:14	word 27:7 31:12	172:11 214:16	120:16 147:7
203:13,19	285:1 328:18	71:2 248:15	working 12:11	161:13 176:7
229:5 232:13	wide 282:19	words 66:14	144:3 145:20	349:9
235:19 262:11	319:1 364:12	108:18 211:8	205:9 213:16	worrying 20:10
262:14 263:1	widely 204:8	218:11 240:11	239:6 242:12	worse 138:6
269:2 284:3	283:3 337:15	256:20 257:3	242:17 250:3	worst 13:20
285:12 320:18	willful 95:9	262:18 329:13	250:20,22	16:21
331:13 337:16	222:11	330:8 331:2	251:12,13	worth 26:22
337:17 341:18	willing 8:16	350:20 355:11	252:5 275:8	227:6
343:9 349:9	13:18 41:11	work 38:1 62:19	283:12 311:7	worthless
350:22 366:21	85:17 87:13	88:21 91:15	312:18 347:5	117:20
367:1 373:1,17	101:5 106:9,10	95:3 99:15	workings 129:7	wouldnt 64:5
383:7,8,11	282:12	100:15,15	works 54:12	82:19 149:18
whack 63:20	willingness 95:6	132:22 133:2	83:10 89:14	180:11 202:9
64:16	willynilly	140:6 143:9,9	153:16 189:18	307:6 318:15
whacks 64:18	107:14	145:17 148:19	227:14 251:22	355:18 380:15
whatnot 247:10	wilson 7:14	148:20 154:10	251:22 295:11	381:4
whats 23:7	wind 346:17	182:10 189:14	304:5 356:10	wrap 9:13 96:10
24:21,22 25:1	winn 6:15 7:16	189:19 195:20	world 13:10,19	134:8
28:14 51:15	winning 8:6	200:14 205:15	28:12 32:12	wrapped 59:15
75:17 76:6	wins 19:18	207:10 217:6	55:15 110:21	wrapping 207:5
78:4 81:12	wiretap 166:11	224:7 234:12	122:7,18	wrestling
84:9 93:12	wish 135:5	238:17 240:5	131:21 132:2	368:17
98:11 123:18	177:21	241:3 246:7,11	133:9 135:19	writ 66:20 67:5
126:16 160:8	withhold 14:9	246:20 255:14	135:21 136:16	67:6 333:9
176:14 177:15	withstand 101:2	270:1 273:15	136:20 137:5,5	write 88:10
192:18 244:22	112:14	273:17 274:15	137:22 140:9	136:20 145:9
250:21 251:5	witness 117:3	283:15 284:8	153:9 158:12	286:18 318:11
256:19 326:4	124:11 385:12	289:12 296:1	166:5 187:6	378:18
330:21,21	witnesses 96:9	308:11 314:3	190:4,5,9,15	writer 102:9
364:21 379:21	96:19 99:21	317:11 319:2	191:9,16 198:1	104:5
380:2	109:16,19	319:13 327:1	237:8 250:22	writers 16:13
whatsoever	woman 37:8	327:12 328:7	289:13 304:8	writing 16:15

83:2 312:12	year 7:12 128:2	166:21 182:14	1	2014 1:7 4:5,10
writings 61:4	129:10,15	194:2 199:7	1 2:9 7:5,20	16:8 75:17
written 6:14 7:9	130:19 217:20	212:19 220:2	203:1 352:11	385:14,19
9:20 30:15	232:14 284:3	241:21 258:13	10 109:2,3	215 30:17 60:14
64:3 118:19	384:6	259:2 260:8,13	284:17 379:13	90:1,9,14 92:3
119:6 121:7	years 10:16 94:9	261:20 265:18	385:18	103:5 128:16
144:6 145:4	123:14 124:13	265:19 270:2	100 352:8,11	175:10 181:1
146:22 195:13	125:2 128:6	272:17 273:8	11 217:12	201:5 257:3
223:13 240:21	137:15,16	276:14 277:22	12 1:7	278:20 279:9
276:2 318:10	149:6,19	279:2 283:5	1200s 76:22	301:4,11,16
318:22 319:3	153:20 157:3	287:10 305:1	1221 1:13	314:20 330:11
326:13 328:5	163:13 167:10	310:15 312:10	12333 82:6	351:17 354:3,4
328:18 384:4	177:2,2 181:22	315:17 318:14	164:7,10	360:14 365:9
wrong 71:16	227:19 229:9	320:12 323:17	229:18 271:14	369:5
93:16 107:16	230:15 288:6	332:3 338:15	278:22 301:5	21st 4:10
166:20 193:9	306:12 311:20	347:9,11	364:17	22nd 1:13
294:20 322:4	322:9,10	348:16 349:16	12th 4:5	25 229:9
328:20 330:7	360:18 361:2	349:20 350:10	14 338:19	27 141:8
331:21 353:9	379:13	351:2 353:18	15 7:5 109:2	2703 169:3
369:22	yellow 9:11	357:18,20	167:10 203:1	29th 137:4
wrongdoing	110:1 207:5	367:4 371:12	230:15 284:18	
281:2	286:4,5 293:15	378:9	379:13 384:14	3
wrongful	293:17 370:12	youtube 139:21	1942 122:13	3 3:9 88:18
222:21	yep 277:6,8	139:22 140:2	1970s 25:21	110:10 141:8
wrongly 52:4	yesterdays	youve 16:4	73:22 210:9	30 1:14 4:5
wrote 45:12	123:22	30:15 61:3	1973 26:2 40:5	109:3 163:19
46:8 119:12	yield 112:13	105:15 108:20	119:12	315 361:1
288:7	189:8	120:14 149:7	1980s 329:4	
	york 241:10	248:22 249:22	1989 14:12	4
X	youd 255:4	273:1 289:4		4 3:16 384:14
x 183:22,22	307:2 318:9	297:10 313:13	2	40 224:8
184:1,3,4	youll 41:4 69:1	322:1 353:9	2 3:1 284:18	45 284:18
363:14	69:2 177:2	354:10 383:16	303:19	47 16:9
xyz 202:1	271:7 286:5		20 9:16,17 41:16	484 104:8
	287:11 293:17	Z	74:11 141:19	4g 136:22
Y	335:16	z 363:14	157:3 286:9	
y 363:14	young 17:7,8,9	zero 151:3	2005 181:15	5
yall 238:1,2	17:19	zeroday 111:19	2007 123:11	5 110:10
yeah 136:9,11	younger 338:16	zones 40:9	137:4 158:12	50 70:12 157:9
147:14 157:11	youre 68:14	zoom 170:19,19	2008 100:5	157:10 306:12
162:20 168:3	69:18 77:19	170:19	217:18 271:16	363:13
168:22 187:21	83:13 99:12		2011 123:13	51 196:22
188:1 200:20	100:18 150:19	0	2013 141:7,10	520 16:12
281:9 339:12	152:13,22	0 303:19		

<hr/> 6 <hr/> 60 39:18 329:14 62 227:19 622 17:11 623 17:12 <hr/> 7 <hr/> 700 220:8 702 31:3 163:11 163:21 164:5 174:3 213:19 256:9 278:22 279:10,19,20 300:11 358:1 74 163:1 75 39:18 163:1 <hr/> 8 <hr/> 8 1:14 4:5 <hr/> 9 <hr/> 9 217:12 99 352:8				
--	--	--	--	--