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

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 Scool of Law

SESSION 2

Privacy Interests in the Countertrrorism Context
and the Impact of Technology

Annie Anton, Georgia Tech University

Alvaro Bedoya, Geogretown Center on Privacy & Technology

Michael Hintze, Microsoft

Hadi Nahari, Chief Security Architect, NVIDIA

SESSION 3

Privacy Interests Identified and Addressed
by Government Privacy Officials

Alex Joel, Office of the Director of National Intelligence

Erika Brown Lee, U.S. Department of Justice

Rebecca Richards, National Security Agency

SESSION 4

Applying Lessons Learned from the Private Sector

Fred Cate, Indiana University School of Law

Harley Geiger, Center of Democracy and Technology

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

PROCEEDINGS

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

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

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

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

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

(Vote taken.)

MR. MEDINE: We will proceed.

So what is privacy? The right to be left alone? A desire for independence of personal activity? The right to make decisions regarding one's private matters? Space for intellectual development, anonymity or obscurity? Freedom from public attention? Freedom from being observed or disturbed by others? Freedom from intrusion into one's solitude? Avoiding public disclosure of private facts about yourself? Freedom from publicity which places you in a false light? Freedom from appropriation of your name or likeness? Control of how one's personal information is collected and used? Freedom from surveillance.

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

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

There will be four panels today. The first will focus on defining privacy interests. The second will consider privacy interests in the counterterrorism context and the impact of technology.

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

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

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

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

I also want to note that we have a strict timekeeper, Joe Kelly, sitting in front, and so panelists are encouraged to keep their remarks brief so we can have a more extensive discussion.

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

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

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

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

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

MS. WALD: Thank you. Panel 1 will attempt to explore, I think it would be too ambitious to say define privacy, and the many separate individual and societal interests that the notion of privacy encompasses.

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

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

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

Thus, the law of privacy consists mainly of a series of situations in which courts, legislators or government officials have decided to recognize a privacy interest, or not to, and to protect, or not to, that interest against a competing value.

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

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

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

After that, and I hope there will be some time left for the written questions which members of the audience are invited to send to the people who circulate to collect them, and then I will question them. I will discuss some of those questions with the people on the panel.

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

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

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

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

David gave a very comprehensive list of some of the things that privacy is. I'm not sure what I would add to that, except to say that I think that for those who are outside the ideological mainstream in this country, privacy vis-a-vis the government can be critical to effectuate other rights, such as the freedom to religion, speech and association.

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

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

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

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

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

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

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

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

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

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

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

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

Second, you don't, in fact, relinquish

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

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

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

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

This is such a commonsense concept and it deserves a home in Fourth Amendment jurisprudence. The sum total of a person's movements in public over extended periods of time may be publicly available information, but using normal powers of human observation it is practically obscure.

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

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

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

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

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

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

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

In some ways these are some of the worst harms that come from privacy violations because they're society-wide. They impact the way we function as a society. They impoverish our social discourse by causing people to sensor themselves and not put ideas out there.

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

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

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

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

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

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

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

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

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

It involves making sure that when data is kept, it's kept accurately. It's making sure that people who keep the data are responsible stewards of that data, that people have rights in that data and some participation in the way that data is used.

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

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

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

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

But, in fact, privacy isn't just an

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

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

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

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

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

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

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

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

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

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

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

The fourth point I'd like to make is that we can't adequately balance privacy and security without a reasonable amount of transparency.

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

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

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

My last point is that the government must get buy-in from the people for its surveillance measures. Without buy-in, people are going to start to take self-help measures, which is something that we see happening now.

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

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

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

And if they can evaluate what's going on and buy into what's going on, things will be a lot better when it comes to balancing privacy and security. Thank you.

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

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

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

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

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

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

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

Rather in my judgment privacy is an inherently instrumental value, one that acts in the service of other societal values. It's a utilitarian value that derives its worth only insofar, in my judgment, as it fosters other positive social gains.

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

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

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

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

Privacy is also about restraining government misbehavior, which is why we see privacy values in the Fourth Amendment and other procedural limitations on government action, another way in which privacy is obviously relevant to this Board.

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

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

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

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

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

It means we need to go to a micro level

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

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

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

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

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

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

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

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

It strikes me that that sort of pervasive collection is one that would require a strong, independent review mechanicism because of the comprehensiveness of its activity.

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

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

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

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

But absolute transparency, as Dan said,

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

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

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

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

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

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

MS. WALD: Okay.

MR. ROSENZWEIG: Thank you. My apologies.

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

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

We can think of today's data practices

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

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

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

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

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

One file might contain detailed

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

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

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

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

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

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

By contrast, a predictive model that

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

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

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

To understand what follows from collecting an item we have to think about how that item can be merged with other available data, and how the merged data can in turn be used to infer information about people. We have to take into account the avalanche effects that can occur both in merging and inference.

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

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

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

The sheer complexity of these systems makes it very difficult to understand, to predict and to control how they behave. Even the people who build and run these systems often fail to understand fully how they work in practice, and this lead to unpleasant surprises, such as compliance failures or data breaches.

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

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

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

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

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

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

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

My final point is that technology offers many options beyond the most obvious technological approach of collecting all of the data, aggregating it in a single large data center and then analyzing it later.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

That said, I think companies, the line between big companies in this country and governments is getting thinner and thinner. And, you know, certainly companies might have some political axes to grind with respect to the workforce, and they certainly have access to people's information.

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

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

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

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

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

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

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

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

It doesn't mean that the activities that cause them are bad, but it does mean that they do cause the problems we need to address.

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

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

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

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

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

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

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

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

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

One is identification, the fact that

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

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

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

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

But these are just some of the ways that the taxonomy addresses this problem. I think it's important to think of the overarching point is don't start with some platonic concept of privacy and see, you know, what fits in it and what doesn't.

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

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

MS. WALD: Yes, sure.

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

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

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

MS. GOITEIN: Sorry.

MS. WALD: Yes, go ahead.

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

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

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

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

MR. SOLOVE: May I make one small point?

MS. WALD: Yes.

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

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

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

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

MS. WALD: All right.

MS. GOITEIN: Very quickly.

MS. WALD: Briefly.

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

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

MS. WALD: Mr. Rosenzweig, your approach, and you talked a little bit about this, your approach for balancing privacy and national security has I think been termed, whether you call it instrumental or consequential, but in one of your articles you talked about you thought limiting the right of somebody to complain or to go to court, etcetera, to intervening on the basis of when they are suffering a tangible harm, like a warrant or being called before the grand jury, as opposed to Professor Solove's views of privacy as a kind of foundational value, recognizable in its own right.

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

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

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

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

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

Now granted, that's an impossible standard, but if that were the instance then in the long run the values that underlie, the democratic values, would be supported and people would no longer fear the collection because the lack of adverse consequence, or by hypothesis, a hundred percent would have gone away.

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

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

We arm police officers, even though we know that they will sometimes misuse their weapons. We don't eliminate that. We try and drive down the error rate as much as possible so that we engender people's confidence in the police.

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

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

MS. WALD: So let me just pursue one thing that you brought up earlier, which has come up in some of our past reports and is bound to come up in future ones, I think, and that is at what stages, if you would go into a little bit more into the point at which you think an independent review of decisions outside of the government's internal auditing and processes are necessary to ensure that you have this kind of trust by the people that the government is not taking risks to its privacy, and in terms of what you yourself suggested that history has got some lessons for us on the "trust us" aspect.

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

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

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

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

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

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

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

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

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

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

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

MS. WALD: Good.

Mr. Felten, you talked about the

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

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

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

MR. FELTEN: Sure. Well, I think the first principle would be to try to look beyond the most brute force technological approach, which is collect all the data that might turn out to be useful and retain it all in a single large data center for as long as you can.

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

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

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

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

MS. WALD: Who should do that, the

government or private industry?

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

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

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

MS. WALD: My last question I'm going to throw out, and you can all take a whack of it if you want to, but several of you, and I think you especially, Ms. Goitein, have talked about the element of control of information as being essential, but then some other people have written in the field said, well, that certainly can't be an absolute value. There's got to be balance. I mean we wouldn't be able to have the kind of national security programs if indeed everybody said, well, I'm keeping control over that piece of information because I don't want anybody to have it, etcetera.

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

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

MS. GOITEIN: So as I said before, I think in the vast majority of circumstances, and that's the way it should be anyway, the drafters of the Fourth Amendment did that balancing for us and gave us what the government had to do to override the privacy right, and that is to show probable cause of criminal activity.

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

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

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

But Congress has a role as well. And when Congress does the balancing on behalf of the people, I would agree with what I believe Dan said, which is that this is a choice for the public to make. This needs to be a public choice and it needs to be an informed choice, not a choice that's made in secret by a small number of officials, but by the public, because this is a democracy.

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

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

And Julian Sanchez from the Cato Institute made an excellent point, which is when you look at how courts weigh national security against the individual interests in question, they tend to weigh national security writ large over that person's particular interest in that information. And that's not the right comparison. You either need to weigh that person's particular interest in that particular information against the incremental threat to national security in that case, or you need to address national security writ large, weigh national security writ large against the values that privacy serves in our society.

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

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

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

MR. FELTEN: Okay, thanks. I think in thinking about these issues of control, it's important to recognize the ways in which people try to reassert control, even if they don't have it legally.

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

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

And those costs can often be substantial. Just ask any teenager about their online use and what you'll hear, and privacy, and what you'll hear is an elaborate story about technical countermeasures and strategic behavior.

MS. WALD: Paul?

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

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

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

You know, I'm sitting here as a Republican on the panel thinking of all the friends I have who are Second Amendment people who think that the government should not collect any information about their gun ownership. And, you know, that's a perfectly reasonable position for them to have. It's not one that we currently accept as society.

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

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

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

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

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

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

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

In fact, I think there are a lot of exceptions to the warrant requirement, a lot of instances where the Fourth Amendment doesn't even get applied at all because the court has this platonic conception of privacy that is incredibly narrow.

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

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

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

And that's really what the Fourth Amendment is trying to impose there, either justification to gather information, such as a warrant and probable cause, or appropriate oversight to make sure that an independent judicial body looks at what the government wants to do and evaluates it.

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

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

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

And I think all branches should be playing a role and have a role to play in this. Congress in the 1970s at the Church Committee, which did an extensive review of intelligence agencies, produced a very illuminative public report about that.

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

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

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

MR. MEDINE: Great, thank you.

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

In some ways in the computer age we're beyond that, which is that the court file that was gathering dust now is easily accessible and public.

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

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

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

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

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

MS. WALD: Well, whoever wants to take it. I might note that time-wise, we're going to have about five minutes per, so if you can keep your answers or your comments relatively brief, we can make sure that everybody gets their full component of time.

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

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

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

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

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

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

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

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

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

So it's got to be when the government chooses to aggregate it or perhaps chooses to act upon the aggregation. And as between those, I don't have too much choice.

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

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

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

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

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

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

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

MR. MEDINE: And therefore should the government not collect the information under those circumstances?

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

MR. MEDINE: As a policy matter.

MR. FELTEN: As a policy matter?

MR. MEDINE: Yes.

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

MR. MEDINE: My time has expired.

MS. WALD: Rachel Brand.

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

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

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

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

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

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

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

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

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

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

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

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

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

MS. BRAND: Okay.

MS. GOITEIN: I have some thoughts but I

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

MS. BRAND: Okay.

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

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

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

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

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

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

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

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

But the challenge for you is going to be trying to figure out what the underlying values are and how to get at those.

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

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

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

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

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

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

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

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

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

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

MS. BRAND: Thank you.

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

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

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

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

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

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

Okay, Ms. Cook.

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

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

But I was also struck by the numerous

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

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

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

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

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

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

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

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

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

And I think it's pretty clear that as a technical matter the kinds of linking, looking for, say, multi-hop links that the intelligence agencies want to do, can be done technically while the information is still held by third parties such as the phone companies.

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

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

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

And those sorts of methods are, I'd say developing, and there's been some interest in the technical problem of how to do this in the independent research community in light of what we've learned publicly about the Section 215 program.

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

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

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

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

What have you found to be the most

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

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

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

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

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

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

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

Training in the first instance so that

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

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

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

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

And this is a case where oversight can operate without needing to get deeply into the nuts and bolts of the technology, just the question of what processes are in place to make sure that your technology does what your general counsel says it should do. And I think there's an opportunity to push on oversight in that area.

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

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

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

I heard actually a lot of commonality among the witnesses, starting with the point that I think you all agree, whether you start from the premise that privacy is a human right or whether you start from the premise that it's an instrumental right, I think all of you agree that it's an umbrella term which covers many different values, many different interests.

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

MS. GOITEIN: Let the record reflect nodding.

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

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

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

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

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

MR. DEMPSEY: In fact, there's an instrumental approach, there's an instrumental value that the disclosure of your medical records to the doctor is specifically premised on the notion that they are, thereby you have not surrendered your privacy rights. And in fact, we want people to accurately disclose information to their doctors, therefore we promise them that their medical records, disclosure to the doctor is not disclosure to all.

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

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

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

MR. DEMPSEY: Right, yes.

Also there were several witnesses mentioned the FIPPs. And I think it's, first of all, important to say we're talking about the Fair Information Practice Principles, which actually there's no definitive version of them.

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

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

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

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

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

MR. ROSENZWEIG: It's a framework for a starting point for asking the questions, but I think that many of those questions don't withstand the technological transitions we're going through.

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

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

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

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

MR. DEMPSEY: Okay, thank you.

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

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

That's a yes or no.

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

I think obviously when you disclose certain information to your telephone company, you are in a contract with that company and that contract regulates your dealings with the company.

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

MS. WALD: Your answer is both?

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

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

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

MS. WALD: Okay, for you, Dan. I think it was Liza Goitein that said that private companies have no incentive to coerce or imprison people, that's why perhaps the risks of injury might be greater from the government than from private companies.

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

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

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

And increasingly we see a cooperation or an industry in the private sector that has grown up to basically perform government functions and help gather data, help analyze data and then share data with the government.

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

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

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

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

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

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

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

MR. ROSENZWEIG: Okay.

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

If I can remember back to my old judicial background, that's something benefits guarantee corporation.

MR. MEDINE: Pension benefits.

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

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

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

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

I think that the implication of the question, which is really the most interesting part of it, so I'll transition into something I do want to talk about, is that it emphasizes the point that Liza made, with which I do agree, which is that the line between commercial collection and government collection is increasingly blurring some, you know, and the idea that regulation of the government but no regulation of Google's collection kind of sits in dissonance. And there are these places that are halfway between.

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

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

MR. MEDINE: Thank you very much.

MS. WALD: You've been extremely forthcoming.

MR. MEDINE: Thanks to the panel and for

the audience questions.

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

(Off the record.)

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

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

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

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

I remind the witnesses that we would ask them to keep their opening remarks to seven minutes. There is a timekeeper, which you might not have seen, but in the front row here, Renee, who will be holding up a yellow card for your two minute warning and then a red card for time's up.

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

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

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

So, Annie, please.

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

We're in an ever changing world where terrorists and criminals are getting smarter and more sophisticated. Their offensive techniques are surpassing our ability to protect our nation. Providing strong technical protections for privacy and civil liberties is a counterterrorism weapon.

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

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

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

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

Requiring government backdoors in commercial products, stockpiling zero-day exploits and weakening software security standards are all practices that weaken our nation's cyber security posture and make it easier for attackers to infiltrate these systems for nefarious purposes.

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

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

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

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

Moreover, the security benefits are questionable at best because sophisticated terrorists and criminals will simply use international products or more secure, less convenient alternatives.

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

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

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

There are some cases where it is critical to protect a person's identity. For example, for victims of domestic abuse we need to ensure that their location is protected and cannot be re-identified by their abuser.

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

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

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

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

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

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

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

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

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

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

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

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

MS. ANTON: Great.

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

MS. ANTON: Good, and I look forward to

meeting them. Thank you.

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

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

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

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

In short, these processes create enormous value, and that value is driving both government and industry to collect as much information as possible and to retain it as long as possible.

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

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

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

I'm here to encourage you to resist this new model. In my written testimony I argue four points. The first is that collection still matters. The collection of personal data impacts a person's core right to privacy, regardless of what happens to that data after the fact.

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

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

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

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

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

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

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

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

And I think that this highlights the fact that the forcible collection of sensitive data in and of itself invades what this Board has called, "the core concept of information privacy". And that's, "the ability of individuals to control information about themselves".

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

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

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

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

What I mean by that is that we as a society are often very slow to realize that a particular use of data is harmful, especially when it involves data of racial and ethnic minorities, LGBT people, and others who have historically lacked political power.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I've done that for nearly two decades, first as an associate here in a D.C. law firm, and as you mentioned for the last sixteen-plus years at Microsoft.

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

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

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

These standards are based on the Fair Information Practices, which we agree remain relevant today, including transparency about the data and how we use it, minimization with regard to the data collected and how long it's retained, choice about collection and use of data, strong security to ensure that the data is protected, and accountability to ensure that we are living up to our commitments.

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

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

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

And this approach is supported by a mature privacy program that includes dedicated personnel with privacy expertise who sit in both centralized roles and are embedded throughout the business. The program includes incident management, response and escalation processes.

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

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

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

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

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

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

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

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

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

Second, we should do more to increase transparency. Transparency is a key element to any program for protecting privacy. It facilitates accountability and enables public debate around policies and programs.

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

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

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

It was a good step that helped foster better understanding of the type and volume of such orders that service providers received, but we believe there can and should be more detailed reporting permitted.

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

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

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

In the year since the Washington Post reported an alleged hacking by the NSA of cables running between data centers of some of our competitors, there's not yet been any public commitment by the government that it will not seek to obtain data by hacking into Internet companies.

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

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

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

As we seek to sell our products and services to customers around the world, discussions that focus exclusively on the rights of U.S. persons are not enough. Many people around the world do view privacy as a fundamental human right, and they have a very real concern about whether and how governments can access that data.

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

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

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

None of this should be taken to suggest that we don't value and appreciate the absolutely critical work that our law enforcement security agencies do every day to keep us all safe.

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

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

While there's not always a perfect analogy between protecting privacy in the private sector, law enforcement, and national security context, we also, we in the private sector regularly deal with questions of striking the right balance between privacy and other needs.

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

MR. DEMPSEY: Mike, could you wrap up?

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

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

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

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

I'm here as a technologist and not as a

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

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

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

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

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

Our world used to be simpler, and sometimes I provide samples of that simpler world. You all remember this as a mobile phone. This is from the time that the phones were actually doing just that, they were a phone.

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

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

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

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

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

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

And it was per Thomas Friedman, and I quote here, "When I sat down to write, The World is Flat, Facebook didn't exist, Twitter was still a sound, the cloud was still in the sky, 4G was a parking place, LinkedIn was a prison, applications were what you sent to college, and Skype was a typo."

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

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

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

In the old and pre-2007 world we said

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

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

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

And they're becoming more connected. Everything is becoming more connected. You have heard things such as IOT, Internet of things, or as I call them, thingsternet.

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

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

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

A hundred hours of video, a hundred hours of video is uploaded on YouTube, and YouTube is not the only recipient of the service, other companies also have these services, a hundred hours of video are uploaded to YouTube every single minute. Every single minute.

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

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

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

And lastly, I close my remarks and I'm

looking forward to the questions.

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

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

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

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

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

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

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

MS. ANTON: Thank you. So you know, as was mentioned in the earlier panel, systems are getting more and more complex, which makes compliance more and more difficult as well.

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

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

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

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

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

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

MS. ANTON: So --

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

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

When I mentioned earlier that I'd like to see more technologists in the room, it's not just to kind of study it after the fact, but actually to be involved in forming the policy. Because a lot of times the policy and the law are written in such a way that we can't implement it.

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

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

MS. ANTON: Excuse me?

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

MS. ANTON: So I work a lot in HIPAA, for instance. We have the new change with meaningful use. I had one Ph.D. student who was really working actively on how do we predict what the change is actually going to be? Because when they finally make that decision we're going to have very little time to implement that change in systems to be able to be able to make sure that we're compliant with it.

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

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

MS. ANTON: Absolutely.

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

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

MR. DEMPSEY: I want to go to Alvaro Bedoya. There was one point in your written testimony that you didn't mention and I want you to talk about it now. I think it's very important.

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

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

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

But I actually think people are, technology is helping people learn about what they think privacy is.

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

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

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

And so I would say that ubiquitous surveillance is making people say, hey, you know what, maybe when I go to the grocery store, or I drive down the street, or I go to work I expect my colleagues at work to see me, you know, the people I know at the store to see me, my neighbors to see me, but I really don't expect anyone to know that I'm at all those places at all times no matter where I go.

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

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

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

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

It's very clear to us that our customers care about privacy now more than ever. And you see that in the amount of resources and attention and focus that we've put on privacy.

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

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

But it seems to me from what you're saying that Microsoft does not believe that its customers have surrendered their privacy rights when they use the Microsoft product or service, and thereby Microsoft has acquired information, Microsoft does not believe that that information has zero privacy interests.

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

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

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

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

MR. DEMPSEY: And that's true, in your view, both of content, so to speak, and non-content, or metadata, or transactional data. There's sensitivity there in both categories.

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

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

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

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

But other things about who you're

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Then when they realize that this is not

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

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

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

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

Hence my opening remarks as to our model in the industry and in technology is we understand the rules, we are very good at, you know, creating those rules and building systems, devices, services and everything that enforce those rules, but it has to be buildable and it has to be enforceable. The attention is certainly there.

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

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

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

MR. DEMPSEY: Do you want to respond to

that?

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

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

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

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

That's actually a really good segue because the first question I was planning to ask was, Dr. Anton, I was interested in what you were saying about not letting the perfect be the enemy of the good in terms of de-identification. In the domestic violence context you want it to be perfect perhaps, and in other contexts good enough will do.

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

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

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

But there might be cases where that kind of identification could be extremely damaging.

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

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

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

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

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

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

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

MR. BEDOYA: Yeah, sure. So the first is a historical point, which is that when the HEW report was issued, I was just reading, it's like pages 74, 75, the committee actually says, okay, we just set out these standards, clearly all of them can't apply to all intelligence records, but some of them must apply because the risk is too high if we don't have some protections.

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

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

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

And so in the 702 context the Board has recommended various measures to identify the scope. In all my time in the Senate I never saw anything that would lead me to believe that it would actually be impossible for the NSA to produce an estimate based on statistical sampling of the number of U.S. persons collected in 702 data.

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

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

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

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

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

MS. BRAND: Thank you.

MR. DEMPSEY: Chairman Medine.

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

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

And I guess I would like to understand more. I understand having or mandating a backdoor weakens protections, but why? It would seem as though terrorists can now hide their communications, which seems to be detrimental to counterterrorism.

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

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

MR. MEDINE: Alvaro, you talked about the expectation of privacy, and if I heard you correctly, but tell me if I'm wrong, is that you're in a sense suggesting that we talk about not what people expect their privacy to be, because I can put up a sign saying I'm conducting video surveillance and I can destroy that, but their expectations of what privacy should be, a more normative standard.

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

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

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

MR. MEDINE: Okay. And I guess this is for Mike, the Fourth Amendment, which is you talked about the balance between government requests and your customers' privacy. Do you think the government should have a warrant every time it accesses your customers' records, particularly if they're American customers?

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

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

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

MR. HINTZE: Yeah, I mean the laws that

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

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

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

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

How would you strike the balance between collection rules and essentially use rules?

MR. NAHARI: That's a very difficult

question, a very difficult one. I don't know if in the technology side of the house, I don't know if we really know where the balance is.

We take a look at the attacks, we take a look at the system, we take a look at the capabilities, we take a look at the mere fact that all of these attacks, all of these exploits are becoming so advanced that I used -- to give you one concrete example, I used to need to be physically around your things that you touched to be able to lift your fingerprint and then have access to your phone and then use that fingerprint to mount an attack and use your biometry.

With the resolution of the cameras that we have these days, sometimes with a very high resolution camera, I just need to have your picture that was taken somewhere in China to be able to zoom and zoom and zoom and then lift your fingerprint and mount an attack.

Now, how do you reflect things like this as to should we build systems that whenever there's a fingerprint, it smudges it and we don't expose it? There are things like this that I encompass all of those use cases as it should be buildable.

But what I'm trying to get across is coming up with the rules that define those capabilities or things that should be and shouldn't be done is a very complex problem.

MR. MEDINE: Thank you.

MS. COLLINS COOK: So thank you guys for another excellent panel.

My first question, and this goes back to what I had said on the previous panel, which is I view our job to be translating these ideas, these concepts, these concerns into practical recommendations.

So starting with you, Mr. Hintze, what have you found effective as a privacy officer to ensure your very large workforce, your complicated workforce dealing with emerging issues takes privacy seriously, your rules are enforced, and that from beginning to end privacy is a part of your culture?

Because we have a new NSA privacy officer, so this is free advice to the new privacy officer over at NSA.

MR. HINTZE: Well, thank you. You know, as I alluded to in my opening remarks, you know, one, there's no silver bullet. You need to take a number of approaches.

And we've taken a number of approaches to drive awareness and sensitivity around privacy throughout our workforce through a number of steps, some mandatory training that's required for all employees that cover a range of ethical and compliance issues, deeper role-based training that's specific to software engineers, that's specific to sales and marketing people, that's specific to different roles that people play in the company that impact customer privacy.

We have, as I mentioned, not just sort of told people what the rules are and then crossed our fingers and hope they abide by them.

We have put in checkpoints in the way

that we have developed our internal systems, the way you develop a software and get it out the door that has to go through certain checkpoints and reviews to ensure that privacy issues aren't missed or overlooked.

So there's a number of things we've done along those lines to make sure that people are aware and have the tools available to them to do privacy right.

But then there's also different checks along the way to ensure that mistakes don't get made.

And nothing's perfect of course, but we try to do a multifaceted approach, or a multi-layered approach to make sure that we catch those things.

MS. COLLINS COOK: And so let me follow-up on this, and it's a somewhat specific example but hypothetical.

Have you found training to be more effective or effective enough in the absence of pairing with mechanisms and processes?

That was a horrible question, so I'm just going to start over again.

So 702, that program has certain legal requirements. In the privacy sector would you train to those legal requirements or would you also have, for example, when an analyst is sitting there attempting to target, or select, or whatever they're going to do, also have at each stage of the screen, or the process, or however they're doing it, rules reflected in the computer system that they're attempting to use?

MR. HINTZE: We do both. To the extent that you can use technology to enforce policy that's always super effective because you get past or you reduce the potential for human error.

But that's not always possible. You can't completely prevent mistakes, oversight, or intentional bad acts. And so you need to do more than that.

You have to have, you have to build the awareness so that the inadvertent stuff is reduced. You have to build in the technology tools to try to prevent that from happening.

And then you need some level of checks to make sure that everything went right. And if it's, you know, somebody who's intentionally trying to circumvent a policy for whatever reason, that there's some way to catch that before it creates a negative impact.

MS. COLLINS COOK: So I think I have time for one other quick question.

In the Section 215 program one of the features was, in fact, that not all of the call detail record went to the government. In fact, names are not provided originally to the government, and subscriber information, simply numbers to numbers. Would that be an example of de-identification and anonymization?

MR. ANTON: Sure.

MS. COLLINS COOK: That was my only question.

MS. WALD: I have a couple of very sort of brief questions, which I think you can answer very quickly and that way I'll get them all in.

I'll begin with Annie. You talked about how it would be good for us, and we already do have technologists on the Board. I'll ask the government when we have the government board here, too, but let me ask you based upon your knowledge here, does the government have technologists who worry at all about privacy?

I know they have technologists obviously, but is this, as a result of your observations and study in the field, something that they consult with the technologists about, hey, we need this kind of information for national security, but we'd like to get it or as much as we can, what's the balance? Does any of that kind of thing go on inside the government with technologists?

MS. ANTON: Right. So having worked a lot with the government I know that they consult technologists greatly with security, with privacy, with compliance issues, and how do we engineer software that takes all of that into consideration.

I think if we look at the past five years or so, or six years or so that you'll see that the NSA was really, really focused on compliance. I think the results of the reports and the oversight has shown that they've done a really good job with that. When there's been an issue, they've dealt with it.

I think someone mentioned the new CPO at NSA. I think what we'll see different now is that not only is the, are we complying with law, going to be something that's factored into all of the software that's developed and all of the tools and the techniques and the procedures, but also now well, just because it complies with law should we really be doing it, and what's the extra step we're going to take to really consider privacy at the onset?

MS. WALD: So you sound reasonably satisfied with the fact that they're taking it seriously and doing the best they can?

MS. ANTON: I absolutely do. I wish, I actually feel very comforted by the fact that the government has a ton of oversight and a ton of laws to comply with.

I personally am much more worried about the large collection, amount of collection that's taking place in industry that people don't really understand.

MS. WALD: All right. So I can go on to my next.

Mr. Bedoya, you talked about how important it was to limit collection to what was necessary or purposeful, etcetera, but in light of so many of the experts on both panels have talked about almost like an almost inevitable momentum of collection, collection, collection, where would you look, what part of the government or where would you look for the mechanism to try and limit the collection, or get that kind of impediment or balance done?

MR. BEDOYA: Certainly. So I think folks have been saying that it's inevitable that industry is going to collect all this data. I don't think folks have been saying that it's inevitable that government will collect it.

And I, for one, don't actually think it's inevitable that industry will collect it.

But taking that as a given, I think the question is about reconstructing the firewall between government and industry with respect to data collection.

And so I'd be surprised if anyone on the panel thinks, or on the previous panels thinks that it's inevitable the government will collect all this data.

One quick other point, Judge Wald, on your previous question, I should note that I believe that the congressional committees that conduct oversight on FISA and on foreign intelligence, certainly the Senate Judiciary Committee lacks a technologist, and I think that's an issue that needs to be addressed.

MS. WALD: I think we talked a little bit about that in our first report on FISA reform.

Okay, Mr. Hintze, you talked earlier,

you said one of your principles was there shouldn't be any bulk data collections.

Now terminology is varied all over the place, so it would help me if I knew what you meant by bulk collection there.

And let me just tell you, one gathering of public health people and they talked about the great importance of public health data, you know, especially for when epidemics come along or that sort of stuff.

So wouldn't some of that come under your ban against all bulk data collection?

MR. HINTZE: I was talking specifically about government surveillance programs that come to industry.

MS. WALD: Okay, I just wanted to clarify that because -- and what do you mean by, give us an example of what you would call bulk data. Because this has been a debate as to whether this program or that program falls under bulk data.

MR. HINTZE: Certainly. I had in mind

the 215 program in particular where government goes to service providers.

MS. WALD: Where it's not targeted?

MR. HINTZE: Yes, it's not targeted, correct.

MS. WALD: I think that's all I have right now.

MR. DEMPSEY: We may be able to go back to Board members for additional questions. I would like to continue with this panel up until the top of the hour.

We have one question from the audience which I will read, and we welcome others if others want to pose questions.

In 2005, the National Academy of Sciences studied whether pattern-based data mining can anticipate who was likely to be a future terrorist. It concluded that this wasn't feasible.

And the question is, is pattern-based data mining in the terrorism context, is it feasible today and will it be feasible ten years from now? Would anybody like to address that? Hadi?

MR. NAHARI: I don't know specifically about terrorism. I'm mindful of what Ed mentioned is that we have limited data.

But there is a program that has been running in Los Angeles in LAPD. We may not necessarily still be able to identify specific criminals, but our predictive modeling systems have been at work. They're able to make a reasonably good prediction about where the criminal activities are more likely.

It is not precisely the question that you're asking, but I can assure that it is just becoming better. I can assure that any service provider that has the amount of data that we are generating, and it's becoming more and more and more generated, is just honing and fine tuning and polishing their models.

Whether it's going to be applicable to antiterrorism methods, I don't know. I think all of these models are heavily data-driven. So one would need a lot of data.

But to the point that these models, these predictive modeling are able to predict things may relate indirectly to terrorism or criminal activities, the systems are suggesting that we are going that way.

MR. DEMPSEY: Other thoughts on that question?

There's a system in Chicago that the Chicago Police Department has deployed, which both has been touted and criticized, but it does somewhat at the neighborhood or block level predictive or predictions as to criminal activity as well as, I understand, individual level, identifying people who may be either victims of crimes or perpetrators of crimes. Again, both touted and highly criticized.

Any thoughts or comments?

MR. BEDOYA: One just quick one, which is the risk of creating a feedback loop. You know, if you predict that there will be crime on corner X, you watch corner X like a hawk, you see every crime that occurs on corner X and you therefore draw an over-represented sample of crimes at corner X, reinforcing your prior conviction that you thought corner X was real dangerous. So that's the main one from my perspective.

MS. ANTON: So this is certainly not necessarily my area of expertise, however predictive is different from being able to reconstruct after the fact. And so can we use these things to then, when something has happened, go back and find whether we missed certain people that are still involved? Yes, I do believe that's the case.

In terms of predictive, I think we have a ways to go. By the same token I get, every morning I get a crime ratings, a crime report for all the crime in my area. And I can tell you, I can predict where there's going to be, on a weekly basis, crime in my neighborhood. So, you know, we're getting there.

MR. DEMPSEY: Well, I mean on some level

that's just Comstat all over again, the systems that have been available to police for decades.

MS. ANTON: Sure.

MR. DEMPSEY: One question, and I'll go down the row again, and I'll pose the question and I think we can just go down the row with additional Board members if they have, the Board members have additional questions.

I had said in talking to each of the panelists that I didn't want this to be a panel about going dark and the implications of encryption, but several of you have alluded to encryption and its significance here, and I would ask any of you who would, to comment on the following, which is, there is a growing trend towards more and more devices, cheaper and cheaper wearables, and the Internet of things, and more and more data collection occurring.

There's also it seems a trend towards more encryption by default, whether it's at the device level or, as Mike Hintze was referring to in terms of the encryption of data flowing between data centers.

So it seems to me like we have two things going on at once, which is not unusual. Somebody referred to the modern era, the era of the Internet of things, big data, ubiquitous data flows, as the golden age of surveillance.

And it seems to me that both trends will always be there. More and more information available both to the private sector and possibly to the government, and increasing pervasiveness or at least increasing diffusion, if not comprehensive diffusion of encryption.

Comments on that as a premise, first of all, the premise of my question, am I right?

And then secondly, where does that leave the government, and would you agree with my assumption that there will still be huge amounts of information available, both to the private sector for its purposes, as well as to the government?

I guess let's go right down the row. Professor Anton?

MS. ANTON: So I believe that there will still be a lot of data that's available to government. When I say that I really support encryption by default, I also really think that our country really, we were the code hackers, and it was really critical in World War II.

And I think that instead of just kind of taking the lazy approach and saying, oh, leave us a backdoor, that we should just get better at cracking the code, because they're getting smarter and we need to get smarter, too.

And so I leave it to the lawyers to decide what the legality of when you can actually apply that or break into a system.

But being satisfied with just having a backdoor means that we're not advancing our state of the craft and our tradecraft here in this country and we're going to be left behind as a result.

MR. BEDOYA: I'll actually pass.

MR. DEMPSEY: Yeah, my thoughts on this, two trends seem to be occurring simultaneously.

MR. HINTZE: Yeah, I mean we're certainly seeing an expanded use of encryption, encryption between customers and the service provider, and encryption between data centers, encryption on devices, etcetera.

And that's being driven by customer demand. I mean customers are concerned about the security of their data. And they're not just concerned about the security of their data vis-a-vis hackers and bad guys, they're increasingly concerned about the security of their data vis-a-vis governments.

And so to the extent that there is that concern out there that's driving customer demand for these security features and companies will continue to invest in that.

Does that mean that there will be no data available? I don't think so. I mean the nature of many cloud services requires service provider access to it.

You can't run an effective email system without being able to filter the content for spam and malware.

And so there will be a point in the communication chain where data is available, and that means that if it's available to a service provider, it's available to a government through lawful demands. So I guess that's it.

MR. DEMPSEY: Hadi, any thoughts on this, and then I'll yield.

MR. NAHARI: First off, I want to agree with Dr. Anton's point, we should just get better. We cannot ask industry, oh, don't encrypt, don't do anything. I would love to follow that when Chinese and Russians also follow that as well. So that's just not going to work.

I'm very respectful of the problems that the law enforcement agency has with the current state of affairs. We just have to get better.

And it works, at the end it's going to work better for us as a nation. So that's number one, I fully agree.

Some of the things, so going dark, I don't know if it's going dark. I know that we are currently in a state that we are really able to think a certain way about the system design, about the system security, about maintaining privacy, that world has changed.

The world and the industry has changed rapidly. The rest of us are catching up. So I think it pays dividend if we figure out, take some time, figure out what are the rules of this new world where we don't necessarily need to rely only on encryption.

I'm a big fan of encryption. I think it's one of the tools that security professionals and everyone has, but there are others. The fact that some data is encrypted is not on its own necessarily the end of the world.

I mean how many times, I know Michael mentioned that we are overusing this notion of metadata, but if you think about metadata as something about the data, it is meaningful when you see some encrypted data is being accessed a little bit more than the other. One could discern, one could learn things about it.

Once we start learning how to deal with this system, then we could maintain encryption, then we could maintain stronger encryption. We could also deal with the cases where we don't have access to clear.

I think our law enforcement, I think our government, I think our legal system, I think us as a society are in the process of learning how to deal with this new world were things that we knew in the past no longer apply.

Lastly, the new generation have figured it out. I think they're doing a lot better. They're figuring out that you cannot expect everything is going to be fully protected for you. They're figuring out ways to live in the world where they're posting a lot of things on Facebook that, I mean us probably won't do.

They're trying to learn how to deal with a system that, you know, you may not have the capabilities of asserting your privacy in the way that our generation did, but still have an expectation about their rights.

MR. DEMPSEY: Does a particular Board member have a question? Yes?

MS. BRAND: Several of you have referred to oversight in one way or another and I just want to ask a question about that.

In my view, oversight is especially important in the intelligence context because of the necessary level of secrecy that attends. It's important in all areas of government, but especially here.

But at the same time, when you start to layer on box checking exercises and paperwork there is a point of diminishing returns and you sort of have oversight for its own sake that doesn't actually deter misconduct or ensure compliance with the rules.

Do any of you have thoughts on principles for what's effective oversight, as opposed to just another box checking exercise?

MR. BEDOYA: So I certainly have a few thoughts for the legislature. I think that there's been a lot of soul searching around how the executive needs a change in practices with respect to internal oversight. But I think there's some pretty serious problems at the legislature.

One of them is the technologist issue that I mentioned. Another is clearances. I can say with moderate to high confidence that most United States senators lack a staffer with TSSI clearance. I hope I'm wrong. I don't think I am.

And the fact is that all of the key briefings for these senators are conducted at that level. And as a staffer, I know there's a lot of staffers in the room, you don't send your boss into a meeting about soybeans without a TSSI staffer -- sorry, no, you don't need a TSSI staffer for that, but you don't send them into a meeting on an issue that seems very easy without a staffer. And a lot of these folks are going in on staff.

Now thankfully folks on judiciary and intel have dedicated TSSI folks for the committee that they can rely on, but outside of those committees you're often flying, I don't want to say flying blind, but you don't have the resources you need to actually conduct that serious oversight.

MR. MEDINE: I have two questions for Professor Anton on de-identification.

One is you commented earlier that phone numbers without names associated with them would be de-identified information --

MS. ANTON: It's actually not de-identified, because if it's my cell phone, I stand corrected on that.

MR. MEDINE: Okay. Because obviously the availability of reverse directories makes that --

MS. ANTON: Absolutely, sorry.

MR. MEDINE: Then I guess you also had commented earlier that by analogy of having a lock on your door was a pretty good protection against burglars but obviously not a perfect protection.

And I guess the question is, in the context of a massive database burglars may not have the incentive or wherewithal to break into everyone's home in a community, but with a massive database with a brute force attack, you might be able to get a very valuable return on it.

So does that suggest that de-identification needs to be essentially stronger or may not even be sufficient?

I mean as you pointed out on the Netflix example, and Professors Paul Ohm and Latanya Sweeney have written articles about the ability to de-identify, is it a useful tool in some instances but not others?

And even where it's useful, does it to have to be a pretty enhanced form of de-identification?

MS. ANTON: Well, I think it's better than nothing. You have to work harder at it to get access to it, right, and to really be able to understand it. But that's going to help us with the, you know, high school kid who's just trying to tinker around, right?

But I think this is another example where encryption is really, really important, and very strong encryption. And so I think it's a blend of both.

MR. MEDINE: Thank you.

MS. COLLINS COOK: Just on the issue of de-identification and anonymization, I had understood it as a concept that could apply in varying degrees. So at a period of time it has been de-linked from the identifying information and now they have to go to court in order to re-associate it with the identifying information.

So I don't think I was asking you to say that it had been permanently de-identified or anonymized.

This question is for Mr. Bedoya. To the extent that we're looking at evolving standards or evolving notions of expectations of privacy, how do you quantify it?

Is it because 51 percent of folks in a

Washington Post poll said I care about this but I'm still using Facebook? Do you look at conduct? Do you look at the fact that people inside the beltway really care? People in ivy leagues really care? I struggle with what is a good way to identify emerging notions of expectation of privacy.

MR. BEDOYA: I'm not going to pretend to know the right answer to that question. It's a really, really hard question.

I certainly think that looking at conduct is extremely valuable, and there's been a lot of discussion about the third-party doctrine. And the fact is it doesn't remotely represent what the American people think about privacy.

You know, if your social network only had the settings of public and only me, that was the only option, you know, people would say this is ridiculous.

And I do think it sounds strange to say it, but we do have something to learn from the best practices of these social networks, in that they very much see the world as a series of segments and they respect the fact that sometimes you want to share something with segment A and not segment B. And so I would say that's certainly valuable.

I don't have a good test about identifying a reasonable expectation of privacy. I'll just repeat myself in that I think we need to see that as a standard that can expand and contract.

MS. ANTON: If I could quickly add, after the Snowden leaks there's an anonymous search engine called DuckDuckGo and the number of people who started doing searches on that search engine increased, I think by over a hundred percent. So there's one way that you can watch people's actions and conduct.

MR. HINTZE: Just one very, very quick add-on to that. It's not a binary thing. You can't say that people say they care about privacy but they continue to use Facebook.

You have to look deeper. You have to

look at about how they're using Facebook, whether they're using the privacy controls, how they're engaging in those services, because if you look deeper you see some pretty sophisticated choices that people are making in ways to protect their privacy that's not apparent on the fact that, oh, you're using a social network, you must not care about privacy.

MS. WALD: I have a question. Between the two panels, the first panel and the second, I heard, I hope correctly, that there is some difference of opinion on a couple of things, or maybe slight.

I think, Ms. Anton, you suggested in answer to a prior question of mine that you thought the government was indeed involved in trying to build privacy into the technological aspects of some of the programs.

On the other hand, earlier I think you said that in threat modeling very little privacy considerations were going into that.

Other people said that it wasn't

inevitable that the government would keep collecting more and more information, but I think I got that impression that maybe it seemed to be going that way from Mr. Felten on the earlier panel.

So my question is basically, very briefly, if there were one area of priority, if you were running the government's overall privacy protection that you would suggest they concentrate on and could perhaps improve privacy protection without endangering national security, what would it be? If you can do it very quickly.

MS. ANTON: I think that we really need to work more on privacy standards and not privacy standards globally, and also that aren't rigged in some way to help some government or sector of industry. I think that's the number one challenge right now.

MS. WALD: Other people?

MR. BEDOYA: Yeah, I would say it's ending programs that involve the bulk collection of American's data.

MS. WALD: I couldn't hear the end.

MR. BEDOYA: Ending programs that involve the bulk collection of American's data.

MS. WALD: Okay. Do you have in mind any except 215?

MR. HINTZE: I didn't have the TSSI clearance so I don't know.

MR. DEMPSEY: Okay, Mr. Chairman?

MS. WALD: Wait a minute, there was somebody wanted --

MR. DEMPSEY: Oh, I'm sorry. Yes, please.

MR. NAHARI: One last thing, and I don't know if this is the elephant in the room. One thing I would put as an item priority is our systems and the technology are very much built as one way. So I would introduce a notion of revocation.

So if something goes bad right now, if I'm releasing all of this information, there is no way for a user, for a citizen to go ahead and push a button somewhere and say revoke all the rights that I gave to XYZ service providers and I want to go ahead and clear everything.

So defining what that revocation means, what are the ramifications of that, and how to crystallize it as a requirement for the industry would go a long way for things that we could build.

MS. WALD: That would go primarily to industry, that wouldn't affect government. I mean if I gave the government some information under some program which I thought was going to benefit me and later on it turned out it was being used in a different way, would your revocation principle apply there?

MR. NAHARI: If I have the right to revoke whatever government had collected about me and I knew things that our government, in the possession of government and I was able to revoke that, perhaps that would be helpful.

MS. WALD: Thank you.

MR. DEMPSEY: So this concludes our second panel. It concludes our morning session.

We will reconvene at 1:15 with a panel of government privacy officers.

(Off the record.)

MR. MEDINE: Good afternoon. The Privacy and Civil Liberties Oversight Board's meeting on defining privacy will continue with our afternoon session with government panelists moderated by a member, Beth Cook.

MS. COLLINS COOK: So welcome back to folks who were here earlier, or welcome to those who were not here.

Just quick one piece of housekeeping, what we've noticed this morning is make sure, and Alex, this will be particularly relevant for you, make sure the microphone is actually the direction you are talking, so that even if you pull it in front of you but then turn to talk to us, make sure the microphone is picking up. They were having problems this morning and we've all been gently reminded as well.

All right, so this panel is about the privacy interests identified and addressed by government privacy officials.

Obviously in the counterterrorism context defining and expressly articulating individual privacy interests while balancing the needs of national security is an extremely challenging task.

As we discussed a bit this morning, widely accepted privacy frameworks like the Fair Information Practice Principles or traditional privacy impact assessments may very well be intentioned with the necessity to protect information regarding the operation of a particular counterterrorism program.

By the same token, some counterterrorism programs could be better served with greater transparency about what information is being collected, about the statutory authorities or the authorities pursuant to which programs are being operated, and about what protections the government utilizes to minimize the negative impacts on individuals' privacy.

So the panel that we have assembled

today for this forum is, I think, uniquely situated to discuss these privacy issues that arise in the context of federal counterterrism programs.

These officials not only assess the privacy impacts of a full spectrum of counterterrorism programs they have also been pioneers, many of them, in the practice of working proactively within the agencies to ensure privacy and civil liberties concerns are taken into consideration from the beginning of programs.

And if that were not enough of their duties, they also are learning to live with us and work with us.

Joining me today are three individuals. Unfortunatly DHS was not able to make anyone available for this as it turned out.

So we have three folks. They will have ten minutes, given that they have a little bit of extra time, few folks, but we will follow the same basic framework.

I will then ask a series of questions for a period of time and then invite my fellow panelists to submit questions as well.

So leading us off is Alex Joel who is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence.

Do you actually fit that on one card?

MR. JOEL: Yes, I do.

MS. COLLINS COOK: That's amazing.

So in that capacity he leads the ODNI's Civil Liberties and Privacy Office and he reports directly to the Director of National Intelligence.

Prior to joining the government, and I think this is also relevant based on our other panels, Alex served as the privacy, technology and e-commerce attorney for Marriott International, where he helped establish and implement Marriott's global privacy compliance program, including the creation of Marriott's first privacy officer position.

So, Alex, did you want to kick us off?

MR. JOEL: Yes, thank you. And I want to thank the Board for --

MS. COLLINS COOK: Oh, I'm sorry, there's a stop light function going on here, green, good to go, yellow, start wrapping up, red, stop, in the front row.

MR. JOEL: Okay. I want to thank the Board for inviting us here to address the public in this very important hearing.

And as you said, the Board does work very closely with us. We feel that the Board's role in providing both transparency and oversight, as well as advice to the intelligence community has been extremely valuable and is a critical part of how the intelligence community protects privacy and civil liberties.

So I want to thank the Board for holding this hearing and for the Board's very diligent and careful efforts to exercise their statutory functions, which I think have been critically important.

This topic is, of course, one that

consumes all of us, not specifically how to define privacy, but how to apply protections required to protect privacy in the context of our activities and in particular in the context of counterterrorism activities.

I'd like to just get to what I think of as the heart of the matter from an intelligence community perspective in any event, which is that we operate by necessity within a sphere of secrecy.

We have to be able to maintain secrets in order to be effective. The more publicly transparant an intelligence service is, the more it informs adversaries of how the agencies are collecting information and the better able those adversaries are to avoid detection.

So as I've said in the past, a fully transparent intelligence service is by definition an ineffective one.

The key for us then is how within the sphere of necessary secrecy do you make sure that the intelligence agencies are acting appropriately, lawfully, and in a way that protects people's privacy and civil liberties consistent with the values of the nation.

In the past what we have done, as you know, is focused on ensuring that we are providing full transparency to our oversight entities. And our oversight system is something that I would like to characterize as a system of many layers with many players.

We have not only within each agency, offices of general counsel and offices of inspectors general, as well as newly created privacy and civil liberties offices, but outside of the agency we have entities like the Department of Justice, which is responsible on a government-wide basis for exercising some of these authorities and oversight controls.

We have of course newly created entities like the Privacy and Civil Liberties Oversight Board, perhaps not that new anymore, which again is designed to make sure that there is a secure place for information to be disclosed and discussed so that the oversight institutions are satified that the activities being conducted are proper ones.

Then of course we have Congress and the judiciary, both of which exercise robust oversight. And I would mention that, for example, the congressional oversight committees, which were established particularly after the Church Committee hearings in the 1970s to provide this granular level of oversight over intelligence activities, has been very effective in my view in providing careful oversight of what we do.

So that's sort of the oversight part of the equation. I think what we have now more fully realized is the need to enhance transparency.

So if you think of it, I mean I was just thinking about this before I started talking, which is always dangerous, but if you think of it as operating within a sphere of secrecy, one way is to make sure that the mechanisms, the rules and oversight structure within that sphere are robust enough to make sure that privacy interests and civil liberties interests are being adequately protected.

And then there's the other way of approaching this, which we're also focusing on doing, which is reducing that sphere.

In other words, providing greater transparency into what goes on inside the intelligence agencies so that the public at large can get reassurance and can also provide input and feedback into how we conduct these activities.

I think if I could just continue along this theme, there are two aspects in particular of what goes on to regulate our activities that I think is of interest. One is the rules that we follow, and the other is the oversight framwork and mechanisms designed to make sure we're following those rules.

So I think on the former, what are the rules that we follow? We can and should provide greater transperancy, but a lot of those rules are now currently being debated and discussed, and you can think of some of the reform mechanisms as attempts to modify those rules.

So you have the activity going on in Congress, for example, the USA Freedom Act and similar legislative initiatives.

You have as part of that also the proposal to create an advocate of some kind, an adversarial mechanism for the Foreign Intelligence Surveillance Court.

Here again in my view is an attempt to influence or affect what are the rules that the intelligence agencies are expected to follow.

And then a different part of that question is what oversight mechanisms, what assurances do we have that the agencies are, in fact, following those rules.

And you're part of that. I've already mentioned the congressional committees, the Foreign Intelligence Surveillance Court, and then all the layers within the executive branch itself at the intelligence community and the Department of Justice level.

So I think, I hope that the public discussion has been shifting a bit from whether or not we're following the rules. I think what I perceived in the public discussion is a greater acceptance that we are in fact trying our best to follow the rules. We're not perfect and we make mistakes, but we're trying to follow those rules as best as we can.

And now the discussion has been shifting to, well, what should those rules be? What are the rules, and what should those rules be?

I think we can and must provide greater transparency into both sides of that equation, and we're working on that.

I would also say that another thing that I know the Board has been pursuing which is the recommendation that the Board made in the 702 report regarding efficacy, you know, to what extent are the counterterrorism programs and measures effective and to what extent do they provide value is a key part, in my view, of the transparency equation as well.

We have to figure out ways to identify the specific value associated with particular programs and activities, and then be more transparent about that so that the American people can render a judgment, as well as everyone else, on the need or desirability for a particular kind of program.

It is very difficult to do all this stuff and still maintain secrets. The intelligence communitity is not built for transparency. I've said this before, it's built for exactly the opposite, of course.

We train, provide policies and systems and reminders to our workforce of the importance of maintaining secrets, you know, maintaining secret the sources and methods that the intelligence community uses to carry out its activities. And this is vital. I mean we have to do that and we're reminded of that need all the time.

But at at the same time, we have to find ways to enhance transparency. It's going to involve some changes in culture, training, a look at policies and processes within the intellgence community and I know that you may want to ask questions about that, so I look forward to that discussion.

So thank you again. I appreciate it.

MS. COLLINS COOK: So turning now to Erika Brown Lee, she is the Chief Privacy and Civil Liberties Officer of the Department of Justice. In that capacity she is the principal advisor to the Attorney General on privacy and civial liberties matters affecting the department's missions and operations.

And as part of the Office of Deputy Attorney General, Ms. Brown Lee oversees the department's privacy and civil liberties programs and initiatives implemented by department components and component privacy and civil liberties officials.

She also heads the Office of Privacy and

Civil Liberties, which reviews and evaluates department programs and initiatives, and provides department-wide legal advice and guidance to ensure compliance with applicable privacy laws and policies, including the Privacy Act. Thank you for coming.

MS. BROWN LEE: Thank you, and thank you to the Board for inviting me here to talk about what is a very important topic.

You asked about private sector experience and other government experience, I also come from the Federal Trade Commission, which in particular the Division of Privacy and Identity Protection, which of course the Federal Trade Commission has a very different orientation toward the commercial side of privacy, but nonetheless an important perspective and an interesting one to bring to this position.

But counterterrorism is a significant part of the department's mission. Since my colleagues on the dias today will be talking from more of an intelligence lens, I thought I would orient my remarks more toward the department's efforts to fight terrorism from within the criminal law enforcement context.

The department has an elaborate architecture that protects privacy in our counterterrorism work, and since I only have a few minutes I'll focus on the lead agency in those efforts, which is the FBI and focus in a little bit more on the efforts with their counterterrorism activities.

But stepping back for a minute, of course as we know after 9/11, it was recognized that in order to address the current threat environment, FBI's functions needed to be expanded, but it was not intended that the expansions would come at a cost of civil liberties.

So in 2008, the department issued the Attorney General Guidelines for Domestic FBI Operations, the AGG-DOM, and later that year issued the DIOG, or the Domestic Investigations Operations Manuel. And combined, those two documents provide significant guidance for FBI activities.

But what I wanted to talk about, and I know I don't have enough time to get too far into the weeds, is just to explain how privacy is sort of embedded throughout the stages of an investigation, from the initial phase throughout the process.

And so, for example, one of the key tenants of both documents is the least intrusive method. So in other words, in any activity that the FBI engages, that's the baseline.

But of course within the counterterrorism context, it's got to be calibrated against the threat to national security, in which case more intrusive methods would be used.

But in terms of a little bit more detail from an operational context, when an FBI conducts an assessesment, for example, which necessarily, well not necesssarily, but oftentimes is proactive, that would involve, doesn't require a factual predication, but it does require a clearly defined objective.

And the least intrusive methods in that context would be even starting with publically available information, to voluntarily provided information, in that perspective.

And then moving up from there with regard to predicated investigations, which of course implies by title, there requires a factual predication to open that investigation, but that has to have supervisory approval.

And both types of investigative activities, whether it's assessments or predicated investigations require or are, I should say, subject to oversight.

Alex mentioned DOJ oversight on the intelligence side, but also on the law enforcement side for counterterrorism, the department's National Security Division has oversight authority for those kinds of activities.

Now Beth mentioned and asked us to talk

about or think about how the FIPS apply, if you're looking for the acromyn, there's lots of them in the documents, but it's not actually in the AGG-DOM or the DIOG. However, they are embedded throughout really, the princples.

If you think about, even from a transparency perspective, right, all that I'm discussing with regard to the DIOG, all 700 pages of it for a little light reading, for anyone who's interested it's on the web with certain redactions.

But also we have privacy impact assessments that are available. And one that I wanted to just mention in particular regards the eGuardian system because that is a specific system or incident reporting system that is designed as a platform to share terrorism-related information across law enforcement, you know, federal, state, local, tribal, territorial jurisdictions.

So eGaurdian, I don't have time to go into much detail about it, but it has an entire architecture of privacy protections governing how information comes into eGuardian, how it's shared across those entities, how it's stored and how it's retained.

Individual participation as a FIPS principle, obviously that's more of a challenge in a law enforcement context. It's not realistic to be able to obtain individual consent in order to pursue criminal investigations.

But nonetheless, the Privacy Act provides some measure of review in the sense that if access or amendment to records is denied, there is judicial review of an agency's decision, and subject to court order, records may be amended or access may be granted.

On the minimization side, I mentioned the least intrusive means already with the DIOG. There's also a prescriptive measure in the DIOG with regard to evidence collected, that if the evidence collected through an assessment or through a predicated investigation has no forseeable future evidentiary or intelligence value, it should be returned and destroyed, and then marked in the file in term of the disposition of that piece of evidence.

Otherwise, information is retained according to the schedule set by NARA, the National Archives and Records Administration, and approved, through which the Department of Justice would seek approval for.

With regard to use, I think that's also a challenge. On the criminal side of course willful disclosures of protected information under the Privacy Act are not something that any agency can exempt themselves from.

And to the extent that information is released that's not subject to a routine use or other permitted disclosure, and of course, you know, routine uses are subject to a compatibility standard that tracks the FIPS language.

If the information is disclosed or even shared in violaton of that, that's potentially a wrongful disclosure subject to not only civil damages but criminal penalties.

And then in terms of accountability, I mentioned oversight from the National Security Division, but also the FBI has the National Security Law Branch, which conducts national security reviews.

And that's a significant review process in that they go out to all of the field offices and review the investigative activities I mentioned, the assessments, the predicated investigations and look to see whether, in fact, superviseory approval was obtained, whether, in fact, there was a clearly defined objective for any assessment, and it's written up into a report.

That report actually comes through FBI channels of course, but then also comes for review by the Chief Privacy and Civil Liberties Officer. And I look at those, obviously, through a privacy and civil liberties lens.

So as Alex was mentioning, there are lots of layers that are applicable.

I know I don't have much time remaining.

But in conclusion, I guess I would just like to leave you with a couple of take-aways.

One is that FIPS, quite to the contrary of certain statements is not dead, it's just embedded.

And I would also say that the processes can always be improved. Certainly I work with the component, each component. There are over 40 components in DOJ, but each component has a Senior Component Official for privacy and I host regular meetings.

In fact, we're having a privacy forum next week that will cover privacy-related activities focusing on law enforcement, but other compoments as well, activities, common privacy issues across components. It is internal though so none of you are actually invited unless you happen to get a job by Monday at the DOJ.

But that's also something that is a way to improve. And I would also say that while privacy impact assessments are very important and a critical part of our program because they're sort of this tangible proof that we actually evaluate privacy, that we mitigate the risks, that we take into account security and accountability, they really only form a part of the architecture for the Department of Justice's privacy program.

So, and I welcome your comments.

MS. COLLINS COOK: Thank you, Erika, for a nice education about the FBI's operations, the FBI in particular.

So Becky Richards is the National Security Agency's Civil Liberties and Privacy Officer. In this, I think, relatively new role, I think it's fair to say, she provides expert advice to the Director of NSA on all issues pertaining to privacy and civil liberties protections, and she conducts oversight of NSA's civil liberties and privacy-related activities.

She also develops measures, which I hope she will talk about, to further strengthen NSA's privacy protections.

Prior to joining the National Security

Agency, she worked as the Senior Director for Privacy Compliance at the Department of Homeland Security.

MS. RICHARDS: Thank you, and thank you for hosting us. I am very honored to have been selected to be the first NSA's Civil Liberties and Privacy Officer.

This is an exciting time to be a member of the civil liberties and privacy community. Our community is growing and evolving and will help inform the debate as the nation reshapes its expectations for and limitations on the intelligence community activities.

Changes in the nature of the threat to our national security, alongside rapid advances of technology, as was discussed earlier, make my job both interesting and challenging.

Technology provides us with both opportunities and challenges, but ultimately we must guide and shape its use to ensure the fundamental rights we hold dear as a nation are maintained.

Today I'd like to take a little time to describe NSA's civil liberties and privacy programs, both in the past, present, and a few thoughts on the future.

Part of the NSA's mission is to obtain foreign intelligence worth knowing derived from foreign communications in response to requirements and priorities validated and levied upon us by the executive branch.

One such priority is counterterrorism, but there are other threats to the nation, such as the spread of nuclear, chemical or biological weapons, or cyberattacks.

NSA also works directly with and supports our troops and allies by providing foreign intelligence for military operations abroad.

As we consider NSA's civil liberties and privacy programs over the past 62 years, it's important to think about how the threat, technological and sociatial landscape in which NSA conducts itself signant mission has changed.

First, the threat has changed. NSA previously operated in a cold war era when the focus of collection for foreign intelligence was directed at nation states, structured military units, and foreign intelligence services.

While threats remain from nation states, they now also come from non-state actors, which require NSA to look at more, smaller and decentralized targets to protect the nation.

The technology has changed. NSA again previously operated in an environment where the communications between foreign intelligence targets were frequently conducted over isolated, government-owned and operated communication channels and equipment.

Now foreign target communications are interspersed with ordinary commerical and personal communications.

Additionally, the sheer volume and ability to analyze and manipulate big data, which has occurred as a result of significant advances in information technology, can expose information of a personal nature that may not have been previosly discoverable and may not be of any interest.

Third, how society thinks about civil liberties and privacy has changed. We've come a long and positive way in thinking about what ought to be private.

Personally identifiable information was not a mainstream issue 25 years ago. For example, Social Security numbers were routinely put on student ID cards and there was no thought of HIPAA.

So with that I'd like to give a little historical perspective. NSA's civil liberties and privacy protections have historically been driven primarily by the Fourth Amendment analysis, which is also reflected in NSA's authorities, Executive Order 12333 Foreign Intelligence Surveillance Act, or FISA.

This analysis framed NSA's protection program by asking where and how the data was collected, i.e., usually overseas, and the status of the individual or entity being targeted, i.e., is it a U.S. person or not.

NSA has consistently conducted extensive legal analysis as it considers new types of collection answering these types of questions. It has built a strong compliance program based on these, with compliance activities embedded in our technologies and systems.

As I have learned more about NSA and its compliance regime, it became clear while this is certainly one way to address privacy concerns, it is somewhat different from how privacy concerns are addressed outside of NSA.

Over the last 15 years Congress has passed a variety of laws to protect privacy in other parts of the government and the commercial sector. These policies and laws focus more on the nature and content of the data and how it is used, not where it was collected or the citizenship of the individual.

I believe we have an opportunity to

bring together NSA's current civil liberties and privacy analysis with a broader approach to privacy and civil liberties.

This new approach also supports the President's PPD-28 mandate to recognize that our signals intelligence activities must take into account that all persons should be treated with diginity and respect, regardless of their nationality and wherever they might reside, and that all person's have legitimate privacy interests in handling their personal information.

To address a broader set of civil liberties and privacy interests, I'm testing a civil liberties and privacy assessment process that expands NSA's views to include considerations of frameworks the private sector and nonintelligence elements of the government use to assess civil liberties and privacy.

For example, for the first time in its history, NSA is using the Fair Information Practices Principles, or FIPS, as a framework for considering civil liberties and privacy risks.

The FIPS are one framework through which organizations can analyze the protections they have in place for personal information.

While traditional NSA civil liberties and privacy questions center on citizenship and location of foreign intelligence targets, as well as collection techniques, FIPS related questions boil down to follow the data.

Data-centric perspectives mean privacy officials ask a different set of questions. What is the data being collected and how will it be used?

As such, we've designed an initial standarized template and during the next year we'll refine the questions and process to ensure we're building a repeatable, meaningful and helpful process to identify and mitigate civil liberties and privacy risks.

A critical part of the civil liberties and privacy assessment process is to make sure we're not merely checking off boxes, but fundamentally weighing the risks associated with the activity to form a holistic value proposition.

In essence, we're asking should NSA conduct a given activity, given its civil liberties and privacy risks?

As part of the assessment process NSA is documenting both standard protections, such as minimization and control on who has access, as well as any specialized tools designed to protect civil liberties and privacy.

Much like privacy analysis performed in the private sector and other parts of the government, we're using the FIPS as the basis for analyzing what existing protections are in place.

As we look to the future, I'd like to spend a little bit of time talking about blending the art and science of privacy.

Historically privacy tends to be a bit of an art form. Several of us stand around and think about how we're going to do the analysis. This can be difficult when we're beginning to think about big data and the complexity that was being discussed this morning.

NSA is fundamentally a technology-centric organization. We have and will continue to contribute to advancing the discussion and research of protecting civil liberties and privacy.

Today the science of privacy has made notable strides that include developing technology and tools that promote privacy, such as unique encryption capablilities, digital rights management and trustworthy computing.

Great work in private sector and academeia is also being developed on coding privacy policies, such that technology supports all specific uses.

But civil liberties and privacy protections need to blend the art and science of privacy if we're going to harness the potential of technology and incorporate our core values as a nation into this era of big data.

So despite significant progress in privacy technology, basic privacy of principles found in a strong scientific basis, have largely proven elusive.

If we can better understand what constitues personal information and how such information is used, we believe it will be possible to determine whether we can develop more practical approaches to evaluating the inherent risk of privacy to the individual.

To that end, our initial thoughts are to develop five sequential building blocks and to introduce the concept of some very difficult math into what is otherwise a very nice liberal arts discussion of privacy.

The first one is to catagorize personal information. We would like to determine if it's possible to identify and catagorize different types of personal information and what that risk is to privacy.

Now we've heard different discussions today, but we want to push folks to think about is certain types of data more risky to privacy, say likehealth data, than other information, say your address, and can we think about those risks.

If we can do that, then next we would like to determine if it is possible to identify and catagorize different types of use.

If we take both of these together, it's possible to develop a catagorization of both personal information and uses of the personal information, it should be possible to develop a scientific process to assess risk.

This process could evaluate the risk of the use of individual types of personal information for different uses, as well as aggregated uses of personal information.

Now with these three building blocks being more of the scientific aspect, I would now suggest we would move to an art form that looks at how we build that to identify what needs to have additional privacy impact analysis conducted so that we're looking at that across the board.

With all four of these together then we would look to see if we could build a responsible use framwork that holds data collectors and users accountable for how they manage data and any harm it causes.

Building a technical means based on principled scientific methodologies to support the identification of civil liberties and privacy risks can help us better protect civil liberties and privacy in a fluid world of big data.

Success is dependent upon input from a variety of disciplines ranging from technologists, social scientists, privacy and civil liberties experts, ethicists, attorneys and computer scientists, to name a few.

We would welcome the opportunity to discuss this in more detail and greater technical depths at a later date.

With that, I thank you for the opportunity and I'm happy to answer what I'm sure are a couple of questions.

MS. COLLINS COOK: Thank you all for your opening remarks.

Becky, I wanted to stick with you for

just a second. When we go and meet with y'all and when we talk to y'all, there is frequently someone from the general counsel's office, someone from the compliance office, someone from your office.

What are you doing that is different than the general counsel's office and a compliance shop?

MS. RICHARDS: That's a great question. So the civil liberties and privacy office at NSA is the focal point for questions surrounding civil liberties and privacy, and it's been brought to a senior leadership position at NSA in order to focus on those efforts.

So generally speaking, our general counsel will answer the legal question, is this legal permissable? And they will often then work with compliance for, what are the rules?

But we haven't had a person asking some of these more difficult questions of, should we be doing this?

Now frequently our oversight folks,

whether it's ODNI and DOJ, were playing that role. And so I don't want you to take away the idea that those questions weren't asked.

But it's really important to have that type of a role inside the building where you are working with the operators and the technologists and can spend a great deal of time understanding what we're trying to do and bring to bear those questions.

MS. COLLINS COOK: Erika, a similar question for you. FBI, for example, has its own privacy officer, has its own general counsel, has its own compliance shop.

What is your relationship and what is your ability to provide recommendations or to actually impose requirements on the FBI?

MS. BROWN LEE: So also a very interesting question. My role and position is department-wide, so of course I have oversight over the compliance for DOJ as a whole.

Each component, as I mentioned, has a senior official for privacy, but in addition has general counsel's office that has significant footprints in privacy. So at FBI they have their privacy and civil liberties unit that's headed by a chief.

I work quite significantly with that person in that office to specifically address compliance issues, to specifically address privacy initatives that I feel are important for the bureau to consider.

Ultimately it is somewhat of a reporting structure. In other words, if there is a recommendation, or a particular policy or statutory obligation, FBI has the responsibility to comply.

But part of what my job is, is to advocate and to make sure that that is occurring on a regular basis and that looking for ways that I can improve the process, looking for ways, for example, I talked about privacy impact assessments. Some of that is, if you look at the E-Government Act, it's written fairly broadly.

I take, you know, a particularly broad

view of what I think should have assessments as part of compliance there. And so that's what I work in particular with the FBI on.

MS. COLLINS COOK: So Alex, a related but different question for you. How do you ensure that you have access, do you ensure that you have access to what various agencies are doing, or do you find yourself periodically reading about new programs, alleged new programs on the front page of the New York Times?

MR. JOEL: I'm surprised by that question. Information sharing is perfect everywhere in government.

MS. COLLINS COOK: I'm also seeking free advice because obviously one of our biggest challenges is going to be knowing what the agencies are doing. You can't conduct oversight of something you don't know is happening.

MR. JOEL: Right. I think that it's a major challenge for all of us. I know that, as you said, it's something that you're focused on. I know that it's a challenge for everybody.

It's a matter of, first of all, understanding the information flows within your own agency and trying to put in place markers for where it's important for you to be consulted.

The main way that I have just practically done it, since I've been doing this for about a decade now and when I first started, you know, it was just me and then we built a small staff over time, has been to form the trusted relationships inside the intelligence community and to make sure that the people that I'm working with and that are in positions of influence and authority to make decisions on programs and activities, understand the importance of consulting with civil liberties and privacy professional.

In my own personal experience working within the intelligence communitity has been that when I first joined I was very pleasantly surprised that people were so focused on compliance and protecting privacy and civil liberties, doing the right thing, following the right directives, and even when they might feel legally permitted to do something, they still gave voice to their own doubts as to whether they should be doing it.

And so I did not personally experience an uphill battle in trying to pursuade intelligence officers, hey, it's important for you to pay attention to civil liberties and privacy.

In fact, it was sort of the opposite where many people felt that they were already doing that, and that it was their job to focus on that.

For example, you mentioned Office of General Counsel. I was at an office of general counsel before coming to this job and we certainly felt when I was there that that was part of our job. We needed to look out for privacy and civil liberties, and not just what the law allowed, but what was the underlying intent and what should we be doing in that light.

So I certainly didn't want to take away

that sense of responsibility from anybody inside the intelligence community.

My approach had always been, it's all of our jobs, it's part of our oath to support and defend the Constitution. There are offices that are particularly focused on that, Office of General Counsel, Office of Inspector General. There are intelligence oversight offices, as you guys have learned, that are.

Now we're creating these civil liberties and privacy offices and I do think we add value because I think it is our full-time job to focus on civil liberties and privacy, so we bring focus, we bring an external perspective, and we have specific expertise, and training and experience that we can bring to bear, and then we can become a voice, as Erika said, an internal advocate for civil liberties and privacy.

But I mean I think different agencies will find different ways of doing it. The ODNI is a fairly small organization, and the ODNI itself has mechanisms for understanding what's going on across the intelligence community. So when a particular program or activity bubbles up to the point of a decision, either it comes automatically through my office or somebody will understand that I need to see it and route it to me.

MS. COLLINS COOK: So a follow-up, particularly to you, Alex, and Erika, both of you have fairly small staffs considering the breadth of your responsibilities, and we talked a lot this morning about the increasing technological complexity of what you are assessing.

Do you have the technological resources to understand what systems are actually doing? And I think that is both in terms of assessing on the front-end whether systems or programs should go live, or to the extent that there are restrictions, for example, if the FISA Court puts a restriction in place on a particular program, ensuring that those restricions are actually functioning.

MS. BROWN LEE: So I think that's a good

point. So but as I mentioned earlier, oversight, there are sort of a variety of roles in the department that have oversight, particularly with regard to counterterrorism.

But my office is fairly small in the sense that given the large footprint of the Department of Justice, but they work incredibly hard and diligently with all of the components to ensure compliance.

We rely quite a bit on internal component work that is done to produce information about what the privacy compliance is, and then also with regard to auditing and making sure that the privacy activities are actually effective.

But I would also say that some of the oversight, just to sort of again stress that, some of the oversight isn't just through my office, it's National Security Division, and FBI also has their branch, so we work very collaboratively.

And like Alex, I have found that within

the department there are a lot of people who care very deeply about these issues. It's not specifically in a privacy role as a title, but they have oversight and I think meaningful insight as to how the activities should consider and be consistent with privacy initiatives.

But, you know, it is something that I take into account and that's part of the reason why we have these internal conferences and whatnot that I'm trying to do to build upon that.

MS. COLLINS COOK: And Alex, what do you do to make sure, the old adage is trust but verify, what do you do to make sure you actually understand the programs and the systems?

MR. JOEL: Right. So it's a variety of things. One is, although I am not personally a technologist, I have been dealing with technology law, and legal issues and privacy issues associated with technology for much of my professional career.

So when I was at Marriott, I was the privacy, commerce and IT lawyer there. And then before that I was at a law firm in downtown D.C. focused on large scale technology transactions.

That doesn't make me a specialist in technology, but it does enable me to ask the right questions and make sure that the information is explained to me appropriately.

I don't have the staff resources to engage a full-time technologist. I think that would be helpful. I do think that you have to be a little bit careful with that because what you really want in that sense is a technology generalist.

There are so many different aspects to to technology, as you know. I mean that's just a word that almost lacks meaning these days because we use it so frequently.

But what NSA does for one particular type of activity will differ significantly from what FBI does, will differ significantly from what all agencies do in terms of database management.

So you've got database issues, you have

surveillance technologies, understanding communications technologies, understanding all kinds of different aspects to that issue.

And then of course the engineers and technologists, as we know, speak a different language from lawyers and so sometimes it's hard for everyone to speak to each other.

So what I have been doing is making sure that the information is clearly presented, that I see the documentation, that I personally understand it, that I trust the people who are providing me that information are giving me a complete picture, and then we also leverage technical experts in the particular field that we have access to within ODNI or through the agency. So if something comes up that we don't quite understand, we can reach out to somebody to have them help us understand it.

I think with a larger staff I would try to have more full-time technical expertise.

MS. COLLINS COOK: Becky, you had mentioned that you've got a couple of pilot experiments going and you mentioned also new technologies that may or may not be available.

How are you working with the private sector to leverage what great thinking is going on, and is privacy a part of the procurement process, for example? And has consideration been given to that, that if we really want privacy to be from the ground up, should it be one of the procurement factors?

MS. RICHARDS: I'll start with the procurement. We actually started with the theory on procurement because in part that's how we were doing things at DHS.

But it turns out NSA is a technology company that has a huge research portion of it and it also has a huge technology division. So it's two different parts.

So I actually have a technical director on staff who's here, Dave Marcos, and he and I have been working through sort of how do we think about the tech, how do we look at both what's out in the world, and so we're actually working with several different groups within NSA to do an initial review of what is out there right now.

And they're conducting that right now so we can get a sense of both from a policy and a technology perspective what's going on, as opposed to just things that we may know just, you know, from knowing different people, whether it's activities going on at MIT or Carnegie Mellon, you know, to make sure we had a broad breadth of understanding of what was the type of research going on.

So they're doing that. We're working on that right now, and then we're working with our research folks and trying to just leverage all of those things.

The procurment process is not really helping this happen best at NSA. And I think that that's, you know, each agency has its own culture and its own aspects. And so a lot of what I've been doing is taking the learning and sort of shifting it to make sure that building the program within NSA works for how NSA works.

And so that means that our privacy program is going to look a little bit different than FBI's or others. But it's based on sort of how the organization functions and where those key decisions are being made. So we're working through that.

But it turns out procurement really isn't really isn't quite the right place. So we're looking through in terms of both the technology, and the research director and others to make sure we understand where those touch points are. And that's a lot of why we're beta testing the processes.

MS. COLLINS COOK: So I think I have time for one last question before I turn it over to my fellow Board members.

Alex, this one's for you. You explicitly pointed to congressional oversight as one of the things that the American people should be aware of, that this happening, it's robust, it's real.

A previous panelist pointed out that

there is potentially one significant flaw or challange with congressional oversight, and that's the lack of cleared staff.

What has your perception been? Has Congress struck the right -- yes, I'm going to a ask you to opine on Congress -- whether consideration should be given to broadening the range of individuals?

I think there's some comfort level with, I think someone called it delegated oversight within the Congress. But when some significant majority of decision-makers in a representative democracy don't have cleared staff, how is the oversight nonetheless sufficiently robust?

MR. JOEL: So the intelligence oversight committees have very substantial cleared staff. And they of course have secure compartmented information. We have SCIFs in which to review all the classified information. And we have many, many meetings, briefings and reports with our oversight committees.

I guess my first response as a matter of principle, yes, Congress should have the degree of staff cleared it needs in order to assist it to perform its oversight functions.

I think that intelligence community assumption had been that by clearing the staff of the oversight committees that that function was being fulfilled.

I think some staff members are also cleared from some of the other committees. I don't have all of that information in front of me but I believe judicary has cleared staffers, etcetera.

Whether or not that's enough staff to be cleared, I don't know. I think Congress, from my personal perspective, it would be helpful if Congress figured out for itself which committees are performing which function and which staff members need to be cleared in order to oversee our activities and then we can assess it.

But I would certainly support a desire to make sure that there are enough cleared staff to perform oversight, absolutely.

MS. COLLINS COOK: So transiting to the member questions and while this is happening, just a reminder there are folks with cards, if you have questions that you'd like to submit from the public.

And to keep everyone on their toes, this time I'm going to start with Pat.

MS. WALD: Okay, you may be sorry about that choice.

MS. COLLINS COOK: I might not be, they might be.

MS. WALD: This is somewhat of a loaded question, but it's one that's sort of in the back of so much of the work we have done and will continue to do.

You know, I laud all of Becky's attempts, and your attempts to inject, Erika, your attempts to inject privacy into all of the various phases of intelligence.

But drawing upon what some of the people in the first panel said this morning, let me just pose a question that, for instance, several of the panel members thought collection was a primary focus of trying to enhance privacy interests by limiting collection somewhat, and leaving apart any debate about whether or not collection by itself can be an injury to privacy, I guess, and that's collection.

Also when you get, another expert talked about the risks to privacy from aggregating data. And we found out, for instance, in the 702 report we did, when you got to the retention of data the analysts might look at it and say, well, I don't see any foreign intelligence purpose to this piece of data if it came from an innocent person who's not the target, but it's conceivable there might be one down the line or some other person I don't know about, the agency, so therefore, I've got to bend to make sure that it's secured.

So it seems to me one of the basic problems here will be, what's the tipping point? In other words, assuming good faith on both sides, there really is a national security interest when you have to make a choice between privacy and national security, but the real question is, how much and at what point?

In other words, when we were doing 215 we were told many times we need a big haystack in order to find the needle, and the bigger the haystack, the more likely we are to find the needle.

But of course a policy judgment has to be made at some point. At this point, yes, we're going to lose some national security things but privacy is more important.

I guess I want to know what your thoughts are about how that decision, which is a basic policy decision, but it seems to come up in every program that we look at, you know, how is it made or how it should be made, even at the most general level. You can all take a --

MR. JOEL: Okay, so I'll start. I'll offer some general observations.

MS. WADE: Yes.

MR. JOEL: So I think on the collection and use and retention point, I would say that it's very important to look up each phase of that. And that's, in fact, how the intelligence community structures its determinations in many ways. It's collection, then there's retention, and then there's dissimanation.

And on the collection point --

MS. WALD: And aggregation.

MR. JOEL: Right. And then of course when you aggregate data, you create additional risks.

So there's no question that if your concern is to protect privacy, the better way to do it, and you're worried about what the government's going to do with your data, it's always better for the government not to have the data. That's the best protection.

So if the government doesn't have the data, there is no risk to privacy from the government because they don't actually have it. So that's why I think it's appropriate of course to focus on collection.

Once a determination is made that the

government really needs this data in order to carry out an important function, then you're shifting to retention. And so there are --

MS. WALD: Let me just interrupt you. I'm sorry to do this.

MR. JOEL: Okay.

MS. WALD: It's an old habit of mine leftover from --

MR. JOEL: Yes, your Honor.

MS. WALD: When you say, really needs, that's where the rubber hits the road.

MR. JOEL: Right.

MS. WALD: Because, sure, it's going to be useful. So where the line is between something which genuinely will be useful to you but will be more of a privacy risk, and the thing of, this is really necessary, because. And we all know it's going to be drawn differently in different case situations.

But that's what it always seems to sort of come down to, and I'm wondering do you have any thoughts about how that, which is a policy --

MR. JOEL: So this is where, and I know Becky, but before you used the term tipping point, which I think is a very helpful term, and sometimes people think of this as a balance or as a scale.

The way that I think of the balance metaphor as it might apply here is not that you're saying, well, that tips it over here so therefore we're going to do it, that tips it over here therefore we're not going to do it. Although to some extent, of course, that happens.

The way that I think of it is that if you're going to do something new, a new or different collection program, you ask the following questions, A, is it lawful? Of course it has to be lawful. Is it justified? What is the purpose? You know, going to sort of a FIPS analysis, what is the purpose for it? Is this collection focused on a valid purpose that we feel should be pursued and is it important to be pursued, whatever the phrasing should be?

And is your activity tailored to that

purpose? Are you doing something? Are there less intrusive ways of doing it? Is this the appropriate way to go about doing it in terms of obtaining this information?

And then what are the risks to that? Sort of now going to the other side of the scale. And how do you guard against those risks? How do you mitigate those risks?

And this is the way that I've always thought of it. You know, it actually fits into some FIPS kind of models. It also fits into some privacy and assessment kind of models.

But if you look at that overall picture it then helps inform you, either the art or science side, I don't know, Becky can tell us which one that is.

It helps inform the decision about whether this is the right thing to do. And I think you have to look at that to tell.

So if you're just going to do one program, well, it's lawful and we think we need it. But now you can't figure out, there are major risks, but you can't figure out how to adequatly mitigate those risks, then that will tell you one thing about the overall risk of doing that activity.

MS. COLLINS COOK: Alex, if we could.

MR. JOEL: Oh, I'm sorry.

MS. COLLINS COOK: That's all right. And Becky, did you have something specific you wanted to say in response to this question?

MS. RICHARDS: Yes, the only thing I would say is we've been asking some different questions to try and tease out some of this conversation as we go through different programs.

And the questions we've been circling around, which are a little bit different than, you know, is this lawful. It's more, what is the type of the data? How intrusive is the data? How broad is the collection? In other words, am I obtaining a lot of people who are sort of an incidental collection, are not part of the target or not? And then what are the stated uses or future uses?

And we've sort of been using those three questions to get at, I think, the overall risk, which this sort of bubbling it really up is we want to stop the government from doing bad things to good people.

And so you know, sort of looking through those different lenses it helps us do that analysis.

MS. COLLINS COOK: So thank you. David -- I'm sorry.

MS. BROWN LEE: I was just going to say, just because you wanted-- all right.

It's an iterative. I was just going to just sort of follow-up on the comments in that I think that forcing mechanism of trying to do, of having ongoing vetting and ongoing evaluation by the right people is where to go, because in looking for the meaningful relationships and developing those, as opposed to, you know, retaining the isolated pieces.

So I would just say that trying to force that mechanism of ongoing vetting is really important.

MR. MEDINE: One of the reasons for having the forum today is to get a better understanding of what privacy interests are being protected by your offices and our agency.

And Alex and Erika have both been in either the private sector, in the case of Marriott or at least at FTC had a private sector focus. How would you compare the privacy interests you were trying to protect in your prior positions with the interests that you are trying to protect now? What are the similarities and what are the differences?

MR. JOEL: So I actually think there are a lot of similarities, but there are of course some important differences as well.

So on the similarity side, and I think privacy officers and people in all kinds of organizations, be they private sector or other government agencies, share a similar challenge or problem set, which is when your organization wants to do something either for a business purpose or for an authorized statutary purpose, and in order to do that you need information.

And for businesses this is typically information about customers or potential customers. And then you want to do something with that information to carry out your lawful activity. So it's a given that your organization will be obtaining and using personal information in many cases.

And so then the privacy officers' challenge is then making sure that that activity is conducted in a way that maintains your key trust relationships.

There are different ways of framing it, but I think that's generally speaking what happens.

And so for a business perspective, what you want to make sure you're doing is delivering value to your customer and that you're not using that information for inappropriate means or ways that are going to essentailly get your customer upset and have your customer take his business elsewhere.

And so a lot of those things are similar. I think that the key distinction for a business is of course that it has the ability to disclose a lot about what it's doing in terms of obtaining that information. And the value that it's providing is also something that gets immediately, it should be immediately apparent to the customer.

To the extent that the value is further down the chain and the customer doesn't see it that much, but is aware that the information is being collected, that impacts the trust that the customer has with the business.

I think from an intelligence community perspective, it's hard for us to demonstrate the value. What are we doing with the information? And so as a result when people are worried about information being obtained by the intelligence community, the value to them seems inchoate, yet the risks seem very real. Like, well, my freedom could be impacted if the government misuses this information.

We can reassure people we have methods in place to make sure that the information will not be misused, but I think, and we need to do a better job of that, but I think the other side of that equation is we have to show, better show what we're doing with the information.

And of course for intelligence agencies some of the most tightly held secrets are the successful use of intelligence, because we don't want our adversaries to know that that method was successful.

MS. BROWN LEE: Okay. So just to quickly answer your question, so I was also in the private sector at a law firm and practicing privacy.

Here's where they're similar, whether it's clients, or even from a government prospective, people tend to be reactive to privacy.

And one of the things that I find the biggest challenge is to be proactive. And it means sometimes taking unpopular positions, whether it's with clients or internally within my organization. But sort of having principled reasons for doing that, and if not forcing putting, you know, very strong arguments to do what you think is the right thing, I think is where it's simialar and where it's hard but interesting.

MR. MEDINE: Becky, you talked about catagorizing certain types of information as being sensitive.

In our morning discussion there was a lot of talk about the mosiac theory where there may be individual bits of information that are innocous on their face but in combination they present a perhaps sensitive profile of someone's activities, thoughts and so forth.

Do you lose something if you focus on what seems to be sensitive information and not take into account the potential combinations of information?

MS. RICHARDS: So actually the goal is

to take in to all those combinations. So the idea and where we've been looking at is that it's very difficult. You know, we want to push folks and I will say that this is an uncomfortable place to be as a privacy person. This is sort of where I'm like, well, it'll depend.

But if we look at where big data is today, there is a lot of data and it's very volumonous and it's a lot of discrepancies. And if we can start to define, which is sort of what I felt like we heard in the second panel, even if -- and this is where sort of I think we're going to try and push NSA, is if we can start to define and put some mathematics behind it.

So that, for example, if you have vaguely anonymous or slightly de-anomoized data over here and over here and the computers start to put them together, we would want the system to then pop something to say, hey, look at this before you decide to go forward.

So the idea is technology is supporting the privacy analysis by looking at whether or not the math underneath it can work.

And so you're going to have to make some really hard choices. Do I think health data is more risky to privacy than my address? And everybody gives the example of, well, then you have the violence against women or, you know, something along those lines.

But at some level if we deal with only those edge cases, we're not going to move forward. And I think the value, we will be losing some of the value, both from a privacy perspective, as well as from a technical perspective.

Because we're sort of in this art form of looking at each individual case, which I recognize at NSA, I'm not going to be able to look at every single, little thing. We want a system to be able to identify the things that need additional analysis, that need that additional judgment.

But what I don't want to have happen is have us backed into a place where the system is doing things that we would find unacceptable because we didn't sort of build something in to help with that.

MS. COLLINS COOK: Thank you. Rachel.

MS. BRAND: Thank you all for being here. For those of you who have been here all day you'll know that this is a little bit of a hobby horse of mine. But I want to ask about the FIPS and why you are purporting to apply them, although you can't really apply them.

So I gather, and Ms. Richards, this is directed to you, at least initially. And I commend you for publishing the paper on targeted collection under 12333. And you said that you were applying the FIPS, and I gather you were talking about the 2008 DHS iteration of the FIPS.

But then you said that, for example, the individual participation FIPPs can't really apply to your activities, and the transparency one can apply in a very limited way.

I guess I'm wondering whether it doesn't make sense to come up with a new set of principles that applies to survellance activities of the government? Because if you look at the DHS FIPS, the transparency one as articulated in this document really can't apply to you because it's talking about providing notice to the individual regarding collection. That's obviously not going to take place. Individual participation really can't apply at all.

MS. RICHARDS: Correct.

MS. BRAND: Some of these other ones are very, very important. Purpose specification is very important. Miniminization, data security, some of these are important.

But yet, this doesn't at all address things like thresholds, evidentary thresholds for collection, which are required obviously by law. But if you're talking about principles that are supposed to sit on top of the fundamental legal requirements, you should talk about thresholds. And there are some other principles that don't come into play here.

So I'd be interested in knowing why you

decided to apply the FIPS and if you've given some thought to coming up with some new principles.

I don't mean to critize this for DHS's purposes because DHS has a lot of functions that involve voluntary interaction by an individual with the government where this makes a lot of sense. So but you're in a different positoin than that, obviously.

MS. RICHARDS: So I guess what I would say is it's a beginning place, and I've sort of stated that a couple of different times because I wanted to start with something.

And so from my perspective, I guess I want to take the parts of the FIPS that work well, which would be basically the bottom six of the DHS ones and then look at how we can work those through.

So what I would say is sometimes there's analysis that needs to be done at an enterprize level. So it's useful for me walking into the agency, which may be readily apparent to everybody, but it was just useful to go through the process and say, hey, here is sort of one framework that we think about for privacy, and as an enterprise we don't do the first two.

One of the questions that led me to ask in some of the conversations I've had with academics and advocates is to say, okay, we don't do transparency in the traditional sense and we don't do individual participation. Is there some proxy? Is there some additional thing that we should be doing, given that?

And I think that gets to your question of, well, are there other things that should be underpinning these? And that's where we're starting to work through those questions.

So I think it was very beneficial to start with that as the beginning one and then use the remaining six principles as the basis for some of these questions.

Part of the problem though I will tell you with the FIPS is they don't give you a judgment. They don't tell you, well, this is good enough or that's bad enough, which sort of gets to your evidentiary purpose. And that's the place where we are trying to then look at the data. What are the risks to the data?

We spend a lot of time now talking about, well, what is the exact risk to this program to privacy and civil liberties? And so we're still working through those and having a lot of really fun and intellectually stimulating conversations about what are the right questions and how do we do that for an intelligence agency at NSA.

But I would just say that it, for us, was a beginning place. I don't think that's it's necessarily the ending point, but it was someplace to start with. And I don't want to sort of throw everything out and start with, I don't know. You know, you have to start somewhere.

MS. BRAND: Okay. Do the other panelists want to say anything about that? Alex?

MR. JOEL: I would just say that even

though the first two do not directly apply, certainly not as written by DHS, they provide useful measures for us to determine to what extent does this raise privacy issues and in what areas.

So that is, I think it's very helpful to use as a guide in the way that Becky has been using it at NSA.

I like the idea of developing a statement of principles that would apply to the intelligence community. So I'll take that path.

MS. BRAND: I think I probably don't have time for another question, but I would suggest if you're going to engage in that exercise that you look at the threshold question and that you also look at oversight because these, you know, they talk about accountability and auditing, but creating a paper trail is not the same thing as effective oversight. And obviously, as I said in the previous panel, oversight is extremely important in this context. So just food for thought.

MS. RICHARDS: And I think it's just important that you don't have a check box. I mean part of the problem I think with the FIPS also is it leaves itself to a little bit of a check box process.

Do I have a privacy statement? Yep, I got a privacy statement. Okay, am I doing everything in there? Yep, okay, I can do that.

As opposed to these sort of questions of, should I be doing that? And that's I think where having an individual at the agency whose focal point is this, really benefits the agency in terms of that conversation because it can very quickly devolve to, I checked it off, I'm good. You have no privacy, but I'm good.

MS. BROWN LEE: And I would just say that the oversight perspective has to also be iterative and changing because I think as technology allows us to, you know, collect more data and in different ways and different data points that the oversight of it has less meaning if you're not also adapting on that side as fast as we are adapting to the technological changes.

MS. COLLINS COOK: Thank you.

Jim, do you have some questions?

MR. DEMPSEY: Thank you. Thank you to the members of the panel.

I have some questions that I want to ask, but I saw there are a lot of audience questions. Was there one or two that stood out particularily? Technically, we only have five more minutes to go on this panel, so I'm happy, Beth, to have you ask one or two of the audience questions.

MS. COLLINS COOK: Sure, and I think you should know you have won the jackpot thus far on audience questions.

Alex, this one goes to you and it draws on a remark from a previous panel.

Why can't the IC inform the American people about how many phone records were collected pursuant to Section 215 and make similar public disclosures regarding the breadth of U.S. person collection under 702 and E0 12333?

So the executive order, understanding that you're not targeting necessarily U.S. persons, but the U.S. person incidental collection.

MR. JOEL: So that's a good question. I don't want to duck it. I'll just say that I am going to in certain ways.

No, but I don't want to, I guess I'm not going to get into the specifics of like 215 or 702, etcetera.

What I'll say is that there are two challenges. I understand the interest and I understand the importance. One is technical capability. Can you, in fact, count it? And for some things, some activities, you should be able to count. But for some other ones, they inherently involve challenges.

I know that one of the PCLOB recommendations in the 702 report was, in fact, to count some of the 702 collection that involves U.S. persons. So there are some inherent challenges in doing that.

From a national security perspective what I'll say is what I have heard internally as we have pursued these kinds of questions is that providing that kind of information can, in fact, put at risk some kinds of collection, especially if you track it over time.

An adversary, a sophicated adversary can put the information together in terms of the volume of collection in one particular area and then draw some conclusions about what specifically is being obtained, what are the specific channels that are being watched, and therefore change behavior.

So our job from a transparency perspective is to continue to discuss that internally and see, well, you know, are there ways of mitigating that? What can we, in fact, disclose in this area? Because it's of strong interest.

MS. COLLINS COOK: So, Erika, I'll direct this next one to you because you mentioned that part of the civil liberties protections and privacy protections are consequences for wrongdoing.

So the question from the audience is, in the case of a privacy violation sufficient remedial measures are critical. What, if anything, do you think needs to be done, either statutorily or administratively to strengthen existing remedial schemes?

MS. BROWN LEE: So, yeah, I do think that the remedies for Privacy Act violations or for privacy violations are, you know, as I said in my remarks everything could be examined and looked at for approval.

I was focusing my remarks on FBI. So of course they have their own investigative unit that reviews. So if there's any particular activity that an agent engages in, for example, that is, you know, collecting information in violation or specifically because of First Admendment purposes, that's subject to review and discplinary action.

With regard to individuals, I agree. I

mean we talked about how the FIPS doesn't really have as meaningful of really a guide for law enforcement either.

I think, you know, it's not something that I can do, but certainly it's been attempted before to remedy the Privacy Act or to amend it.

We are, the administration is committed to looking to expand the protections of judicial redress for non-U.S. persons, and DHS has a policy of doing so administratively.

But I think statutorily it's a hurdle. I think it's something that I would be willing to have a conversation to further that.

MS. COLLINS COOK: So just to keep this even across the board, Becky, this one is for you.

And I think implicit in this question is a very interesting premise. Do you anticipate that wide swaths of data will no longer be collected now that you are asking questions about whether they are really needed and the civil liberties downsides?

So I would say the premise is that it's your job to shut it down, which I think it's a widely shared premise.

And I think the basic question is, do you think you're going to be effective?

MS. RICHARDS: So I think that also starts with the premise that the collection we're doing currently -- that's starting with the premise that we're collecting too much information today.

And I think what I would say is that what we're working on is sort of a premise, so if NSA is filled with a lot of people who do math for a living, we're in the process of third grade math, which is folks need to show their work. So they need to show why they're doing what they're doing so that then we can have those conversations.

I don't want to presuppose we're going to do more, or less, or either way of those. But I do think that what we haven't done well is explain what we're doing.

And if you sort of consider that NSA has a long history of saying absolutely nothing to anyone, and in the last year and a half we've had to create a voice for ourselves to explain what it is we do, and recognize that most people, there are a lot of Ph.D.s in math at NSA who don't necessarily take well to speaking in public. It's a work in progress.

And so my hope here is not to be judged by how much we turn on or turn off, but by demonstrating what the value is to the country in terms of what we're doing and demonstrating that we're protecting civil liberties and privacy.

MS. COLLINS COOK: So thank you all for your remarks and your active back and forth on the questions.

MR. MEDINE: And we'll be taking a 10 or 15 minute break, and at 2:45 we'll resume with the private sector's views on these issues. Thanks.

(Off the record.)

MR. MEDINE: Good afternoon. Thanks for

everyone's endurance who's been here all or most of the day.

This is our final panel today, but an important panel on what the private sector has learned about privacy and how that might relate to the considerations we go into with regard to national security issues, and Rachel Brand will moderating.

MS. BRAND: All right, thank you, David, and thank you to all our panelists for being here.

The way we've structured the day is that the first panel this morning had to do with the theoretical underpinnings of privacy and exploring what interests underlie privacy. The second panel had to do with technology. The third panel was a government panel.

And this last panel is supposed to be focused on solutions, and particularly those solutions that folks in the private sector might be able to suggest.

So what we'll do here logistically is

each panelist will start with up to seven minutes of remarks. And for the panelists' benefit, Sam Kaplan is sitting in the front row here with yellow and red cards. So when he holds up the yellow card, you'll know you have two minutes left, so please pay attention, and the red card means that your time is up.

At that point, as the moderator I will ask about 20 minutes of questions, and then each of my fellow Board members will have five minutes of questions, and then we'll open it up to questions from the audience.

And as with the previous panels, when I start to ask questions some of our staff members will stand up in the back, and Lynn Parker Dupree in particular, and Prem, will stand up and hold up cards and you can go get yourself a card, write down your question and then the staff will pass it up here.

So we'll just go down the row and we will start with Professor Cate. I am not going to go into length on their biographies because I think they're all available to you.

But Professor Cate is a Professor at the University of Indiana School of Law, and he's been on a number of previous boards and commissions on privacy.

And so, Professor Cate, let's start with you.

MR. CATE: Thank you very much. This is the time I think to say that I'm colorblind so I'll have no idea what cards you're holding up. So perhaps you'll wave them in a definitive way and I will pay attention.

So first of all, I was sorry not to be here for this morning, but the last panel was absolutely superb, and it's a privilege, both to be here, and I really want to applaud the Board for taking up this I think really difficult, but fundamental, issue about what is privacy and how in practice might we go about protecting it, both in the private and the public sectors.

I want to really just offer some observations, as opposed to any specific, if you will, recommendations or conclusions.

One, and this was touched on in the last panel, I think the FIPPs are frankly not tremendously useful.

I'm not suggesting abandoning them, which is a big change for me. Ten years ago I wrote a book chapter called, the death of the FIPPs. But fortunately, I've gained a little bit of knowledge here.

But I think we use them almost talismanically, like we can roll out these eight principles, or depending on what list of FIPPs you use, and that that will get us somewhere. And that far too frequently, both in the private, and certainly in the public sector, they really don't get us anywhere.

What we end up is we end up, just like talked about in the last panel, looking for substitutes for the FIPPs. Well, we can't have consent, what could we have, rather than asking what was the purpose to be served in the first place?

And maybe consent's no longer relevant as a tool to achieve that purpose, rather what are we trying to actually do here? Really the question you've been asking all day, what are we trying to protect? What do we think protecting privacy really means?

I say this, by the way, about the FIPPs in part because I'm not sure that they've ever worked terribly well, and certainly in the U.S. environment where they've largely come to mean notice and choice.

I'm not sure that they work well in a world of massive data, whether we call it big data, or whether we call it just high volume data, but the notion of a sort of FIPPs-like approach, particularly with a focus on the individual when the broader issues may be, frankly, societal. They may be the impact on the economy. They may be the impact on civil liberties, not of one person but of everybody. And I don't know that the FIPPs help focus us in a useful way on that.

And then frankly, I think the FIPPs have led to some sort of silly results. And you know, I would just mention I've always been surprised, for example, the Department of Homeland Security privacy impact assessment on border searches of electronic devices, which focused a lot on notice as a privacy protection.

Well, at the point that your device has been seized from you and its contents copied it's difficult to think that notice is meaningful protection. It may be necessary, but whether it's protection or not, I think it's not.

Second point, one of the things we are seeing emerging in the debate in the private sector, and we see this especially in Europe in the context of discussing the general data protection regulation there, is greater focus on risk management, or risk assessment and risk management.

And I don't mean to use this just because it's sort of the jargon of the day but rather because risk management is an incredibly valuable tool that in privacy we are unbelievably far behind on. You know, security we have much clearer ideas what risk management mean. Privacy we really lack that understanding.

And part of the reason is because we don't know what risks we're guarding against. We're very unclear what are the harms, what are the impacts, what are the negative effects that we think we are balancing, if you will, with the positive outcomes of the use of data or what have you.

And so one reason I think the risk management approach offers a lot of value in both public and private sector is that it makes us stop and say, what is it we're trying to accomplish? What are the positive benefits and what are the potential negative impacts, not measured in terms of FIPPs, but measured in terms of actual impact on individuals, or on society, or on the economy, as we think about it.

When using risk management, or if you hate risk management, in either case, third point, I think there's a lot of reason to focus more attention on use of data.

And this has been a real weakness of the U.S. legal system. Those of you who have suffered through law school know that the Fourth Amendment has almost nothing to say about use of data whatsoever.

In fact, you can have illegally seized data that the court acknowledges is illegally seized and they will still allow it to be used someplace else because there would be no disincentive for the collection, it's only the collection in the Fourth Amendment that Supreme Court jurisprudence has been focused on.

And for this reason I think we really would be better to be thinking more about reasonable and effective limits on use. And in fact, I think that's what the public most commonly cares about.

And one of the practical reasons for that is because there's almost always a legitimate reason to collect the data. There's always some reason, there's some employment reason, there's some security reason, there's some private sector reason. You know, Verizon had a reason to collect this data. And then the question was, who could access it and how could it be used?

But our legal system has focused enormous attention on collection, and then once the data are in the government's storehouse then we feel that the data are more commonly out of control. And I think that is a critical area to focus on as well.

Fourth, as I've mentioned, I think the Fourth Amendment, while it's a critical legal limit and I certainly concur -- that's yellow, right? Yes? Thank you. And for the rest of you, you'll know I just got a yellow card.

I think the Fourth Amendment of course is a critical legal limit and we must of course observe it. It's not a very useful guide for telling you what to do in the future for a positive analysis of privacy issues.

And I think we should again be careful about that. Too often in our rhetoric we say well, it's permitted under the Fourth Amendment as if that tells us anything, other than it is not illegal under the Fourth Amendment. But it doesn't tell us anything about either the ethics, or the desirability or what have you of doing it.

And then fifth, I would just say in almost all of these areas, and I understand in national security this seems particularly maybe odd, I think redress is something we need to continue to focus on.

We see many uses of data in the government setting and in private sector which are done without regard to redress, with just sort of, well, if it affects a person inaccurately every now and then, what does it really matter? We'll deny boarding to people on airplanes, or we'll provide extra security for the wrong people.

This is not an efficient use of government resources and it's not a good way to think about privacy.

And I think we should be very clear in those rare exceptions where we say there might be no redress available here for the individual, in which case we now have to provide it through other means, inspector generals, or the PCLOB, or other ways of approaching it.

But at all times we should be thinking about redress, not just because of the rights of the individual, but because of the interests in ensuring that the system works as advertised and as it should. Thank you very much.

MS. BRAND: Thank you very much. Our next panelist is Harley Geiger. Harley Geiger is Advocacy Director and Senior Counsel at the Center for Democracy and Technology, and he focuses on issues related to civil liberties and government surveillance, computer crime and cybersecurity. Thank you for being here.

MR. GEIGER: Members of the Privacy and Civil Liberties Oversight Board, thank very much for inviting me to speak at your meeting today, and thank you also for your excellent work on ensuring protection for privacy and civil liberties in national security and terrorism programs. And congratulations on having one of the best acronyms in town.

When it comes to evaluating privacy protection, the Center for Democracy and Technology believes that the Fair Information Practice Principles are a very important framework for both government and the private sector.

Now you can add other privacy frameworks on top of that. We certainly do not disagree with Professor Cate that societal impact is a very useful consideration, and we certainly agree that protections focused on the purpose of data collection are also useful.

But we view the FIPPs as an indispensable framework for evaluating privacy protection with data collection practices.

Now the individual principles of the FIPPs, as you know, are overlapping and mutually dependent on one another. It is a framework. It's not a smorgasbord that you can just choose and pick, at least not unless you don't want robust privacy protection.

And there is obviously some discussion in the private sector about doing away with data collection limitations or the data minimization principle of the FIPPs, seeing as how we are now all in an age of big data.

But in the time that you've given me, I want to address this head-on in the context of government surveillance.

First, CDT believes that there still should be collection limitations on private sector data collection, and that the data minimization principle of the FIPPs should apply to the private sector.

Second, the government should not take its cues entirely from the private sector when it comes to national security surveillance. Data collection from the private sector is fundamentally different from national security surveillance.

Therefore, even if the private sector were to collect data in a relatively unrestrained manner in some alternate universe, then intelligence agencies should still nonetheless not follow suit.

The missions of the private sector and the national security functions of governments are totally different. That should go without saying. The private sector typically does not use the data that it collects to detain or take kinetic action against the individuals as part of its mission.

Several major private sector companies have repeatedly responded to public outcry over privacy with enhanced transparency and privacy controls.

The national security arms of government are not as transparent or responsive and are not likely to be.

Many major companies, in addition, allow or are required by law to allow consumers to limit the collection of information about them. More and more services are differentiating themselves on the basis of strong privacy protection.

And of course, individuals can choose not to participate in a commercial service as a means of limiting direct data collection about them. But data collection for national security purposes does not permit any meaningful choice.

So this is not to laud private sector data collection practices because CDT does view them as generally insufficiently protective of privacy.

But because of the differences that I just briefly listed, and other reasons, even if the private sector fails to robustly apply the FIPPs government agencies should not follow suit.

If anything, because of these differences government should strive for a more strict and consistent application of the FIPPs than that of private sector data collection.

And so I have a small set of broad

recommendations to make.

First, the government should place greater emphasis on applying the data minimization principle of the FIPPs. Back-end minimization procedures alone are not sufficient. Front-end minimization is also critical.

Trust is breached at the point of collection. Once the government collects information, non-statutory internal restraints on access and use can fall away like sand castles on a beach. We saw this happen with the 702 backdoor search loophole.

So surveillance should be restricted at the front-end by narrowing limiting the collection of data to what is directly needed to accomplish a specific purpose.

The data should then be retained only as long as is necessary to fulfill that purpose, and the data should be destroyed unless a determination is made that the data are needed to accomplish the specific purpose.

The specified purpose of data collection itself should be subject to meaningful restriction.

For example, limiting the scope of what is relevant under Section 215, or the definition of foreign intelligence in Executive Order 12333.

So the goal should be overall to move from mass data collection to targeted data collection of both U.S. and non-U.S. persons.

Second, the government should provide much greater transparency regarding the interpretation of surveillance laws. Section 215 of the PATRIOT Act exemplifies this.

Nobody was surprised that the NSA is collecting phone records. What was surprising was that the NSA has secretly interpreted Section 215 to allow for the collection of all phone records in the entire country.

This is bad data minimization. And yet, a fair reading of the statute does not seem to grant them with this authority.

So declassification of FISA court orders, or, when necessary, summaries of opinions would substantially boost transparency. We should not be a nation of secret laws.

Third, the government should provide greater transparency around the extent and scope of requests for data under national security authorities. This includes government reporting about its national security surveillance activities, such as how many requests were made, under which surveillance authorities, and for what type of data, as well as how many U.S. and non-U.S. persons were affected.

The government should authorize the private sector to make similar reports.

Information is power and privacy is control of information. An entity possessing information about an individual has power over that individual.

Large scale government collection of information about individuals threatens the relationship between citizens and the state because it upsets the balance of power that supposedly exists in democratic society.

Therefore, CDT urges PCLOB to recommend that the government recommit to a robust application of the Fair Information Practice Principles, as well as other considerations, regardless of what the private sector does, with much more targeted data collection and greater transparency. Thank you.

MS. BRAND: Thank you. Our next panelist is John Grant. Mr. Grant is a Civil Liberties Engineer at Palantir Technologies, and he previously served on the staff of the Senate Homeland Security Committee where, among other things, he oversaw the Department of Homeland Security. Thanks for being here.

MR. GRANT: Thank you very much, and thank you for the invitation to speak today.

As I never tire of telling people, I was a congressional staffer who worked on the legislation creating PCLOB 2.0, so I take a pride of parentage in the Board and I'm sure it's every parent's dream to one day testify in front of their children.

I know that the Board and a lot of people are familiar with Palantir so I'll spare everybody the extended commercial. Just suffice it to say, Palantir builds a data management and data analytics platform that works with data.

We started in the law enforcement, intelligence space and have expanded to deployments around the world and in a variety of contexts in the financial sector, medicine and elsewhere.

A core tenet of Palantir is that our technology isn't successful if in the course of achieving an organization's analytic mission we're not also able to be deployed in a way that protects privacy.

And that's something that the founders of the company instilled from day one, and that is why my job exists, a civil liberties engineer.

Well, one of the things I learned when I went to Palantir, and this is different from the Hill certainly, is when you walk into a room and you say to engineers, I'm worried about this thing you're building, it creates a privacy problem. The response is, oh, okay, how do I fix it? Which is not often what you get sometimes when you raise these things in other places.

So it's our job as a civil liberties engineering team to come up with suggestions for how to fix it.

I am a lawyer, as you may have guessed, so I do not necessarily possess a lot of technical skill. So the main role for us is to translate between the lawyers and the engineers and back.

So what I wanted to focus on today a little bit is some of the technology at a high level, and then I had some actually suggestions for moving forward that I think are actually fairly low hanging fruit.

So just briefly to provide a little context, as I said, Palantir is data management and data analytics, so we're not dealing with the collection of data. So this gets more to Professor Cate's point about the use of data.

And we have two sort of high level categories of technology that deal with managing or protecting privacy with the use of data, and that's access controls and oversight mechanisms.

But I want to start by pointing out, and I think this is something to keep in mind, that just as technology has expanded the power of surveillance today and the amount of data that can be collected, it's also significantly expanded the level of privacy protection that is available at the agencies.

If you imagine 50 years ago if there was an FBI file, this was probably pieces of paper in a Redweld sitting on a desk somewhere, or maybe locked in a desk drawer, hopefully locked, or maybe in a dusty basement archive or something like that.

And you know, there'd probably be very limited tracking of where the file was, you know, hopefully a log book with a name and who had the record. But who knows?

And anyone who accessed the file would

be able to see whatever was in the Redweld. You'd just be able to rifle through it and you could see anything, even if it wasn't directly relevant to what you needed.

Oversight into how the file would be used would really be nonexistent. You wouldn't see exactly who added information to the file, who deleted information from the file. And deletion would largely be hopefully a burn bag or a shredder, probably just crumpling it up and throwing it in the trash. A more precise deletion would be a black magic-marker redacting a few points of information.

Today. So today technology allows us to do a lot more management of data and oversight, and management at a granular level, and that's what the access control point, which is you can now build access controls to manage data very precisely on a data point by data point basis.

And you can do it in a more nuanced way. You don't have to make a choice between access or not access. There are ways to sort of have gradations of access. You can make the access controls dynamic.

So there's a lot of options. And the many options you have to configure those access controls give you a near infinite variety of options in how to manage the data, who can see the data and what they can do with the data.

The other point is oversight mechanisms, and this is really thinking a lot about audit logging and also using technological, electronic work flows to control exactly how data flows around an organization, and who can see data, and exactly what kinds of analysis they can do with it, even automating, or at least hardwiring in an approval chain for use of data and things like that.

And these can be very detailed. So the hardwired approval process and things like that, that can be very complex. It can involve multiple actors, it can involve multiple stakeholders.

And then the auditing of how data is

used itself can be incredibly granular and incredibly detailed.

And I'm skipping over a lot here, but I want to get to some of the other points. But just these two capabilities are a significant improvement of what existed before and can get us a long way.

And there are things that exist today. Now, I'm obligated to say that of course Palantir does these the best, but these are not technologies that are exclusive to Palantir. And they can be deployed and they can be used in a lot of different contexts.

So what is the problem today, and why aren't these capabilities being used more than they could be and at the level that we think they could be?

A couple of things. One issue is technical awareness. Lawyers don't know technology and engineers don't know law, and you need people who know both of these things to be able to make the decisions of how to use these technologies, how to incorporate them effectively into programs.

Lack of resources. You need people who can actually manage the data. And we talked about this in the earlier panel. Alex Joel has a very small staff. Erika has a very small staff. And they're managing huge amounts of data and huge organizations. They need resources, they need infrastructure to actually be able to do this.

Privacy is hard. How exactly do you look at an audit log? How do you use it effectively? How exactly do you manage access controls at this data point by data point level, especially when you're dealing with mass amounts of data?

And the last one is death by anecdote. The argument, the debate, the cost benefit analysis right now tends to be the national security sector saying one time we caught this bad guy using this information, and the civil liberties community saying one time this unjust thing happened to a person because of this program.

There needs to actually be a much more -- you can't just make this argument on anecdotal grounds. You have to actually look at the data and you can find out more specifically how these programs are working, how effective they are.

So solutions. Obviously we suggest some of the solutions in listing the problems.

Education. I think, and Palantir actually sponsors fellowships with Paul Ohm's Silicon Flatirons Project and other places to make sure lawyers can learn technology and that engineers can learn law.

Engineers don't have to be lawyers, but it actually should be a requirement to have an engineering ethics program and to have courses that teach engineers privacy, because they're going to build the technology that's going to hit the streets and it's going to be months or years before the law catches up.

So shouldn't engineers be able to catch, you know, how what they're building is going to affect privacy and be able to start thinking about these things?

Infrastructure. If privacy is an important value for us as a society then we need to invest in infrastructure to support it.

Concrete guidance. We actually need to go beyond just systems should have use limitations. We need to actually tell people how are you're going to do it? And I can get into that more if people have questions.

But we need to be writing really specific guidance, rather than just the, you need to have notice and consent, you should be thinking about use limitations, things like that.

And last, everything in the world can be datafied these days, including how these systems are working and how effective they are. And we can do the analysis, and we can get beyond anecdotes, and we can start analyzing data and figuring out is this effective, is this not effective, is this having negative effects, is this creating bias analysis, etcetera.

Thanks very much.

MS. BRAND: Thank you. And our last panelist is Chris Inglis. He is currently a venture partner at Paladin Capital Group and is the former Deputy Director of the NSA. Thanks for being here.

MR. INGLIS: Great, thank you. And I'm honor bound to say that I spend most of my time teaching at the Naval Academy in the Computer Science and the Cyber Operations Department.

First, I, like the other panelists, am grateful that you've established this venue for what I think is a really important dialogue, and I'd like to make four quick comments and then help us get to question and answers.

First and foremost, I absolutely agree with the panel's premise, which I believe is, is that the framers of the Constitution did not intend for security and privacy to be in mortal combat and we're therefore trying to figure out how do we achieve both.

And it may well be that we cannot trade one for the other. I think that's right, we cannot, but we have to work harder to achieve both. And I think technology and practice from the private sector can be helpful there.

Two, I agree that government is different, not simply in the powers, the tools that it might bring to bear on its citizenry or others, and therefore should be constrained, but the government alone has the requirement to essentially meet the standards of the First, Fourth and Tenth Amendments within the Constitution.

I will tell you that from my NSA experience, the Tenth Amendment was the most significant of those, which essentially says unless you have the authority to do something, you do not, you know.

And against what has been said, which is that backdoor searches or 215 was NSA's interpretation, both of those were specifically permitted under court approved procedures and specifically were interpretations of the law that went through three branches of government.

I think that's right and proper. That doesn't necessarily justify them. It may be bad policy at the end of the day, but the rule of law has to pertain, right, in terms of how the government gets things done.

Point three, I would say that largely I agree with what John had to say. Matter of fact, I wholly agree with what John had to say, that the aspects of law and technology are often at odds with one another, not because they cannot be reconciled, but because they're perceived as independent biases on any particular solution.

And I would add a third, which is that what typically plays out in any one of these systems is that you're trying to effect a technology, law, and the operational practice of those who essentially make use of the technology.

And the unsurprising result is that because they do not change at the same rate, they essentially change at very different rates, keeping them reconciled or synchronized from moment to moment is really hard.

Therefore, mechanisms, FIPPs-like mechanisms or other things are not likely to satisfy the need.

What you need are threads or systemic solutions that essentially you pull through and you take both art and science process to essentially try to figure out how to make some solution here.

I'll wholly agree with John that education's going to be absolutely essential. At NSA ultimately when we found ourselves in the midst of some compliance incidents for which no one had intentionally made a mistake, we actually had to sit down and figure out how do you achieve a horizontal join between the technologists, the legal practitioners and the operators, all of whom were trying to achieve something that was slightly different, but ultimately invested in the same problem set.

The last point I would make is that I do believe that there's a role for big data, what is sometimes called mass collection. There's a role for big data, but the principles that should pertain to the government's collection of that should be the same as surgical data, which is necessity and proportionality.

The government should be able to justify on what basis this is necessary, such that it could then argue, not for an encroachment upon civil liberties or privacy, but how do we then work harder to achieve the sustainment of privacy and civil liberty. And it should only achieve that in proportion to that need.

Therefore, I think that all those four comments aside, I would say that the private sector probably has a lot of experience in this regard that the government can take advantage of.

My own sense is that the government collects far less information than is perceived by the public, and certainly far less information than the private sector does.

Again, I don't excuse the government for that. The government should be held to account, but the government can, in fact, bring technologies in that might well scale quite well for the government's purposes because we'd have to scale them down, as opposed to scale them up.

I'm open to any questions you may have.

MS. BRAND: Thank you. Just a reminder to the audience that there are PCLOB staffers in the back with cards and if you'd like to direct a written question to the panelists, hold up your hand, find one of them and then write down your question.

And for the benefit of the audience and the cameras, for the panelists, when you're answering a question if you wouldn't mind moving the mic back and forth. I'm sorry, we don't have as many mics as we probably should.

So I'd like to start by asking about oversight, and I'd like, Mr. Grant, to direct this question to you first.

Both in your oral statement and in the written statement that you submitted to us, you talked about a wide range of mechanisms, paper trails, electronic work flows and things like that, and frankly, on the written statement it seemed like an overwhelming array of different ways to engage in oversight.

I think for a couple of reasons you need to choose your oversight mechanisms. One is that any agency is going to have limited resources to dedicate to oversight.

And secondly, as I mentioned in a previous panel, there may come a point where there are diminishing returns on oversight. You need to leave these people doing the work at the NSA or other agencies time to actually do their job, not just comply with oversight mechanisms all day long. So you have to find some balance.

So have you given some thought to what constitutes an effective oversight mechanism? How do you rank different mechanisms in terms of their effectiveness?

MR. GRANT: Yes, so I think we should actually think about oversight as a big data problem and then apply the same thinking to it that we would apply to trying to analyze signals intelligence and trying to analyze huge amounts of transactional data for marketing.

It's a similar issue. You have a huge amount of data, as you say. There are massive amounts of audit logs, for example, in an organization like the NSA, and that's a lot of information.

But you can use technology and analytic tools to make sense of that information and derive the insights that you're looking for.

So but part of the issue is, A, you need to do it, you need someone. So we see this all the time in Palantir and I know other organizations see this as well, which is, everybody checks the box on FISMA for audit logs. We've got the audit logs and we will go through an enormous number of hoops to make sure it's logging exactly the information that it's supposed to.

We get fewer requests to actually look

at the audit logs once the auditing mechanisms are turned on.

And looking back to my congressional experience, there aren't many laws that I can recall that tell anyone they actually have to look at the audit logs, they just have to.

It's the Seinfeld joke about renting a car. Everybody can take the reservation but you have to hold the reservation. You have to use the information.

So I think, I mean to me that's how you make oversight more effective, you use these techniques.

And that's another thing. The oversight people and the information security people and things like that, they should be as good as your analysts, and you need to have good people who are also doing the analysis and conducting the oversight.

So to get to your last question, which is the most effective? I think it's using that auditing data. I think it's using that big data that you've got and having a team of people that can proactively comb through it.

And not only are you going to look for people doing something wrong, but you can also ask questions such as, you know, does our data retention policy make sense?

You could look at the data and say, you know what, it turns out we keep data, this data set for five years. Nobody ever uses the data older than three years in that data set, so let's change the data retention policy to fit with the actual usage of the data.

MS. BRAND: Thank you. Mr. Inglis, I'd especially like your thoughts from your time in government, what did you view as an effective oversight mechanism?

MR. INGLIS: So first and foremost, if there is an authority that is granted or a burden that's imposed, and they come hand in glove, you know, that's not a one time thing. There cannot be a repurposing somewhere later simply having gotten past that threshold.

At NSA the typical events might be constituted as collection, processing of data, analysis of data, dissemination of that data, and the burden was imposed at every step according to whatever the authorities were that were granted for the acquiring of that data, the acquisition of that data in the first place.

And what we ultimately found is that in order to achieve that, because data ultimately is aggregated, synthesized, a typical counterterrorism analyst, we take the iconic analytic effort, doesn't simply use data from one source, they use data from many sources.

And at that point it is really hard, if there are different expectations of the different data sets to try and keep it straight in your head as to what you're going to do about that.

So the focus has to be how do you bind the attributes for a particular data element at the moment that it comes into being?

MS. BRAND: Could you pull the mic a little closer.

MR. INGLIS: At the moment you collect a piece of data, how do you bind the attributes to that data that essentially include, but perhaps some other things as well, what was the authority under which this data was collected? What are the burdens? What are the imposed constraints that come along with that? What are the proscriptions, if any, associated with that?

And that should be atomically bound to that data element through its life, through its life of collection, processing, analysis and dissemination.

Now at some point there's going to be a second order use of that data where someone essentially reads a broad swath of material, synthesizes that in their head and then constructs a document across an air gap.

That gets hard, but at least in that primary use of that data if you had a systemic view of it from start to finish, you make the auditor's job or the compliance oversight much, much easier.

And you therefore then in your system, in your technology essentially impose a constraint or a check every time something exercises privilege against that data, whether it's a collection, or analysis, or processing, or in dissemination. That makes the auditor's job much easier.

And frankly, it has a nice deterrent effect on those inside the system because they know at every moment that they are held to account.

But in my experience in government it's not so much the deterrent as it is the assist in an otherwise very, very rule-laden environment.

A typical counterterrorism analyst at NSA would often deal with hundreds of constraints on the data sets that are available to them because various orders of the court, interpretations of the court, kind of sharing arrangements with various other nations would all come along with their independent assessments of how the data can or should be used.

So the bottom line is that technology can help us by essentially doing an atomic bind, right, meaning that it's organic to the data itself of what's its provenance, and that provenance should never be lost through the history of that system.

MS. BRAND: Thank you. I'd like to turn to the FIPPs, and Mr. Geiger, I was happy that you raised those, and Professor Cate as well. So I'd like to direct this question first to the two of you.

So, Mr. Geiger, I noticed that in the written statement that you sent to us, you talked about the FIPPs but you didn't really talk about the individual participation FIPP.

And I guess when I talk about the FIPPs I'm referring primarily to the DHS version.

You said in your oral statement just now that the FIPPs are not a smorgasbord, they're a framework, you can't just pick and choose among them. And if that's the case and if you have to employ the individual participation FIPP, how can that work in a surveillance context?

MR. GEIGER: So that is the toughest FIPP to apply in this context, absolutely.

One way that you could do it, which is not politically viable and perhaps not even good policy, would be to loosen standing requirements on individuals to bring suit for violations of law.

But my, I think, more reasoned answer is that if the individual participation FIPP is lacking in the national security context, then the rest of the framework has to work overtime to compensate.

And that includes data minimization, which is why I emphasize collection limitations and transparency, as well as the rest of the framework.

And I mean I absolutely recognize the challenges in applying individual participation, but this is one area, again, where government is different than the private sector and I think that difference should express itself in particular in the data minimization principle.

MS. BRAND: Professor Cate, do you have thoughts on that?

And I would ask also, there's been a lot written and said in public more recently about how perhaps the consent and individual notice FIPP really doesn't work very well in the private sector, either because nobody really understands what they're consenting to. Even if they understand it they don't have any other option, so they have to consent to get the service, and it's kind of a meaningless exercise.

Do you have thoughts on that and whether the individual participation FIPP can work in this context?

MR. CATE: Thank you very much. I do have thoughts on that, especially being one of the people who's written some of that.

I think the challenge of the FIPPs is that the they often lead us in the wrong direction. And I think this is a real challenge. I'm not in any way trying to make it sound easy or make it sound like there's a simple answer here.

But, for example, if we think about the FIPPs in sort of their classic 1980s OECD FIPPs, we're talking about notice and consent, we're talking about purpose specification, we're talking about use limitation to the purpose specified, and then we add things like data minimization and individual participation.

And frankly, almost all of these seem challenged in a modern data environment, private sector or public sector.

In other words, how does that really work? You know, there are 60 people in the room, they all have cellphones, they have recording devices, they have video, they have audio, I don't have a policy statement from any of them. I don't know about my individual participation rights. I suspect they would look down on my wanting to interview them each about it.

It's not a meaningful way to approach the issue. The issue is an important one, which is how to protect privacy. But shifting the burden to the individual, which is what the FIPPs have the larger effect of doing, is a very difficult way to approach that. And I think it's an impossible way to approach it in the public sector environment.

But it also may lead to completely wrong results. In other words, one of the surprising things to me, and I can't believe I'm going to say this in a place that's being recorded, but about the Section 215 was that the NSA collected all this data and did so little with it. It was astonishing.

And so you would like to say, you know, when people talk about atomically binding the limits on what you can do with the data with the data, I'd like to think if we thought of something new we might do with the data that might really have a major effect on national security, we'd have a process for some sort of risk analysis, what's the benefit, what's the risk, what are the processes in place to protect it, now let's do that thing.

In other words, data has real value. It does in the national security environment, it does in the private sector environment.

And I think we need to be thinking about approaches here that aren't binding everything to some mythical transaction that took place at which in the FIPPs world we say the individual agreed to this, even though I can't think of a case in which the individual actually agreed to it or it was meaningful consent.

And then in the national security world we just overlook that. We just say, well, we've agreed for the individual because we think it was important, without again doing a clear and well-documented type of risk assessment using clearly articulated values and harms, benefits and harms.

MS. BRAND: Go ahead.

MR. GEIGER: If I can just make three additional comments on the FIPPs. One, so it does sometimes lead programs in the wrong direction.

It is a useful framework for evaluating privacy protection, but the application of the FIPPs, what you're actually doing with the program, you may pass muster under your privacy impact assessment, but the actual the way the program is conducted on the grounds may not in fact be privacy protective.

So I don't think that the FIPPs are a silver bullet, but the principles themselves I think are very useful for the evaluation of the program.

Second, there's been a long-standing controversy about notice and consent being inadequate, but that is why I said at the outset that the FIPPs is a framework. I mean each principle is dependent on the other.

This came up very clearly in the healthcare context. People don't know what they're consenting to when they receive a notice from their doctor. They don't know what the HIPAA privacy notice really says or means, or what HIPAA does, which is why there has to be a lot of additional privacy protections in place to actually meaningfully protect that individual's privacy.

And then lastly, FIPPs are not the only framework. I think that it is a very useful, I think it's an indispensable framework, but there are certainly other frameworks that can be applied and should be applied to the evaluation of security or data collection programs writ large.

MS. BRAND: Although this was the subject of the first panel today and not necessarily this panel, I want to ask about it anyway. So apologies if I'm springing this on you.

But I'd like to give you all a chance to give any views you might have on privacy, what is privacy, the sort of nature of the underlying privacy right.

And Mr. Inglis in particular, when you were at the NSA, I assume you spent some of your time thinking about how to protect privacy and civil liberties and as you were doing that, what did you think that meant? What privacy interests were you trying to protect?

MR. INGLIS: I would say I don't think that has changed over time, though the technology might hold that at risk in different ways and there might be some downstream consequences, given the scope and scale. But the fundamental question always comes back to two things.

One, with respect to the perspective of the individual, is there a reasonable expectation of privacy for, fill in the blank what that information might be.

That's the stuff of great legal debate, but operators think about that as well, particularly the operators inside the government because they're constrained by the Tenth Amendment to think about what is it they're actually authorized to do, everything else then being proscribed.

But the second way to think about the issue of privacy is then what might you learn if you take these discrete data sets and combine them in a way that might then give you some insight into things that were not self-evident from any one of the discrete data sets.

You have to therefore think about the problem in the aggregation, synthesis downstream. Again, you might have some thresholds there that you have to think your way through that you don't want to go beyond at that particular point in time.

I would tell you that at the National Security Agency ethos is as important as the compliance rules, the FIPPs mechanisms and things of that sort. Absent ethos, absent the art, right, the science will lead you astray and you'll essentially get into a place where science alone cannot help you essentially navigate the challenge, the question of how do you achieve both security and privacy in a world where they are massively converged in a place called the Internet.

MS. BRAND: Professor Cate, do you have

a thought on the nature of privacy?

MR. CATE: I was afraid we might run out of time before you got to me on this.

I would say two things. One, this is an area where I think public sector versus private sector is a really important distinction and I think it has to be kept clearly in mind.

In the private sector I think of privacy mainly in terms of, if you will, harms or impacts on individuals or on groups of individuals.

So whether that's the way we think about it in the Fair Credit Reporting Act, like a higher price for credit or denying someone a benefit, or whether it's some other way in which we think about an individual being manipulated or being driven to pay a higher price or what have you.

In the public sector I think that is also true. I think all those specific impacts, those harms, if you will, although I don't mean to limit them to physical or financial harms, are present as well.

But I think there's probably something more in the public sector, which is privacy, from I think the very beginning of the constitutional debate, was seen as something about the balance of power between the individuals and their government, between the citizenry and the government.

There is something quite striking, and this I completely agree with Harley about, the more the government knows about individuals, the greater the risk that that information will be used in a way that alters that balance of power, that makes the government more powerful and makes the individual less powerful.

And it's, you know, a widely observed but an ironic twist as we've gone into the twenty-first century, we've in many ways gotten less transparency to the citizen about the government and more transparency about the citizen to the government.

That is a clear alteration in that relationship, that power relationship or that oversight relationship.

So in that sense that's why, again, whether one focuses on collection or use it may be a not so significant matter, but I think at the end of the day it is use that matters. It's knowing how can the government use this information in a way that might affect me, as opposed to is the information out there, which seems to almost be the answer is yes now.

MS. BRAND: Mr. Grant.

MR. GRANT: I don't have necessarily the answer, but I think I have sort of a framework for thinking about it, which is to start to think about it from the perspective of social media right now because I think in that space you're seeing how, especially younger people, are viewing privacy.

If you ask, so most of the engineers at Palantir are, they appear to be about 14, and we had some discussions internally about sort of our own information security policies and should the company be able to look at social media like

LinkedIn, Facebook, publicly available information, but look at it as part of our own inside policy. There are ways to detect phishing and things like that using this kind of data.

And they vigorously objected to their own employer looking at that data, again, for a reason of information security.

So it was interesting to explore with them and to say, but you tweeted, you tweeted that, which means people are going to read that. It is a tool for communication to the world.

And they still felt, yeah, it is publicly available, anybody can Google it, but they still have an objection to government collecting it, or even government reading it, and then their employer reading it and things like that.

So I don't know exactly what that means in terms of coming up with a final definition of privacy, but it suggests that people, there is a different view of it. And that even public information, there's still privacy inherent in public information somehow.

And like I said, I think talking through sort of attitudes towards social media and understanding that could help us figure out what is this, the newer conception of privacy in this technological age.

MS. BRAND: Did you have something to say Mr. Geiger?

MR. GEIGER: Sure. I mean, I said most of it during my opening remark. I mean I do view privacy in the lens of control. I view it as an individual's ability to control information about herself, but then also the control that the entity holding information can exercise over individuals.

I think it is very important not to just look at privacy harms, or privacy interests, or the extent that privacy can translate to control over a individual or their decisions in the context of today's technology.

I think that it's very important to try to look out the next couple of decades and sort of see what is coming down the pike. And there are some very pervasive, very privacy intrusive technologies that are, that I think we will see in our homes and maybe even in ourselves in our lifetimes and certainly in our children's lifetimes.

And the laws have absolutely not kept pace, and without a change in the law, again, I reiterate that internal protections on use and access, while important, are not sufficient because they can change. They have changed.

When we talk about protecting privacy, I think that we should be looking, as I said, to what we are protecting several generations down the line.

MS. BRAND: Just to get back to the topic of this panel again, Professor Cate brought up use restrictions. We've been talking about that throughout.

We're focusing on how the private sector might have solutions that the government might learn from. Private companies are obviously doing something to control the use of information they collect. They have to. They have a privacy policy that says what they're going to do with your information and they have to comply with it.

Are there mechanisms that the private sectors has used for enforcing their use limitations that are particularly effective that the government might learn from?

Mr. Grant, do you have a view on that?

MR. GRANT: So we see this a lot obviously in terms of, so we, ourselves, don't hold data but our customers hold data, and trying to help them implement compliance.

Honestly, actually, they use the same basic mechanisms that I described in my testimony and often they have the same basic weaknesses.

You know, do they have the infrastructure to manage access control to the granular level? A lot of them do not because it costs money and it takes time.

Are they conducting the oversight of the data? Probably more so than some people and possibly the government, again, because of limited resources. But they're still probably not doing it at the level that you would hope.

One thing I notice is that a lot of them, there is, even in Europe where you have more commercial privacy law and more commercial privacy compliance requirements, a lot of times it's best guess.

So, for example, one that we've been running into recently now is looking into cybersecurity and information security, data exfiltration risks in the private sector.

And in these giant, multinational companies they're trying to deal with employee privacy laws that are all over the map.

And they're asking questions like, if a German employee sends an email to a U.S. employee, what privacy rules apply to the content of that email?

In Germany you have to actually tell the employee, I'm about to start monitoring your email. In the United States you can pretty much do whatever you want with a few exceptions. They don't know what the answer is so they make their best guess.

So I think there are interesting lessons in terms of what the privacy is trying to do, but I actually think they're facing a lot of similar problems that are related to scale, that are related to lack of understanding of what the rules should be, as the government.

MS. BRAND: Anyone else have a thought on that question?

MR. INGLIS: If I can add to it. So my own sense is that there's probably a lot of great technology out there that can be used, but any technology can fall short of your expectations if you don't use it in the right process, and therefore, we ought to give as much time and attention to process within which that technology might be used as the technology itself.

In the following process it might be useful to consider that first and foremost before you acquire any capability, whether it's in the government or within the private sector, you think your way through the necessity proportionality considerations, you know, is this necessary and have I done this only to the degree that it is necessary.

And then what we're trying to achieve is not simply the balance between security and privacy, but transparency is the third leg of that stool. And absent transparency, you often find yourself in a place where people don't believe that you achieved the right balance of the first two.

That then derives, you know, the possibility in the government the need to essentially acquire explicit authority, which always comes with constraints, constraints are bound to that, and some measure of accountability for those constraints.

The process elements that then are essentially implemented to pull that off, I think should have the aspect of continuous compliance, not discrete compliance at various phase points, but continuous compliance. You think about it all the time, first, middle and last.

Kind of a stretched analogy is part of the problem with the absence of cybersecurity in so many environments is you think about that as a bolt-on. Until such time as we build our systems, operate our systems continuously with that foremost in mind as the primary attribute, it'll break our hearts.

The second process element of implementation is an external component. Internal components are really essential. You have to hold the people accountable internal with the system.

But unless there's an externally imposed accountability mechanism, you can wind up with mismatched expectations or the system might, in fact, go rogue.

And then three, there has to be at various phase points required reporting, which is important because that then forces some synthesis, some kind of retrospective that says, how do we actually aggregate our experience in this to come to some conclusions.

So is it meeting our expectations? Is it working as it should? Are we a little bit right of the course, left of the course such that we actually need to invest some time and energy in the process itself?

Absent that, you find that you're the frog in the beaker and it's just getting a degree hotter moment by moment, all of a sudden you're the boiled frog. And you hadn't realized because you didn't step back and take hard look at it that you actually got off course a little bit some time ago.

MS. BRAND: Thank you, and I think my time is up, so we'll start with Mr. Dempsey and go down the line.

MR. DEMPSEY: Thank you, and thank you to the members of the panel for giving us your time today.

In a way building off of something that

Chris Inglis said, or at least that I heard you saying that we need the technology controls, we need to build the technology in a way that implements these controls, but at the same time we need policies that surround them. You need the legal rules, etcetera.

I think, John Grant, my first question to you, you talked a lot about the potential in terms of tagging information, and audit controls, and permission controls are very granular, but just to state the obvious, that's not a substitute for legal rules and policies.

MR. GRANT: Absolutely not. We try to say, you know, even when we talk about our privacy enhancing capabilities and stuff, if you think you're buying a switch that you can flick that protects privacy, it's not going to happen. It's not possible.

You have to be able to respond dynamically to changing situations. You have to be able to make human-driven nuance decisions about data and about how it's used and is it being used appropriately. And that's just something machines can't do.

And it's the same reason we argue at Palantir that you can't build a find terrorist button, that you need a human at the top of the decision-making chain and at the top of the analysis chain to do it.

And so I distrust any technology that says don't worry about it, we've got privacy covered. And so what the goal should be for technologists is, what kinds of tools do policy makers need and then the oversight officers, the oversight boards, and the civil liberties protection officers and things like that, what do they need and what makes their job easier or possible, especially when you're dealing with data at scale.

So an easy example is there's a lot work, a lot of research going into improving access control interface. When you're dealing, with terabytes of information in the cybersecurities space, how can you create technological shortcuts to allow a human to make the decisions about how to manage that data?

And that's how you do it. You think about how do you support the policy, not how do you replace the policy.

MR. DEMPSEY: Let me go to Fred. Fred, totally accepting your point about the limitations of the FIPPs and totally accepting your point about the importance of focusing on risk and focusing on use, you're not saying that collection is irrelevant, that obviously the Fourth Amendment is in some ways a collection limitation.

And that, you know, in a commercial context that company that had the flashlight app that was out collecting data, nobody even got to the harms analysis, that collection was inappropriate in and of itself.

MR. CATE: Right. You are absolutely right and I agree completely. In other words, I'm not suggesting collection is irrelevant, I'm suggesting we've made collection too much of the end of the story, so that once you cross, you know, it's like a spillway in a dam, once you're over the collection limit, then anything else goes.

MR. DEMPSEY: Well, the ironic thing is that at NSA, as Chris Inglis said, their view is they never thought of it that way, that they thought that you have your collection authorization which is critical, your retention, your use, your dissemination, your retention limit, that each one of those --

MR. CATE: But if I can just respond to that. I think there's something of a mismatch here. And I'm not in any way doubting either what NSA was doing or what Chris is saying.

But one of the astonishing things, for example, when I read the Section 215 report that came out from the NSA's civil liberties office, a well-written report, it was full of all of the limits on what they were doing and the incredible what can only be described as bureaucracy around that, both technical bureaucracy and human bureaucracy.

But it sort of ignored the fact, which is what I think has struck most of the American people, is how was the authorization obtained in the first place?

You know, we had a law that said relevant to a specific investigation, you know, 99 out of 100 people through relevant to a specific investigation meant, might be focused on specific individuals.

Apparently the 1 out of 100 who didn't was a FISA judge, and then had other judges there along with him, and apparently some members of Congress.

So I think one of the critical issues when thinking about going forward is if this were the private sector there would have been immediate customer feedback.

You know, if that were Facebook interpreting that to say, by the way, you know under that privacy policy that says we'll only collect data for limited purposes, it means that we're going to collect absolutely everything, and then there would be customer reaction.

What do we create that will mimic that in the classified environment, in the intelligence environment? Maybe that's the PCLOB. I mean maybe that's literally having the outside of the agency but focused on privacy and civil liberties that says we understand the challenge but we think you've got the wrong end of the stick.

But I think it is being overly focused, for example, on the Fourth Amendment that creates this problem. As you well know, the FISC just dismissed the Fourth Amendment issues by saying, well, third-party doctrine, there's no problem at all. Let's go ahead.

And somebody should have been saying, wait a minute, you're talking about collecting data on everybody. And then that would have focused the discussion in a way that all of the technological controls and all of the bureaucratic controls that have been now well-documented in the agency, somehow never did.

MR. DEMPSEY: That's very helpful. I don't want to further rehash 215, the history of 215, and anyhow I have a red card so I guess that's the end.

MR. MEDINE: So let me just follow-up quickly on that point. Maybe what we need to do is supplement the FIPPs with the OMG standard, which is, you know, in private practice I would have a client and I'd say, everything you've proposed to do is perfectly legal, but are you nuts?

I mean how do we embed that stepping back and saying, okay, the lawyers have technically signed off, everyone has technically signed off, but this is a crazy thing to be doing?

MR. CATE: Well, I mean I think one positive step is adding someone like Becky Richards and an office to support her within the agency. I think that's one way.

So you get people who aren't just

thinking about the law, but rather people who will say, I understand legal clearance is taken care of, but I still have the oh, my God response.

Are you allowed to refer to God at a PCLOB hearing?

MR. MEDINE: It's free speech.

MR. CATE: I feel very nervous about that.

I think the PCLOB is another way. In other words, you say we're going to have some of those similar roles, not by any means identical, but outside of the agency.

I think this is where I would say, although this just may reflect my naivete, you know, I would like to think that although we certainly need to have secret operations, we wouldn't have secret law.

And so if a law that said one thing was being interpreted to mean the opposite, that someone would feel the need to signal that, as opposed to going out of their way to continue to say, no, it doesn't mean what we actually think it means, and it means what only you think it means.

And so that we would build in avenues for transparency about the law, so that at least we all knew what the rules were going into it.

And I think that's a huge problem when the law itself is effectively classified because of the way in which the interpretative process works.

MR. MEDINE: Sure, John.

MR. GRANT: Can I just jump in on that? How we embed that in the private sector, or certainly in our company, and it goes back to my point about education.

Engineers and technologists think of things in terms of does it work or does it not work, and they just want to make things more efficient.

But it's not because they don't care about privacy and civil liberties. They end up living in the world they create. It's just they don't realize that this raises an issue.

So if you improve education across the board so that the technologists throughout the NSA and throughout the private sector that are building the capabilities and things like that, if they're all conscious of privacy and civil liberties, they're going to raise these questions too. They're going to say, what are we building?

And especially technology is an interesting place because it's the place where the engineer, the lowly engineer is more powerful than the CEO, because if the engineer says, I'm not going to build this, then that's it. And if the CEO says, I'm going to fire you, they say, okay, I've got four more job offers to go somewhere else. So there's a really interesting power imbalance there within the organization.

So if you instill the values that you're looking for throughout the organization in the people, that's where you're going to get the OMG response.

MR. MEDINE: I have a question for

Harley and Chris. In our 702 report we noted that most of the information that was collected wasn't reviewed and therefore wasn't minimized, and that even of the information that was collected oftentimes it wasn't minimized in terms of being deleted because there wasn't a determination about whether it had foreign intelligence value. Harley proposes doing the minimization up-front when it comes in.

So I have a question for each of you. One is, Harley, is that a practical matter given how much information is coming in?

And I guess to Chris, if that's not a practical way, how do we do minimization better?

MR. GEIGER: First, an unsolicited answer to your first question, which is in addition to the proposals that have just been discussed I think a FISA court special advocate would also help with the OMG standard.

I think that it's a multi-layered solution having privacy and civil liberties offices in agencies, a PCLOB and a FISA court special advocate hopefully gets us there.

In terms of whether front-end, so what I had said was that front-end minimization and back-end minimization are important. And so I actually, one of the things that I had said was that the determination ought to be made whether the information was needed and then flush it as a default unless that determination is made.

This is different than the way that I think it's done, at least in some agencies where they keep the information unless they make a determination that they don't need it, which is very different. And that sometimes causes information to languish. I think that that should be flipped.

In terms of front-end information data collection, I do think that it can be feasible, but it also depends on the specific program, it depends on the purpose.

And if the purpose is we're going to collect everything, that sets off the OMG standard for me.

But if the purpose is narrower, and I think generally speaking it should be, then yes, there should be data collection limitations.

I understand that there are technical limitations there and that depending on the actual means of data collection, sometimes it may be unavoidable that you collect more than you need, but then you should be flushing the information that you don't need.

MR. MEDINE: I'm probably going to run out of time, so Chris, if you have any reactions to that?

MR. INGLIS: Yes, so on both parts, so the question of 215, I know we don't really want to rehash whether that's good or bad policy, but from an NSA perspective three branches of government participated in the creation of that program, sustainment of that over years time, multiple administrations, more than three dozen judges.

And so from an NSA perspective, charged to essentially effect the will of government, short of a referendum amongst 315 million people, which we do every two years, I don't know how you actually kind of make a significant change in terms of how the government comes to some of those conclusions.

The PCLOB is an extremely valuable addition, but you know, I think that we're always going to find ourselves in a place where stakeholders stand in the shoes of those they serve.

With respect to your specific question, it's problematic on a couple of counts. You know, first and foremost, if you try to minimize at the point of collection you then ironically, paradoxically begin to focus on things that you shouldn't.

The strange truth in the world is that there are two ends of every communication in the world, sometimes more, right, if you add in the courtesy copies and the blind courtesy copies.

And if your interest is legitimately in party one and you begin to then focus on party two, right, who is involved in that conversation, without merit, without some reasonable or probable cause, you then begin to encroach upon their expectation of privacy, absent some kind of reason to do so.

So the policy at this moment essentially uses this, upon recognition, which isn't a sloppy policy. It just says do not focus undue attention on that, and when you do encounter someone who deserves further protection, take it. You must take it.

Built into that then are some time limitations for how long you can hold that data, and some necessity and proportionality conditions that say how much data is enough, for what purpose, and how long are you going to keep that without some meritorious reason.

So if it participates or contributes to a report you keep that for longer. If it doesn't, then there are time limitations, you age it off. And those are always prescribed by those who essentially grant us our authority.

MR. MEDINE: Thank you.

MS. BRAND: Ms. Cook.

MS. COLLINS COOK: So following up actually on a phrase that's been used a number of times today and asking the same question I asked a previous panel, there's this notion of reasonable expectation of privacy.

To the extent that that evolves over time, which I think that it does, how does one ascertain what is a reasonable expectation of privacy?

Is it based on a Washington Post poll that 50 percent of Americans are uncomfortable with X, Y or Z? Is it the conduct that individuals nonetheless engage in, that they're uncomfortable about communications surveillance but people still use their phones, they still engage in the world?

If we were going to look to reasonable expectation of privacy as a touchstone, how should we ascertain what it is?

This is a question for the panel.

Chris, I'll start with you because you had indicated that the NSA did look to reasonable expectation of privacy as one of their guidelines.

MR. INGLIS: First and foremost, there's a basis of law which doesn't, if the technology changes over time give us, say, a free pass to say because the law allowed us to use the old technology in this way, the new technology, which is more intrusive, can simply just continue unabated.

But there is a wide practice of law and the NSA considers that, you know, as it makes its appeals for authorities, which are always conditioned upon a Department of Justice representation and the right authority, either under 12333 or the courts.

Second, there is an expectation at a place like NSA that you think through the eyes of those whose privacy would be encroached upon, right. So you think about what's the expectation of the individual and is their expectation such, regardless of what the law might say, that this is something that deserves some aspect of privacy.

And that necessarily then has to inform the conversation about what authorities you seek and what then provisions you seek those authorities for.

Interesting dialogue earlier about the 215 program and the internal bureaucracy. At NSA we thought that was a feature, right, that the court essentially proscribed use of that database for anything but the very surgical and narrow application of it.

The sense at NSA was, is that if we had even requested to use that for other purposes, say, domestic terrorism, which is not our provenance, or say, weapons of mass destruction, rogue nations, that that would have been an encroachment into privacy that was excessive and therefore not meritorious right up front with respect to the possibility we might ask for that.

The program as designed was very

surgically, narrowly framed on something alone, which was warranted and justified under the concept of necessity and proportionality.

And we had to avoid the creep beyond that because of an expectation based upon the consumer looking back at us, as to what they might think.

MS. COLLINS COOK: John, you also used the phrase as well I think here, and so if you have some thoughts on this.

MR. GRANT: The thing that jumps to my mind and it gets back into, again, when I was talking about analyzing data to sort of support the effects of this program, I think it's reasonable to expect that the government won't look at data that's not useful.

That is a reasonable expectation of privacy, that the information that has not proven effective for some purpose, that that won't be collected and analyzed.

And that's what we've been doing, as I said, rewriting our internal information and security policies, and as we've surveyed everybody at the company they've said, I'm fine with you looking at some of this data, just tell me that it's useful, tell me why you're looking at it.

Because of course they're interested in protecting our own internal information security at Palantir, and of course we're interested in protecting our own national security.

So I mean this isn't the only standard. Obviously utility can't be the only analysis point because there obviously are interests beyond that, but I think it's a significant question that we don't answer very well right now.

And this is, you know again, across the board from that sector to the private sector, everybody wants data and they think they can do all of this stuff with data.

And we get customers all the time who'll come in and say, I've got to understand the Twitter. And we'll say, well, what do you want to know? And half the time, we'll say that information, if you want to understand do a lot of people like Justin Bieber or cats, then Twitter's great. If you want to understand more complex, nuanced theory, then maybe we should think about something else.

And I think that government should do the same. And I think the government can answer those questions, again, looking at, analyzing how data is used and using that data about data.

So to me that's one area where you would sort of expand that definition of reasonable expectation of privacy, which is it's reasonable to expect no one will look at data that isn't useful.

MR. GEIGER: The question you pose is a very difficult one. I mean courts are wrestling with it all the time. And everyone has a personal opinion about it, and so do I. I believe that reasonable expectation of privacy is a terrible framework actually.

The Fourth Amendment is supposed to

protect against unreasonable searches and seizures. The reasonable expectation of privacy is a judicial-made creation that has now allowed for some very unreasonable searches and seizures. Section 215 is a great example of that.

Under the reasonable expectation of privacy framework, U.S. versus Jones notwithstanding, because I know that's kind of a mysterious opinion, but the Supreme Court seems to be sort of moving, inching along perhaps in a direction where they are doubting the reasonable expectation of privacy framework as it's been applied in the past several decades.

But under current law would it be okay under the reasonable expectation of privacy test to have a network of drones or a network of ground-based cameras that watch everything that you do the moment you step outside of your house?

I mean there is a very strong argument that, yes, that is okay under the reasonable expectation of privacy framework.

So I think that it's the wrong framework to be viewing a lot of this stuff. I think that it does not have to be left out of the conversation, just like the FIPPs, it is one framework.

There should be multiple lenses, but none of them, including reasonable expectation of privacy, like the FIPPs, are going to be a silver bullet. And they're not going to provide you with a clear answer.

MS. COLLINS COOK: I think if I have time for one additional question, I'm still seeing yellow.

So moving up the analysis of data and requiring agents or analysts to make an assessment of whether or not information is relevant or is necessary to maintain, rather than potentially letting that information simply age off of your system, what about the privacy implications of that type of approach, which to me, I have been unable to get past this notion that that would require agents or analysts to put eyes on more communications than they would otherwise review. And so what is your answer to the privacy implications of that shift?

MR. GEIGER: I mean I suppose that there are two ways to do it. You could require the agent to look over every piece of data that they've collected.

If the amount of data is small, which is my main point, I mean having, not data retention but collection limitation at the front-end. If the data population is small that is less of a problem.

If you're requiring the agents to look through a large amount of data that you know contains information about individuals who are not connected to a crime or terrorism, that becomes more of a problem.

Then on the flip side I suppose you could have the agent merely looking at data that they know is connected to other parts of their work.

I mean I don't think there's a hard and fast rule. It's going to be depend on the program, it's going to depend on what the agent is looking for.

For that reason I think that data minimization, again, on the back-end is not the answer. It has to be part of the framework. And collection limitation at the front-end is a crucial part of that framework.

MS. BRAND: Judge Wald.

MS. WALD: Whether or not you think that it's important to limit collection or you think perhaps you can wait a while or see and go after it more forcefully at the use end, I'm interested in what you think the role of the courts are.

In our other systems like criminal justice, ultimately, and even under the Fourth Amendment, the courts are kind of the final analysis. And even in many of our civil regulatory systems ultimately they come up.

So the question is two parts. At what stage, whether you believe in collection limitations or you believe more in use, do you think the internal, all of the internal audits and various other techniques that we've talked about are not enough, that you need some kind of an outside look at it?

But secondly, I think as a former judge I ask this question, if you were scared to come before -- and that is, do you really think that the limited role that the FISA court has been allowed to play in terms of the secrecy of its operations, and even with our recommendation and other people's suggestion about adding an adversary, and even some of the judges on that court, not only did they come out in different ways, all judges do, but they were frustrated themselves in terms of the technology sometimes.

Judge Bates remarked that it was practically impossible, given all of the complexity of the technology we've talked about and the fact that these judges would come in from their regular work for a week at a time and then go back again, is that the best kind of outside, not outside surveillance, outside look, an independent look, or is there some better way to get the notion of an independent, the Supreme Court always talks about independent and neutral?

It's a big question. Go at it, starting with Professor Cate, any way you want.

MR. CATE: Thank you very much, Judge Wald. I would say I think the role of the courts is absolutely essential. I think the important feature of that role is it needs to be an independent role, and I think one of the concerns with the FISC is that as this set of opinions went back and forth and, you know, small modifications, and updates, and briefings and corrections, it involved the court in the more daily operation of the agency than I think we would typically think appropriate or desirable, that we really want an independent, neutral and detached court.

The challenge of technology is huge for all of us. Even engineers have difficulty keeping up with the technology. I think there are, and we have seen some ways of dealing with it. One is court-appointed experts.

Another, as we saw in the Supreme Court's most recent privacy opinion this summer it cited heavily to amicus briefs from CDT, and from EPIC and others where they explained the technology and the impact of the technology, and the court clearly relied on them. And I think we shouldn't overlook that.

And then of course courts also have remarkable powers to compel the parties to explain the technologies in clear and understandable language and to not accept their filings or to not rule on their filings until they do.

So I could say more but let me share the microphone.

MR. GEIGER: I absolutely agree with everything Professor Cate just said. The courts play a very crucial role in the oversight of national security surveillance programs. I think that the court is constrained by a lot of statutory limitations.

I think we would welcome, at least the

privacy advocacy community would welcome court oversight of minimization procedures and on the ground controls on privacy.

I know the court does some of that, but I know that it is also limited to sometimes just a certification.

We have talked about having a special advocate. I don't necessarily view that person as an adversary because I think that in many cases the court and the government are also trying to protect privacy, they just maybe differ on the strength of that privacy protection. So I think that the special advocate could, in fact, be an ally.

But then also technical experts and amicus. One of the problems that we're seeing in the debate over bringing in amici or bringing in a special advocate is that there are some forces in the court, perhaps formerly of the court, who would like to see greater restriction placed on those parties, so that it is the FISA court that instead gets to decide what role and what access to information these amici will play, which will severely undercut their effectiveness and their ability to help the court. So I would urge resisting those calls.

MS. WALD: Don't you think, this is a follow-up just on the point you made, don't you think that in some cases, even the legal or even possibly constitutional reasonableness of something is dependent on understanding the technology of it?

I mean I think Judge Bates felt that way --

MR. GEIGER: Certainly.

MS. WALD: In one of the cases that was declassified and put out that way.

So you think that they are equipped to do that now, or do you think the advocate will fill that role, or do you need more?

MR. GEIGER: So I don't know enough about the judges to make a determination about their level of familiarity with technology.

But I mean this technology that is

being exploited in some of these instances can be extremely complicated, and so, no, I would not imagine that most lawyers have that sort of training and so I think that there -- I know that the court already has powers to some extent. I think those should be loosened to bring in technical experts as amici to explain this in as clear a manner as possible, because I think you're absolutely right, technology does have a direct bearing on the rights that are being manipulated.

MR. GRANT: And so I'll just jump off that one. I think that it's critical to have a translator role for the court, someone to help in an unbiased way try to explain the technology.

And you know, this isn't just an issue for the court, it's an issue for Congress. You know, I was trying to write cybersecurity legislation before I left and one of the challenges was you have to have a really complex technical debate and members are naturally going to be uncomfortable taking a strong stand when they're not a hundred percent sure what the technological considerations are. And the end result is you sort of paralyze things.

I think the critical question, so the court role is vital and it's important that it takes time because, you know, by nature that briefs out the issues and it helps you understand things.

The challenge is what are you doing in between. Because technology becomes ubiquitous even in a matter of months sometimes, and it starts to have a real effect on people's lives right away, and it's going to take 10, 15 years sometimes for the court to eventually settle on what they want to do.

So what do you do in the meantime and how should people be guided? Should there be ethical limitations on what the private sector wants to do? Should the government figure out ways to sort of slow walk in technology? And what's the framework for making that decision and implementing that? I think that's the real challenge.

MR. INGLIS: I largely agree with what's been said. I think that with respect to the role of the court neutral and detached is, I think, the right way with respect to their opinion on the efficacy of the policy or the government's representation. But they have to have a solid, if not exquisite understanding of the technology, and I would distinguish between the two.

I think the role of an adversary and a technology expert at the court, you know, has great merit and would, I think, add to their ability to at least understand the technology.

And we have to hedge our expectations, not because the government wouldn't want to reform, but at NSA could be perhaps exhaustive about technology at some moment in time in its presentation to the court, but at best it can only be illustrative as to where that technology is going to go. Nobody knows where the technology's going to go.

And the use of a certain technology,

even if the technology doesn't change, change is in and of itself. People make different use of technologies.

And so forecasting that is, I wouldn't say a fool's errand, but it's really hard.

MS. BRAND: Thank you. We have a couple of public questions. We may only have time to get to one of them.

But Professor Cate, I think this is directed at you. It says, if you don't like the FIPPs, what alternative do you suggest?

MR. CATE: So first of all, to be clear, I'm not saying I don't like the FIPPs, I just don't think the FIPPs are the be all and end all.

And second of all, I suggested risk management as a pretty useful tool as a way of identifying both potential negative impacts and also beneficial impacts.

And you know, one of the things we haven't talked about is the value of the use of data for national security or foreign intelligence gathering or whatever.

And one advantage of a risk management approach is it helps focus on both sides of that equation. It helps drive towards specificity. So if you ever want a documented decision that reflects that analysis, it's one way to help focus attention on it.

And then as we identify those potential harmful impacts, negative impacts, whatever we want to call them, we can then look for tools that help minimize those impacts.

So if the harmful impact is if you collect all this data it might be stolen, we can talk about security.

If we collect all this data and the fear is that the government might repurpose it for some other use, then we can talk about use limitations that would help address that.

But I think a great advantage of doing this is it makes clear in a way that the FIPPs do not, where should we be focusing our attention, whether we are academics, or the PCLOB or, you know, with the process within an agency.

MS. BRAND: Okay, thank you.

Mr. Chairman.

MR. MEDINE: Thanks again to the speakers on this panel and all the panels throughout the day, as well as the audience members who submitted questions.

I think we've had a remarkably informative and thoughtful discussion. We've heard from academics, government officials, advocates, technologists in industry, which is a lot, and we've covered a broad range of topics, FIPPs, Fourth Amendment, collection and use, encryption, de-identification, oversight, accountability, technology, mosaic theory and bulk data all in one day.

So you've given us a lot to chew on. I think this is very helpful for us as we consider how to move forward carrying out our mission to balance national security with privacy and civil liberties.

So unless any other Board members have any comments, today's Board activities are complete.

We encourage anyone who has comments, whether panelists, or members of the audience, or others to submit written comments. We're accepting comments on regulations.gov through the end of the year.

A transcript, again, of this day's activities will be posted on our website, pclob.gov.

And with that, I move to adjourn the hearing. All in favor of adjourning say aye.

(Vote taken.)

MR. MEDINE: We are adjourned. It is now 4:15. Thank you very much.

(Whereupon, the hearing was adjourned.)

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