THE BROOKINGS INSTITUTION
FALK AUDITORIUM

DEVELOPING THE NIST PRIVACY FRAMEWORK: HOW CAN A COLLABORATIVE PROCESS HELP MANAGE PRIVACY RISKS?

Washington, D.C.
Monday, September 24, 2018

Opening Remarks:

CAMERON KERRY
Ann R. and Andrew H. Tisch Distinguished
Visiting Fellow, Governance Studies
The Brookings Institution

The NIST Privacy Framework: The Road Ahead:

WALTER COPAN
Director, National Institute of Standards and Technology
U.S. Department of Commerce

Industry Principles for Privacy Risk Management:

DEAN C. GARFIELD
President and Chief Executive Officer
Information Technology Industry Council

What Does Risk Management Mean in the Context of Privacy?:

CAMERON KERRY, Moderator
Ann R. and Andrew H. Tisch Distinguished
Visiting Fellow, Governance Studies
The Brookings Institution

TRAVIS HALL
Telecommunications Policy Analyst, National
Telecommunications and Information Administration
U.S. Department of Commerce

DAVID HOFFMAN
Director of Security Policy and Global Privacy Officer
Intel Corporation

PETER LEFKOWITZ
Chief Privacy and Digital Risk Officer
Citrix Systems

HARRIET PEARSON
Partner, Hogan Lovells US LLP

MICHELLE RICHARDSON
Director of the Privacy and Data Project
Center for Democracy and Technology

What Are the Practices and Tools That Can Inform a Privacy Framework?:

NAOMI LEFKOVITZ, Moderator
Senior Privacy Policy Advisor, National Institute of Standards and Technology
U.S. Department of Commerce

JENN BEHRENS
Partner and Executive Vice President of Policy
KUMA LLC

KEVIN GAY
Chief of Intelligence Transportation Systems
Policy, Architecture, and Knowledge Transfer, Federal Highway Administration
U.S. Department of Transportation

HARLEY GEIGER
Director of Public Policy
Rapid7

ZOE STRICKLAND
Managing Director and Global Chief Privacy Officer
JP Morgan Chase

JOHN VERDI
Vice President of Policy
Future of Privacy Forum

* * * * *

P R O C E E D I N G S

MR. KERRY: Good morning and welcome, everybody. I'm Cameron Kerry. I'm the Ann R. and Andrew H. Tisch distinguished visiting fellow here at the Brookings Institution. I want to welcome all of you here to Brookings. Welcome those of you who are participating in the webcast this morning. And as you see, we can Tweet or otherwise communicate about this with the hashtag #PrivacyFramework.

And this is certainly a timely discussion this morning. We are in the middle of a time of ferment in privacy policy. Most of you probably saw the headline in Politico the week before last, "The Invasion of the Privacy Principles," as many different organizations in town are working on privacy policy and they're looking ahead to the prospect of legislation. Tomorrow the Senate Commerce Committee begins what is apparently the first of a series of hearings. Other committees, other members of Congress are at work on bills in one way or another. So that's really the setting for our discussion this morning.

As a former Commerce Department official, I am certainly pleased that the Commerce Department, NIST, and NTIA is playing a leadership role in the Executive Branch discussions of these issues and I hope, in some respects, building on work that we did in the prior administration when I was there. But certainly the times have changed both in terms of the issues and I think the intensity of focus.

And I'm certainly pleased to have the NIST framework as a focus of this discussion today. I believe that NIST is one of the great unsung stories of the federal government. Every time I said I had to work on an issue, NIST had some piece of it. It counts four Nobel Prize winning scientists among its staff and is no stranger to the issue of privacy. For more than 15 years, NIST has put out the 853 Series of documents that prescribes privacy standards and practices for federal agencies. And when we set out to

rebuild the privacy program in the Commerce Department, our internal privacy program, turned to NIST for an acting chief privacy officer.

And, of course, the cybersecurity framework includes privacy elements. Naomi Lefkovitz, who will moderate our second panel, was the key leader.

So today's program is going to explore the applicability of that sort of framework approach to privacy. We'll have discussions of those issues, how we do that, some of the practices involved. Among the panels we'll have opportunities for questions.

I do want to acknowledge the support of two of the organizations that are represented on our panel: JPMorgan and Intel Corporation. We welcome their support. Brookings' choice of speakers is independent of that sponsorship. In fact, I didn't know that they were sponsors until I was told I had to do a disclosure statement because they were on the panel. (Laughter)

So before we have the panel discussions, we will hear both about the developing framework and a framework being developed by ITIC. So we will begin with Walter Copan, the NIST director and undersecretary of Commerce, as well. He is a scientist, a chemist; spent a long career in research and development in tech transfer and commercialization issues, both at national labs at the Energy Department and in the private sector; and served on government advisory committees, as well.

So please welcome Director and Undersecretary Walter Copan. (Applause)

MR. COPAN: Thank you so much, Cameron, and thank you all. I'm honored to be with you today to discuss what we all recognize is a pivotal issue for our time. For two decades now, the Internet has been a job-creating, economy-growing, consumer convenience bonanza, and it has changed business, democratized information access, and transformed how we interact as human beings. The Internet, mobility,

computing, global positioning, communications technologies have driven unprecedented innovation and economic value in the United States and around the world.

Companies that are now major forces in these fields and with substantial market capitalizations to match did not even exist two decades ago. Internet applications permeated every aspect of our lives and surveys in the last few years show that Americans collectively check their mobile phone 8 million times a day -- 8 billion times a day. Amazing.

Which brings me to today's dilemma: how do we maintain the clear societal benefits from the Internet and from the emerging technologies like the Internet of Things, artificial intelligence, and quantum computing without jeopardizing our privacy and security? It's boiled to two words, an appropriate answer might be: it's complicated.

That's also the impression that most consumers have when they actually try to read the Terms of Use of their privacy agreements, when they try to have the decisions made when companies ask them to do so. They click to accept the terms. What will it mean? What risks might they encounter? And what are the unintended consequences?

Indeed, finding ways to continue improving with the Internet while simultaneously protecting privacy is difficult and complicated, but it is just as clearly necessary. An approach to protect privacy is to develop and implement more regulation.

The European Union implemented its General Data Protection Regulation, or GDPR, and it came out in May of this year. The text includes 11 chapters, 99 articles, and more than 170 recitals, or "whereas" clauses, that explain why a particular provision is needed. The new GDPR requirements were described by the *New York Times* as bringing sweeping changes to how companies operate online.

We've also seen how some of our largest companies have struggled and

they deal with these struggles publicly. The concerns about privacy and data use have dramatically affected stock prices and other financial performance measures, as well as reputations. And now California's taken up the issue and issued a new privacy law this summer. And across the nation and around the world we see a developing patchwork of regulations. It's driven by good intentions and with a goal to properly consider ethics. It is also an unsustainable model.

It's too soon to tell how large an impact these regulations will ultimately have on the products and services that rely on access to users' data and whether there'll be substantial, measurable improvement in desired privacy outcomes. At a minimum, the new EU regulations have spawned a rash of privacy policy messages in consumers' inboxes. And it's reminding consumers that free Internet software is typically paid for by access to personal data. Big data has big value.

It also made companies worry that mistakes in implementing privacy protections could be very costly to them. Under the GDPR, companies can be fined up to 4 percent of their global revenues, which for some multinational corporations could amount to many millions of dollars.

The Trump administration's committed to helping U.S. companies find practical privacy solutions that support both innovation and strong privacy protections. My agency, the National Institute of Standards and Technology, is part of the U.S. Department of Commerce. NIST has announced a collaborative process to create a privacy framework; hence our meeting today. We envision this as an enterprise-level guide that companies and other organizations can use to manage privacy risks. In parallel with our effort, the other two Commerce agencies, the National Telecommunications and Information Administration and the International Trade Administration, are creating domestic policy approaches for protecting privacy that

ensures consistency with international policy needs.

For those of you who may not be so familiar with NIST, we trace our heritage to 1787, Article I of the U.S. Constitution. Later in that same Article is the language that created the U.S. Patent and Trademark Office, also part of the Department of Commerce. We were reconstituted in 1901 as the National Bureau of Standards. And to better reflect our broad scope we were renamed the National Institute of Standards and Technology in 1988.

NIST has a reputation for integrity, for the highest level of science and technology excellence, for being unbiased, transparent, collaborative, and honest. NIST is a non-regulatory institute. We're often called industry's national lab.

We specialize in measurement science and research in partnership with the private sector and we support all of U.S. industry, from legacy technologies to emerging high-tech industries. Computers, aerospace, 3D printing, telecom, medical diagnostics, advanced materials, cybersecurity, chemicals, bioscience, quantum-based technologies, NIST is right in there. Name any market sector that's emerged over the last century and it's likely that NIST was part of its development and certainly helped improve its products and services through better measurement science, through standards, engineering, and accurate performance data.

NIST is also the National Metrology Institute of the United States, and we support development of measures and standards internationally on behalf of the nation, as well as for fair trade. We work with each state and territory of the Union to ensure that we have trusted systems of measures so that no matter where you go to pump fuel that you can be sure that the right amount is dispensed. You can rely upon the accuracy of your electric meter connected to the grid. And so you can understand that there's an accurate measurement system for the ride-hailing apps that you use, perhaps even to get

here today, so that you'll be charged fairly for your trip.

So we are the federal agency tapped also in the President's Management Agenda to improve the process of moving technology from laboratory to market, from federally funded R&D to commercial application. And so, in fact, NIST is the only science and technical federal laboratory that is explicitly charged with fostering innovation to help industry create jobs and to grow the economy. So we're always looking for ways to help American companies improve their products and services to enhance competitiveness and to create useful standards together.

I mention this as background because it may not be obvious why NIST has taken up this challenge, the privacy framework initiative. Through the lens of the S&T community, and as Cam mentioned before, we are a respected, Nobel Prize winning, world-class research organization that regularly announces groundbreaking research results, as well as discoveries for advanced manufacturing. But over the last decades NIST has been increasingly called upon to use its deep technical expertise and strong relationships with industry to find common ground and to help disentangle seemingly intractable issues.

For example, on August 14, 2003, a cascade of electrical grid failures caused some 55 million people to lose power in eight Northeastern states and in Southeast Canada. Investigations found that both human error and equipment failures had caused the event. Today, both new standards and new regulations adopted since then have lowered the risk dramatically that a similar blackout could happen again. NIST's role in this achievement, beginning in 2007, was to assemble all of the relevant stakeholders from equipment makers to state regulators and to create a framework to achieve improved interoperability of the electric power grid, the so-called smart grid devices and systems.

Now, 10 years later, more than 70 industry standards have been put in place with NIST leadership and with NIST support that now substantially lower the risk of blackouts. At the same time, these consensus standards make it possible for renewable energy sources, such as wind and solar, to be effectively integrated into the grid.

And yet, even with something as seemingly straightforward as electricity distribution, privacy was a big issue. Some stakeholder groups and communities objected to the use of smart meters. They were concerned that patterns of electricity use could reveal private behaviors inside homes and other buildings.

Of course, an even more direct relevant example to our topic today is NIST's work on the cybersecurity framework. There's that word again. The NIST cybersecurity framework was first issued in draft form in 2013. The project came about because of recognized concerns with the vulnerability of the nation's critical infrastructure, things like the electric grid, water companies, telecommunications, et cetera. And at that time there was a disconnect between the acknowledged need for stronger, more comprehensive cybersecurity protections and the actual implementation of such efforts, just as at this time for this discussion there's currently a disconnect between the acknowledged need for better agreement and a shared vision for strong privacy protections and agreed methods for achieving such a vision.

In 2013, the headlines focused on cybersecurity breaches, where consumers' credit card information, Social Security numbers, and other sensitive, personally identifiable data had been hacked, even from large corporations or federal agencies. The threat of identity theft had long been recognized by the public, but the frequency of these breaches reached a critical point in 2015.

Then a regular survey by the Census Bureau and by the NTIA found that 63 percent of online households were specifically concerned about identity theft. And

perhaps even more important in 2015 was the chilling economic effect from worries about IT theft. Forty-five percent of online households responding to the survey said concerns about cybersecurity risks stopped them from conducting financial transactions, buying goods and services, posting to social media, or expressing their opinions online.

Now, NIST has had success in creating, disseminating, updating, and evaluating the cybersecurity framework for use by organizations of all kinds, and it has made a positive impact for our security. It has also been adopted as a standard by other countries.

Our current project to create a new privacy framework is based on our experience, proven process, and success with the cybersecurity framework and the other frameworks that came before it. In case you're not familiar with the cybersecurity framework, just a brief description of Version 1.1, the current one. It is voluntary. It's created collaboratively with expert input from across private and public sectors. It can be used by any size or any type of organization help manage cybersecurity risks.

It's written in English, and by that I mean it's understandable for everybody from CEOs and entrepreneurs to the geekiest cybersecurity expert. It breaks cybersecurity risk management into five buckets for easier decision-making and prioritization: identify, protect, detect, respond, and recover.

It's a guide and not a one-size-fits-all prescription. It gives options to companies to consider and is backed up with best practices and documented solutions to implement depending on the specific threats facts by your organization, carrying out your mission with your resources.

It focuses on desired outcomes. It provides a common language and definition so that suppliers can better align cybersecurity choices to customers' needs; so that people within an organization can hold one another accountable; and that

organizations can better communicate to any stakeholder, including international customers and governments, how they manage risks.

And finally, it turns out today's best practices and it transforms them into common practice through periodic updates. And it is not a magic bullet, but it's driven by what our scientists call a feedback loop.

It was originally created by soliciting feedback from thousands of stakeholders from industry, academia, government from U.S. and internationally. And that document is now revised to meet the new realities in the marketplace and to incorporate new cybersecurity approaches.

Many organizations from government to multinational corporations to small businesses have successfully improved their cybersecurity posture by using that framework. By 2015, a Gartner study found the NIST cybersecurity framework was being used by more than 30 percent of the U.S. organization surveyed and it was expected to reach more than 50 percent by 2020.

Which brings us back to this morning's topic, a privacy framework. If we have a strong cybersecurity framework, do we even need a privacy one? Yes, we do.

Strong cybersecurity is a prerequisite for managing privacy risks, but it is not sufficient. Privacy risks also arise from how organizations collect, store, use, and share information, as well as from how people interact with the products and services. We need a different set of considerations to manage cybersecurity and privacy risks appropriately.

So if you accept that a separate privacy framework is needed, then which elements of the cybersecurity framework plan should we consider in developing the new framework? All of them.

We believe the new privacy framework should be voluntary, adaptable

for use by any organization as an enterprise-wide tool. It should be understandable and implementable from the C-Suite to IT experts to privacy advocates. It should provide a common language and inform privacy risk management decisions. It should be focused on outcomes tailored to an individual organization's needs. And it should also help organizations meet privacy obligations here and abroad.

The intent of this new framework is to increase the effectiveness of privacy protections by enabling conscious, well-considered choices that are made by organizations based on their customer needs, that are clearly communicated and understood. The new framework is further intended to enable innovation through technology solutions with privacy protections engineered in. The ultimate purpose of this effort is improved trust between businesses and their customers, between organizations and the public.

Right now there are many different perspectives on what strong privacy protection will look like or what that even means. It's difficult to communicate quickly within and between organizations clearly about privacy risks. The conversation is complex, conducted in legalese sometimes more often than in English it seems, and it's confusing even to experts. So what's missing is a shared lexicon and a practical structure that builds, that brings all parties together, and is flexible enough to address diverse policy and privacy needs.

For the rest of this morning's session we'll be hearing about the details and the challenges ahead in achieving what's a deceptively simple goal: better privacy based on addressing actual risks in a way that supports continued innovation. As the cliché goes, it's a tough job, but somebody's got to do it. And we at NIST thrive on challenges and we hope that you all do, too, because we will need everyone's help to be successful in addressing this challenge.

Today's discussion is just a beginning. We'll be quickly following this up with another public workshop to gather more feedback in Austin, Texas, on October 16th. There will be many more opportunities to share your good ideas, recommendations, as well as concerns in this journey. And over the coming year, we will offer multiple opportunities for input and to contribute to drafts of the privacy framework to help improve it.

The bottom line is that we want the U.S. to lead the way to a privacy future that maximizes privacy protections, innovation, and trust. We are looking forward to working with all of you to get there. Thank you so much. (Applause)

MR. KERRY: So Director Copan, thank you. Thank you very much for that introduction to the framework.

Now we want to turn to Dean Garfield of the Information Technology Industry Council, which I mentioned earlier. Brookings just celebrated, a year or two, its 100th anniversary. And I had not known until preparing for this event that ITIC has been around in some form for at least as long as that, beginning as the National Association of Office Appliance Manufacturers, something that gives a little bit of a Commerce Department connection because IBM was founded by a former Census Department employee, Herman Hollerith, who designed a machine to replace what the humans, who were called calculators, spent years crunching the data from the Census. So I've certainly been aware of ITIC's presence in technology policy, but not of that history.

And Dean Garfield has been a leader in technology issues and IP issues for many years, first at the Recording Industry Association and the Motion Picture Association, and president of ITIC since 2009. And really has given that organization today global reach.

So, Dean, welcome back to Brookings. We look forward to your

comments. (Applause)

MR. GARFIELD: Hopefully I've held up well for being 100 years old. (Laughter) Let me begin by thanking Cam and the team at Brookings for putting together this dynamic event, thanking Dr. Copan and the team at NIST for all of the great that they're doing. I'm attempted to simply associate myself with Dr. Copan's remarks and sit down, but I think there would be some folks, at least on my team, who would be disappointed if I did that, so let me endeavor to do two things. One is to speak to the imperative to act first, and then second what I think we should do.

In many respects the imperative to act is driven by us, the manifestations of our imagination that are the transformative technologies that are carrying the day. As we think about context for this conversation, it's important to have it be grounded in what's going on. And it is my firm view that what's going on is truly awesome.

We are, in fact, I think it will be as significant as hominoids going upright and walking out of Africa 200,000 years ago or homo sapiens becoming the dominant species on Earth 13,000 years ago. The integration of the cyber and the physical, the convergence of physical, cognitive, biosciences is leading to innovations, like CRISPR where human beings have the ability to code and to change DNA and genome in the same way that we code software.

It's leading to artificial or natural intelligence that will lead us to cure diseases that we previously thought were incurable or to just lead to safer streets. I notice that DOT will be speaking on one of the panels later.

It is leading to quantum computing where we'll be able to take on the most complex computational challenges that may ultimately sustain our planet. We are truly living in awesome times.

It is that integration that is the context for this conversation and that leads

Dr. Copan to say it is really complex. The connective tissue among all of those things are human beings and data, and protecting the individual rights as well as the broader societal issues that are at play.

As human beings it is our instinct to draw parallels to what we know as we deal with really complex challenges. And so in the context of data or instinct it's to revert back to what we know and set rules based on that. Whether it's land or the modes of production, how often have you heard the comparison of data to oil? And while it isn't true that data will likely be the engine of economic growth for our generation, it is not oil.

It is a renewable resource. It is both here, everywhere, and nowhere. My ownership or access to data doesn't dispossess you of that data, as well. Nonetheless, governments, as Dr. Copan noted, around the world are racing to cabin it, to control it, to own it, and to set up rules that align with what we know. From Brasilia to Beijing to Bombay, from South Africa to South Korea, even in the small island that I came from, Jamaica, they're moving ahead with rules around data trust and privacy.

Thomas Jefferson spoke to the imperative well when over 200 years ago he noted that our Constitution and laws should not change with the wind. But our laws and institutions must go hand-in-hand with the transformation of the human mind. And so as we discover new truths, it is important that our laws and institutions change to reflect those new truths. And we are in a period of new truths, and so our laws and institutions must change to reflect that, as well.

And so what should we do? We should do what Dr. Copan said. (Laughter) From our perspective, and Cam noted the oversaturation of principles, our organization is not working on a set of principles. We are working hard to develop a framework that avoids fragmentation and advances interoperability and that helps the U.S. Government and, hopefully, the world to work through these complex issues. And

that is ultimately what we think is needed here, which is an interoperable framework law in the United States that builds on what existed before, but adds based on context.

And fortunately, there is much to build on. As Dr. Copan noted and I'm sure we'll discuss in the panel, there's GDPR, but there's also CBPR and laws in a number of other nations.

There is constructive criticism or critique that can be offered to GDPR, but there are as much that GDPR also got right. It's really difficult to be first and so they deserve a lot of credit for being first in giving us data that can, in fact, inform what we do.

GDPR is founded on an initial principle, which is the idea of protecting individuals and individual rights. That is something that we should incorporate in what we do in United States and figure out how we give meaning and manifest that through advancing controls that enable consumers to make choice, that enable consumers to have access to be able to delete, correct, or port data.

GDPR is also founded on principles that we should all support, the idea that the usage of data should be purposeful, fair, and transparent are one that I think are included in all of the principles that have been released and should be integrated in whatever law is advanced here in the United States.

GDPR recognizes that choice is not the sine qua non, not the seminal construct or consideration in thinking through the relationship between an individual and another, between a business and another, or an individual and a business. And that context is critically important. Those are considerations that should also be integrated in whatever we develop here in the United States.

CBPR advances the art, as well, in recognizing the international nature of data today and the importance of data portability. Whatever we do here in the United States should incorporate that thinking, as well.

But as Dr. Copan noted, there is important work that's being done here that we can build on and extend, as well, that may be uniquely American, but are principles that would benefit the world given the context in which we're currently operating. The idea of being explicit in considering all of the equities involved in the ecosystem is something that GDPR does not do that we would encourage in any legislation that's advanced here in the United States.

The idea of leveraging technology to actually advance the consideration of privacy and the consideration of advancing trust is something that is not fully integrated in GDPR and that should be, particularly as we consider the definitions of personal data. The ability of technology to anonymize or pseudonymize and otherwise protect should be a part of the consideration as we think about the foundational definitions.

The societal benefits from all of the innovations I mentioned at the beginning and the importance of research is something that is not as fully integrated in GDPR as it should. And so in the United States there's the opportunity to do that.

The idea that privacy risk assessment should be a continual process and not a check-the-box exercise focused solely on certain categories of data is a consideration that for some reason was left out of GDPR, and so we think is worthy of consideration here in the United States, as well.

And finally, the idea that science and standards should be a foundation of the consideration around data, privacy, and building trust, in our view, should be a part of the consideration here. And it's exciting to see that that is something that is moving ahead even in advance of legislation advancing in the United States.

Any of you that have paid attention to the guidance process in Europe as a result of GDPR and the quantum nature of -- that's supposed to be funny. (Laughter) Maybe I should have used the word "interesting" as a way of conveying the thoughts; has

not been grounded in standards or science.

Dr. Copan noted the cybersecurity framework in the United States and the processes and implementation there that, in fact, was grounded in standards and science and did something that was critically important and, hopefully, will be a model for the approach that we take here, as well. The idea that whatever we do should pull together both the public and private sector should be advanced in a fashion that is adaptable so that we are not choosing winners and losers through legislation or regulation. The idea that rather than, which I thought was a stroke of genius, rather than focusing exclusively on U.S. standards, but looking globally to identify best practices from around the world that would have broad applicability in mitigating risk has helped the cybersecurity framework to be particularly impactful around the world, as Dr. Copan noted.

And so the imperative to act is, I think, clear and hopefully a little bit clearer as a result of our conversation and certainly hopefully by the end of the day. What we should do I suspect even after this conversation will continue to be cloudy, but over time I hope will achieve clarity.

We were noting in the conversation before coming in here that we've been talking about data security, privacy, trust for a long time. And it seems the time has finally arrived through the good work of NIST and NTIA -- Travis is smiling; we're all counting on you, brother (Laughter) -- to move the ball forward in a significant way.

The thing that is encouraging to us and to me and the nearly 70 companies that are members of ITI is the growing recognition that these are not technical or technological issues. These are all of society issues. The only way that we will get it right, so to speak, is by all of us as human beings recognizing the context, engaging, and marching forward together.

And so I very much look forward to working with and collaborating with all of you as we develop a framework in the United States that's workable globally and that helps us to achieve what we all aspire to for humanity. Thank you very much. (Applause)

MR. KERRY: Good. I've got everybody ready. Dean, thank you; for your very thoughtful discussion about what goes into a framework. Walter Copan talked about developing a framework that's, among other things, voluntary, adaptable, based on standards, implementable.

Those are things that the Cyber Security Framework succeeded beyond our expectations when we started down that road five years ago. Dean talked about some of the -- and Walter as well -- some of the international acceptance that that's gotten, and wide implementation across a number of sectors, a number of types of companies.

And referred to something that was, I think very much a key focus as we set out to do this, I remember talking with Walter's predecessor, we didn't want this to be a check list approach. This panel is going to take the question: can we replicate this with privacy?

You know, a somewhat different and perhaps more value-laden subject than cyber security, we have got, I think a terrific panel to talk about that, even though one of our aircrafts is missing.

So, on my left we have David Hoffman, who is the Chief Privacy Officer and Global Security Chief for Intel; and next to him, Travis Hall from National Telecommunications and Information Administration of the Department of Commerce; next to him Harriet Pearson, currently leads the Privacy Practice at the Global Firm of Hogan Lovells, and formerly the Chief Privacy Officer at IBM, and a Founding Member of

the International Association of Privacy Professionals; and then finally, Michelle Richardson, next to her, is the -- she's got a new title -- at the Standard for Democracy and Technology, Director of the Privacy and Data Project, has worked at CDT on surveillance issues and security, worked on those issues at the SLU, and the House Judiciary Committee as well.

And then missing, but apparently on his way from Boston, and several flights have been cancelled and delayed this morning, is Peter Lefkowitz, the Chief Privacy Officer and Digital Risk Officer, at Citrix, and formerly Chief Privacy Officer at General Electric, who has both industrial and technology experience.

And we have great privacy leadership here, and both from the government and civil society sector, and from the private sector, Harriet, David Hoffman, Peter Lefkowitz, have all been important parts of the leadership of the International Association of Privacy Professionals.

I want to start with Travis, give us a little bit of context here. So, you're at NTAA, NTAA has got a process unfolding as part of the administration's process here. How do these things fit together?

MR. HALL: Absolutely. Thank you so much, Cam. And thanks everyone for having us here. I'm really looking forward to the discussion. So, for those of you who don't know us, the National Telecommunications and Information Administration hasn't been around quite as long as NIST. We are actually celebrating our 40th Birthday this year, which is exciting. But we are the President's primary advisor on telecommunications policy, in addition to work on spectrum and broadband.

And we have traditionally been very heavily involved in these types of policy issues, in the previous administrations, both privacy and cyber security on the policy side. And that is kind of how we are moving as well, in terms of where our work

works alongside NIST's work.

And where the National Economic Council kicked off both of these processes a couple of months ago, tasking NTIA with developing a set of principles for the administration on consumer privacy, and NIST to begin its work on the Privacy Framework.

I have heard that there's some confusion between the two, how they play together. The way to think about it, we are looking at what the policies are, like, for the United States. How do we actually move forward to actually kind of structure and potentially do something different in terms of U.S. consumer privacy policy?

Whereas, NIST is working on a set of tools to actually do risk management, and those tools don't really care if you're talking about just the U.S., of if you're talking about trying to comply with different parts of GDPR, or if you just simply are a company that wants to actually do something a little bit better, something a little bit different to match your own particular privacy policies.

I've been very, very fortunate to have worked very closely with my colleagues at NIST, particularly Naomi Lefkovitz, as well as in the International Trade Administration, and I've learned quite a bit in the process, and one thing that we do have in common with the two approaches where these are two separate processes doing two different things, but we are working very hard to sing in harmony, is with the risk management approach.

For what we are doing, and let me talk in just a second about what we are doing. We are looking towards risk-based, outcome-based approaches that could be done through tools that NIST is developing. So that is like how the two play together.

And I think it is important, you know, Dean brought up the analogy of oil, that is oil before, and it's one that's been trotted out a lot, usually in terms of like,

everybody wants to collect it, and wants to use it for great economic gain, and that's true. It's also leaky and potentially toxic.

So, its use is great, but you have to think about the risks of its use. And different types of use, and different types of flow, right, oil also flows, right? Different types of flow carry different risks, and as such you need to have different types of controls, and different types of friction about its use, and so you have to be more thoughtful about its use, the riskier the use of both data and oil.

And so that is something that NIST is developing tools for, we are talking developing kind of overarching incentive structures for, and what we are doing is, in terms of our initial tasking, was to develop a sort of principles, we are actually taking something of a step back, but I think in the longer term, a step forward.

We are developing a -- we are going to be putting put a request for comment, that puts forward a straw man approach that has two parts to it. The first is a set of, we are calling outcomes, you don't have to squint very hard, you'll see the FIPPs, the Fair Information Practice Principles in them, that's basically saying: what should consumers expect as a result from the system?

Why we are not using principles and we are talking about outcomes, we are trying to push away from, you know, talking before about conversations about compliance checklist, or legal font sizes, and more towards: how do you actually get better results for consumers without mandating the path there?

The second is a set of high-level goals for Federal action like: what are some next steps, and what are some high-level ideas of how we actually get to those results?

It's going to be very, very high-level, and I use the straw man, it's not going to be in the request for comment, but that's what it is. We are truly asking for a

comment on how to achieve these goals, and how to move forward together. And that will be coming out very shortly.

Again, we've been working very closely with NIST, although they're two separate processes looking at two different aspects of the coin.

MR. KERRY: Great. Thank you. So, David, Intel is all over the cyber security framework process, I remember the Cyber Security Summit where President Obama went out to Stanford on the First Anniversary of that framework; Intel presented a key case study on how it had implemented the framework. Based on that experience, how do you see that process, that experience mapping on to privacy?

MR. HOFFMAN: Thanks, Cam; and absolutely. First, let me thank you for inviting us to speak here, and for holding this. I think it's in an absolutely critical conversation. You asked in your original opening: can we create a similar framework? I think that's an open question of whether we can? Should we? I don't think that's an open question, we definitely should.

Will we? I'm not sure. And I think that's what we need to evolve here. We, Intel was fully committed to the Cyber Security Framework, we saw it as the perfect approach to play a role to help make progress on cyber security, and there were several elements of that that we thought were fundamentally important.

And Dean and Walter both touched on some of them in their remarks. I thought the most important piece of it, was the interoperable nature of the framework. We have an interoperable global digital infrastructure. We need to make sure that whatever approaches that we take promote our ability as individuals and as companies to use that interoperable, global infrastructure in a way to promote international data transfer.

I'm actually not a big fan of the data is oil analogy, because I think of oil

as sort of naturally toxic, and something that the world is actually trying to move away from using. As Dean pointed out, we want to move towards the use of data. Data has got huge potential, particularly in the area of artificial intelligence, and what we are going to be able to do for humanity, if we can describe how in inoperable way, and globally use that data productively.

If we are going to train artificial intelligence algorithms to really provide us with benefit, we need diverse data that comes from all different places in the globe. How are we going to drive that? We are going to need a voluntary, flexible, interoperable framework to be able to talk for, and to teach organizations on how they are going to handle data.

What was, I thought, so important, was a true innovation in a way that the Cyber Security Framework created its basis, was that it created a situation where we, as Intel, who've got vendors that we work with all over the world, we could do our own analysis under the Cyber Security Framework to understand our risks, but we actually then took a step forward, and one of our former employees who is in the room, John Miller, who actually led this work, driving it into our procurement guidelines, that we would actually have -- that required all of our vendors to look to it as a guide for them doing their own analysis.

That wasn't just the U.S. approach that was a global approach towards procurement. This is exactly the same kind of thing that we need to promote the innovative and ethical use of data, and if we are going to do that, and we are going to keep it flexible, the way we do that is focusing our risks.

So, I think once again: can we do it? As Walter said, it's going to be hard, it's going to be complicated, but we definitely should try.

MR. KERRY: I have a follow-up question, but I'm going to put it to

Harriet instead. I mean, you said, can we? What are the challenges in doing that? So, Harriet, you were very involved in the privacy aspects of the Cybersecurity Framework, and I think a critic of some of that approach, or a skeptic, maybe, is a better way to put it. Let me explore that a little bit. What made you skeptical there? Does that carry over here? You know, can we?

MS. PEARSON: Maybe the better way to characterize it is, and I'm speaking only on my own behalf, I should say -- is that we start at skeptics, and turned into believers in the approach used, and the current Cybersecurity Framework, starting with Version 1.0 and 1.1, on privacy, and it's a success story in many ways, how the privacy issues were addressed and are addressed in a Cybersecurity Framework.

And there are some common attributes there, some lessons to be learned from the process, that NIST so ably ran a few years ago to develop the Cybersecurity Framework, which is widely acknowledged, has been, and is being very influential in how to address how organizations address cyber security risks.

The skeptic part started with I think, as all important and first-mover initiatives do, you take a first step, and you put something out and people pile up all over it, right. And they say, oh, well, there's something, right? And we are all in the process, the policy process. Business is just the same thing, you put something forward and so it attracts skeptics and critics. And guilty as charged; I have my share of moments, and both on the receiving end as well as on the giving end.

Yeah, skeptical a little bit to say, wait a minute, this draft, and the first drafts, you know, the first draft of the privacy section in this framework was full of value judgments that attempted to, you know, try to do a good thing, but really went too far to details, to out of what NIST would typically be expected to do. And over time, in a group of organizations brought privacy expertise to the development of a Cybersecurity

Framework, which was one of the learnings, right?

You can't have cyber-focused technologists or engineers, or process folks develop without privacy experts, right, so we came back and developed all sorts of inputs to the Privacy Framework, and it evolved to a pretty good place I think.

And what characterized it? One, is that it was used for all industries, it wasn't trying to be something to only one industry, and so that was from the start the intention, it became that way. Drawing input from all kinds of experts, including experts who are particularly suited to provide that input, but balanced with other stakeholders. So, I think that's the strength of a collaborative, consultative process.

So, I'm glad to hear from the Director, that that is indeed what's planned for this initiative.

Recognize the need to keep it simple. You know, if you're going to be implementing cyber security activities in an organization, you're not going to solve for privacy world hunger. You're going to try to create privacy-related actions that are the ones that could be predictably, reasonably predictably kicked off by actions that are needed to secure an organization.

So, if you're going to need to monitor systems, or collect data, and maybe share it with other organizations, you probably ought to have some activities that relate to being careful about processes used to share information, or being mindful of the privacy issues related to monitoring systems and have a process for considering that.

And outcomes-based was where the Privacy Framework landed, which is, it wasn't -- you know, we've minimized data, that wasn't ultimately what was in the Privacy Framework, because actually how do you assess that you've done that? What's the measure?

You know, maybe in years from now, I don't know when, we'll have a

way of assessing that, but at this point, we assess things like: has privacy actually been taking into consideration the process of building out a risk -- building out a monitoring program? Or is privacy an active part of considering how we share information for cyber security purposes?

Those kinds of things in 2018, we can actually assess whether an organization has done those. And that I think, fundamentally, is part of the reason the privacy part has done its part to be part of the model here for how we use the framework.

And I think if you look at the Privacy Framework, and can we do it? Is privacy a risk that can be managed? Well, we'll have a consultative process, and the devil will be in the details, but everything about what I've learned, doing privacy, and counseling on privacy, and making privacy operational inside organizations over 20-plus years, says, yes, we can, but the devil will be in the detail.

And some of those issues are going to be: what is a privacy risk? Or, privacy as it's used in the NIST work to date: what is the privacy problem, and how do we define it? And what is the scope or the boundary of a system where we are actually going to look at that risk?

Is it the boundaries of a single company, an ecosystem? What does that boundary look like, and how do we use that? What is the kind of information that should be part of a privacy risk process?

Is it, what is personally identifiable information? That definition is undergoing some evolving I think, and that's where NIST can't answer that question, really, it has to be answered -- it's a value-infused question maybe in part. And so that's where perhaps, you know, NTIA might help, or maybe some baseline -- all sorts of things, there are lots of sources for how we answer that question, and then, you know, fundamentally: what's the process we use to get there?

And is it going to be reflective of the stakeholders, from civil society to business, and recognize the fact that there are of course, benefits or positive trending risks, as risk management personnel or, you know, experts would call them, in addition to the risks that colloquially we think of, which is there's a bad think that could happen, of course, to privacy if you mismanage data, but there are many, many positives as well.

So, both factor in to how risk management is done in organizations as a discipline, as a capability, and it's used widely. So, why not here?

MR. KERRY: So, Michelle, Center for Democracy Technology is one of the institutions that has been engaged in discussions about what legislation could look like, and talking with other organizations, with privacy advocates, with academics as well as with companies. You know, from your standpoint, what can a Privacy Framework like in this framework accomplish to protect privacy?

MS. RICHARDSON: Thanks, Cam. I think the framework that we're discussing now has a different goal than the underlying legislation that people on The Hill are thinking about. And so it has a very unique value, and it should be a double track here.

We were very complementary of the Cybersecurity Framework, and civil society participated in that process, and we are largely happy with the outcomes. And so we would like to recreate something like that for privacy.

We have to admit that privacy is controversial, right, and the cyber security frame, the company and the users' interests more closely align. And we've set up a business model for some companies, where they are antagonistic, when it comes to privacy.

So what does it look like there? I would say the potential here lies in making systemic changes to the way we handle data. I see a lot of the conversation we

are also having around privacy, focus on user control, pushing everything back on the individual user to manage dozens if not hundreds of apps and applications and connections for information that they may not understand.

But this framework would put it back on the people who are collecting, using engineering systems to make systemic change. And that is very different than the other models that we are hearing about.

I also like that the framework will move us away from edge cases, I feel like we are very quickly in a what-about game. While when we talk about, well, let's put some limits on how this data is collected and used. We get the what-abouts of security, rocket science, solving brain cancer, we talk about basically everything but the central collection and use of data that happens every day, purely legal, the things we are actually signing up for.

And so this is exciting to push us back into discussing that, right. Our concerns that I would say, we have to be very careful about the definition of harm, the whole system is going to ride on whether you believe there is harm beyond economic loss.

And this is where we hope to draw on the great work that NIST has already with their NISTIR 8062, being really thoughtful about things like loss of autonomy, loss of trust, discrimination as harms, that should go into the matrix.

And finally, I think the difference between a framework and best practices is going to be really important here, and the great thing about the Cybersecurity Framework with its core and then tier structure, is that it doesn’t have to apply to everybody. Right?

There's probably no single organization that does every single tier, and we need to look at privacy the same way. We don't want to start out by scoping down the

shortest list possible of privacy outcomes and privacy controls. If this is going to stand the test of time, be flexible, apply it to different organizations, it needs to be thorough.

MR. KERRY: So, I'm going to pick up on something both you and Harriet talked about, and put this to the panel as a group. And Harriet, you said, what is privacy risk? So, what I privacy risk; I mean, I think a central question in a risk-based framework. Michelle, you talked about privacy harms. All right, let's explore that a little bit.

MS. PEARSON: Let's mix it up.

MR. KERRY: Where does that link then, right? Harriet, do you want to start?

MS. PEARSON: I'll throw out a definition, which I'm making up on the spot, (laughter) let me just say that. So to me, if you're in the boundaries of, let's say I have an organization, let's say I a $100 million, a $200-million company, generally, roughly, and I'm trying to use the Privacy Framework to guide my actions. What is the risk that I'm trying to govern?

And I think one very simple operationally-focused, it means I can actually implement it and do it, is I want to make sure that I've managed privacy risk in my organization so that I don't depart from the policies and the requirements that I have set for the handling of personal information.

That's the risk I, and I've spent a lot of times inside organizations, I'm trying to govern that risk, and I'm looking for tools and frameworks to help my life make that possible. Where would I look I look to help me manage the risk of not using personal information -- let's leave aside the definition of personal information for a second -- in a way that departs from what I ought to be doing.

That is a simple, straightforward definition that we would be focused on what I as a business am trying to get done, and if I manage that, if I do that right, that is

actually helping privacy and meeting privacy expectations.

And I suspect folks will not agree with that totally, at all, because it does not answer the question: what's the value here? What should that policy be, and I would submit that that might be answered outside of the bounds of assessing privacy risk if I'm using a framework in my own organization. That's a first cut at it.

MR. KERRY: Who is next?

MS. RICHARDSON: And I think the important thing here is that we see this Risk Management Framework is operating regardless of the service or the data. I'm concerned that often risk management is sort of weighing the value of the service, versus the collection of the information. And it's like an on/off switch, right?

If we say that this product is worthwhile then you collect and use whatever you want. But what could be exciting about the framework is that you don't have to make that choice, it's what you are collecting, or use in the everyday decisions that companies are making.

Again, that's going to start with the harm, accepting harm and may be putting themselves in the shoes of their users, and accepting that our ideas of harm have changed, and are changing rapidly, and they are not shrinking, and we need to accept that and change our programs and systems to accommodate that.

MR. HOFFMAN: I would just add, I'd say for the 20 years that some of us have been doing privacy; the topic of trying to define privacy risk has been something professionally fraught with risk.

MS. PEARSON: Really? (Laughter)

MR. HOFFMAN: But let me take a stab at trying to divide the conversation into three different areas. First, I think any organization needs to have a risk management exercise that is managing the risk to the organization, your managing

data that relates, or is likely to relate to an identified or an identifiable individual.

You need to understand what the risk is to your organization for doing that. I actually think that's critical, but it's fundamentally different from, I think, what a lot of people are thinking about when they're thinking about privacy risk, because privacy risk they're thinking about, okay, the use of that data, how could the use of the use of that data impact the individual thinking about privacy as a fundamental human right?

Well I feel like the conversation is moving from us. We started maybe 15, 20 years ago thinking: was that just economic harm, or was that more than economic harm, physically we've moved beyond that now. The general recognition, this is bigger than just economic harm, but now I think we are moving to this third category: is it just risk to the individual or is it also risk to societ6y? And how are we going to quantify that?

I think that's one of the big lessons from Cambridge Analytica that we had use of personal data that had implications beyond just individuals. How do we capture that in some sort of a risk management exercise?

So those are my three categories: risk management for the organization, risk analysis for the individual, risk analysis for society. But then I would say we also need to not do that, we can't do that analysis in a vacuum without talking about the benefits. And it's really critical, particularly, and trust me, organizations will figure out the benefits to the organization. We can take care of that. I'm not worried about that.

But benefits to the individuals, and benefits to society, and how do you include those in the risk management exercise, and then how to determine and use that as a guide, of what you're going to do, and what you're not going to do. I think, once again, we need to have that conversation. It's going to be difficult to figure out a process of how to capture that.

But once again, coming back to Harriet's point about outcome space, just

merely forcing the exercise and the conversation gets real benefits I think.

MS. PEARSON: May I follow on that for a second? It is, you know, we should not underestimate what happens in an organization when you ask a simple question of: Did you consider this? I mean, think about the last time, somebody in a position of authority ask you: Did you think about this? Did I? Well, yeah, it forces you to focus, and as long as people in authority positions, in organizations say - we are going to use this.

We are going to make that a part of our DNA, a part of our process, show what you did, and then potentially, our friends in government, regulators would say: oh, you said you use this, what did you do?

Those are powerful questions with an effect that is not going to ask you to check the box and show all that, but it's an effect that says, well, I'll better have an answer here that's thoughtful. And while I think we all aspire to tackle larger matters, and deal with them, I think one of the success factors, potentially for something as ambitious, intellectually ambitious as a Privacy Framework, is to be modest in what Version 1.0 might be, and understand that it's dynamic, and it will evolve, if needs to be, to evolve to be successful, of course.

And so Version 2.0 might deal with more, and so the first version can be scoped so that it could be accepted use, and as technology gets better, as processes get better, as the discipline of doing this work gets more evolved. I remember, I mean, Dave and I we were part of the start of the privacy field, right, 20-plus years ago, and there were what, a few, 10 of us, 15 of us?

And at last week I give a plug to IPPA, and the (inaudible), I mean, they're over what, 50,000 now, or something like that. Some huge number --

MR. KERRY: Yes.

MS. PEARSON: -- of people in that, organizations who are doing this work, and that means there's work to be done, and there will be more work to be done. So, it's a couple of comments to follow that.

MR. KERRY: Yes. So, I want to pick up on something Dean Garfield talked about a little bit, GDPR, and some of the good things about GDPR. I think there's a lot of thought that one of the things, that it did accomplish, would simply sort of force people to look at their data, and their data governance, and the starting point is, you've got to get your arms around the data.

What do you see as the role in a Privacy Framework for data governance? What are the overlapping lessons from the Cybersecurity Framework, or the GDPR, for a Privacy Framework when it comes to not so simple proposition of data governance?

MR. HALL: Well, since I didn't answer the last question I'm clock in first. I think that, just to follow up on Harriet's point, I think the number one thing that a framework as proposed can do is, one, is force the question, right, actually have companies grapple with it, in ways that the C Suite cares about and understands.

And then also, what NIST I think will do that GDPR did not, is provide the tools to do so. I mean, if you're looking at the Cybersecurity Framework, what it does is it provides a scalable model where you can't -- where mom and pop, all the way up to Fortune 500 Company can use it to actually talk about, and think about, and think through these types of questions.

And GDPR does have some language not into risk analysis, right, but it doesn't actually provide the tools to actually move forward to do this, and this is where the NIST Framework can be a useful thing. Again, not necessarily just complying with a company's own policies or interests, or whatever the U.S. framework is going to look like,

but then also, also GDPR.

So, I do think that the NIST Framework will help companies have that conversation, and to do that initial mapping. Data governance is hard, but some companies aren't really thinking about it, at least not as rigorously as they can, and some companies that are thinking about it, still could benefit from some of the tools, some of the standards that NIST will be able to point to and provide, similar again, to the Cybersecurity Framework.

MS. PEARSON: Another parallel to the Cybersecurity Framework is it's a framework, it's not a standard. And the debate when the Cybersecurity Framework was put together was, what about ISO 27001, what about this, what about that, it was like, yeah, and that, and I don't know if it will transport, or be perfectly parallel here, but data governance is a discipline and I think people are doing already.

And so, what do we learn from that? How do we speak that language? Those are activities organizations are taking to manage, and govern, and extract value, and secure, and to comply with all the things one does with data, not just personal information.

And I'm sure the smart people in this will not ignore that, right, so they'll figure out a way to tie and not ignore an adjacent area of activity. So, I think that goes to the framework being interoperable, because it shouldn't ignore, and it will have a bridge to useful endeavors like that.

MR. KERRY: Michelle, anything that you want to add?

MS. RICHARDSON: Yes. I feel like when we often have these conveniences, we have sort of the engineer track and the lawyer track, right, and the lawyers talk about: what's the bare minimum compliance I have to do? And the engineer say, well, I could do everyone, just someone has got to tell me what to do, right, and so

hopefully this will escalate the decision to someone higher up who doesn't just see a compliance issue, right?

They see threat to the reputation of an organization. They see that people can be called before Congress, apparently, we are learning this year, right? That there could legal liability and that some decisions need to be made at a higher level, so hopefully this will be something that will be operational for people at that point in the organization.

MR. KERRY: Good. Peter Lefkowitz, welcome. You've been introduced in absentia. You can jump in here, or we can give you --

MR. LEFKOWITZ: I'll wait for the reset. And I apologize to the panelists, and I apologize to all of you. I didn't realize that 6:00 a.m. flight would become the 8:30 a.m. flight.

MR. KERRY: So, I do want to pick up on something that Travis said, and kind of put some punctuation on it, but Dean Garfield talked about this as well. And alluding to the guidance process under the GDPR, and the opportunity here I think to model an approach that's more technically sophisticated, and more collaborative, interactive, and adaptable.

So, Travis, I think that that clearly seems to be an objective here. Does everybody agree that there's that opportunity here?

MR. HOFFMAN: Yes. I'll just mention. I think there's a great opportunity here. I think with your earlier question you asked about GDPR, I think there's a number of thinks that are great about GDPR, and once again, going to interoperability, just merely moving from the patchwork of nation state implementations other than 95-46 Directive to a comprehensive approach in GDPR is something now that we look at potentially a patchwork of state legislation here in the United States, I think we need to really look at.

I think it's an open question of how well the guidance is going to work, coming from the European Data Protection Board, now that that body will really function differently than the Article 29 Working Party did.

I think the structure that we have here, where we have the potential to have a high-level law, and then we have context-specific NTIA efforts, that could really provide real guidance and best practices to describe how would it work in individual areas that the great work that NTIA has done in the past around drones, and facial recognition, and other efforts?

And then an effort really informed by technologists to look at how to do risk management exercises, and to fit those three together. If I was advising the members of the European Data Protection Board, I'd say, look, we should be looking to what's coming out of that system to help inform us how we are going to interpret GDPR.

MR. KERRY: Peter?

MR. LEFKOWITZ: Well, I'll add to what David is saying. I think the compare and contrast with the working party is instructive here. You look at the opinion just by way of example. The 2014 opinion on de-identification did an absolutely wonderful job, at least the engineers that I know who really technically, the back half of the paper, did a fabulous job, mathematically, with what constitutes de-identification.

But it then added the overlay of, however, under the law, nothing but complete the identification that could never be reconstructed by anybody counts, and therefore it essentially eviscerated the back-half of the opinion.

And so it seems to me, very much, as David is saying, that there has to be room as there was left under the GDPR, and hopefully there will be left under a Federal Law here if one emerges, for industry standards, for context, and NIST can provide tremendous insight into, by way of example, de-identification, risk balancing,

focus on the ways in which data is used, as opposed to just a linear progression from science, to practice to law.

MR. KERRY: So, Peter, just before you got here, we had a fair amount of back and forth on privacy risks, what it is, how you assess it, how you incorporate that into a privacy framework, and make it risk-based. You have Risk Officer in your title, so you clearly must have thought about this, how do you assess privacy risk?

MR. LEFKOWITZ: So, first just a moment on the Risk Officer title. I came into my company, Citrix, just as the company was moving to the cloud, and moving to very large-scale analytics of metadata for security purposes. And so there was a need to really do some very deep risk balancing. I think for us, and probably for everybody today, in an accountability world, you can't just say privacy officer. I really believe that.

You can't just say privacy officer, or not database with U.S. personal information, European personal information, Australian sales data that doesn't have personal information, it's all part of the mix. And so that's how we arrived at the title of Risk Officer.

The item that I'm struggling with, Cam, I hope it's not too big a job from your question, the item that I'm struggling with, that I know NIST is very focused on, and that I know is going to play into this, but that I think is really important, is that risk requires a sense of context, not just what are you collecting, not just the notice that you've given, but what is the value of the re-use or use of the data, how much risk is there in that residual exhaust of the data that's been either collected or aggregated or created.

And so I think a lot of the really interesting risk balance that we all face in the field, and I'm looking at, you know, Harriet and David as Privacy Officers over time, of major institutions, the balance that we face in the field, is not just to look at, well, you know, is 36,000 words enough for my privacy notice, because there are some now that

are 36,000 words.

But rather, how am I planning to use data, how am I planning to protect it, what is that sort of balance that I can bring to the table, and can a NIST standard, looking at the FIPPs, really get in deep enough to help me with that analysis?

MR. KERRY: Let's turn to the audience for questions. We have microphones moving around. So, please stand and identify yourself, and you ask your questions. Sir; up in the front here --

QUESTIONER: Thank you. Hi. Carl Gallivan, Retired Special Agent, U.S. Customs. I was a 9/11 responder, domain reference, AnIdeaLivesOn.net. My question really would be for Director Copan, and it is that: can any government entity be trusted to ensure the privacy of individuals, unless it itself is transparent in the most important respects regarding its data?

Now, as 9/11 responder, I was among a team of people who sifted the rubble of the World Trade Center 7, at Fresh Kills landfill, the third tower that collapsed on 9/11, which is largely a suppressed memory not discussed in the media at all to day. The 9/11 Commission completely avoided the issue of World Trade Center 7, the 47-floor tower that collapsed on 9/11 because it undermines the official conspiracy theory.

Now, because of that NIST was compelled to develop a model explaining how it collapsed attributed to office fires. And to this day NIST refuses to release its data used to model the collapse of Number 7. So, my challenge to NIST and Director Copan, perhaps you'll answer it even now: will NIST release the data regarding the modeling of the collapsed World Trade Center 7? Architects and engineers, and responders such as myself simply need to know.

MR. KERRY: I'd like to keep the questions to Privacy Framework. If you guys want to take that question offline, that will be fine, but -- Ma'am?

QUESTIONER: I'm Molly Ehret, and I'm Cyber Risk Advisory Practice Lead for coal fire. My question is probably for Harriet or Michelle. We've been trying to, as a consulting firm trying to help lots of our clients understand privacy, and be compliant, and so far we've been using frameworks like NIST 800-53, Rev 4 and 5 of course, we've been using HITRUST, we been using the HIPAA Privacy Rule and so on.

That's of course in lieu of the Privacy Framework which I'm so glad is now being worked upon. Here's my question to you. Right now, when we are working with clients across the industry, we are continuously faced with the absence of laws, regulation, mandates, something that actually provides teeth to all these things. Right?

With 800-53, and so on, you have DoD standards, or mandates that help provide additional force on this that makes corporations, organizations look forward to, or implement this. There is no choice, there's, if you don't do this, we'll be doing this to you, or we'll be removing contracts and so on. So, my question to this panel is, or maybe to NIST, in the backgro8und as we work on this Privacy Framework, are we looking to develop some kind of law that would make us, corporately, and nationally responsible to making sure that companies actually do take care of privacy regulations.

Because right now it's a framework, hopefully it will evolve into a standard, and then so what? Would it be (inaudible), the Times, the large companies, the IBMs, the Gartners -- and I'm sorry I don't need to call on IBM and Garnter, but I do look up to them. And the small companies too, what is there that will make them comply with the framework that we are working on.

MS. RICHARDSON: As far as legislation -- just real quickly -- I think people are working on it, it's not clear yet though, what time frame that is going to happen on, but it is being discussed that it will be baseline, privacy legislation, and will apply to all entities.

There's a possibility it could happen next year, right, people are trying to beat the implementation of state-level privacy laws, but if we don't hit that, the legislative process often takes three to five years, if you're optimistic. Right? So, in the meantime we really appreciate you working with your clients though, to think about privacy in a holistic way.

MS. PEARSON: I need to make an additional comment on that. So, I work with clients across many industries, companies of all sizes, and my own team has about 30 lawyers working full time advising clients on compliance with privacy laws in the United States. So, I think a baseline principle or our understanding is that we have over 50 privacy laws in this country, many privacy laws.

And almost any company that I know of has to work within the bounds of privacy laws that come from both consumer protection standards as well as sectoral specific. So, it may not be a very popular thing to say in D.C. these days, but we have many privacy laws.

Now, are we in a point where we are adding to it potentially, via legislative process, lifting the bar higher, in baseline, legislation? We are. We are debating that, as Cam I think said, or as Dean Garfield said, you know, laws have to evolve to react to and accommodate the needs of the day, but we have many laws, but so maybe we'll take offline a little bit, I'll point you to some frameworks, because they are -- start off with the International Association of Privacy Professional's website, they have frameworks, there are accounting frameworks.

We have a lot of different tools at our disposal to help companies assess what is expected, but where we don't necessarily have clarity is the deeper level, which is actually it, so beyond saying that these are the -- here's what you need to do, it's like how do I do it, there's a dearth of that. I think that's right. And as an engineer and a lawyer,

I've tried to fuse that, and I think that's where NIST's new work comes in.

MR. HOFFMAN: Can I just add on to that.

MS. PEARSON: Yeah.

MR. HOFFMAN: I completely agree with Harriet, that we have a huge number of laws, I think they are largely as a body now, inconsistent, and incomplete, and not sufficient for what we need. Intel has had the position now for 15 years that we need, a comprehensive U.S. privacy law that recognizes privacy, it's a fundamental human right, and one that is based off the OECD Fair Information Practice Principles in a flexible way that allows for data innovation in line with the U.S.'s tradition of innovation.

And I think that's possible, I think this is a unique moment, and I think we clearly have gaps, and we've seen what those gaps are.

I think that lawyers are not happy to hear that, because actually with the way -- direction that we are going, we are going to see a lot of different state laws, we are going to see more laws, and it's going to -- in the same way that it's done, the State Breach Notification Laws, we are going to drive a huge amount of work to large law firms to figure out the mess and how to comply. I think we need a focused effort to provide something that's consistent.

MR. HALL: And I just want to jump in really quick for another plug. We are going to be very soon putting out a request for comment with the proposed approach on how to move forward, and we are looking to people to help us figure out what that path should be.

MR. KERRY: Let me go to the middle of the room here, on my right. And then we'll go to Dean Garfield?

MS. KITCES: Hi. I'm Lauren Kitces. I'm the Global Privacy Manager at Willis Towers Watson. As a company that operates in about 140 countries, we deal with

an inordinate number of different regulations or requirements around the world. And with the interconnectedness of data, and the transfer of data being so prevalent these days, how do you find the ability to overcome the hurdles of all of the different regulations?

Because, whether FIPPs or OECD, there are frameworks that exist already, obviously are principles that are enshrined in many or most of these laws, but so many of them go so far beyond that base level, and have such a variation, as was just noted even in the U.S. alone. So how do you see overcoming the hurdles of those variations within this framework?

MR. KERRY: Peter?

MR. LEFKOWITZ: So, obviously we are at the beginning of the process, and we are speaking about hope here, but I'll give you a couple of places of hope -- I see the Director is looking at me, so I'm happy -- a couple of place of hope. Number one, from an industry perspective getting back to Fair Information Practices, getting back to the fundamentals, allows people to pull the lens up a little bit, right.

The first state legislative efforts have been very focused on purely consumer data business kind of things, I think we really need to pull that lens up, and look more at, you know, it's not one type of data with one type of use, it's really about collection, use, reuse, security, retention, destruction, right? So that's number one.

Number two, the power of NIST, there's something to be said for an organizing body, an organizing body with a great deal of engineering, mathematical ability, and with the ability to bring people together.

And then number three, to go back to another conversation, there are hooks and laws around the world now. There are hooks in Canada, there are hooks in Europe that hopefully will be developed, hopefully there will be hooks in the U.S. for standards-based work, for industries to develop standards.

We start to see industry in various places now, picking up on this notion, right, the future privacy foreign work with the automotive industry, the work on smart cities, and smart city standards. There are standards that are developing in the hope that we will create something that is interoperable internationally, and so draw countries closer together so data doesn't have to stop at borders, the airplane doesn't have to turn it's monitoring off when it leaves France, or the MRI machine.

And that number two, I think simply by virtue of the imprimatur and what we've seen from the things like the Cybersecurity Framework, will create a little bit more of a fundamental baseline.

MS. RICHARDSON: I would also say your question sort of shows how important it is that the framework be comprehensive, right, for people to find the flexibility and the controls that apply to their business in a specific country, or different regulation. They need options, right? If it's going to be incredibly narrow on outcomes and controls, you may not be able to use it in a way that actually serves our business.

MR. HALL: I want to just reiterate what was already said, like, it is the hope that this process is going to be providing those types of tools, that aren't just useful in the United States, that are useful everywhere regardless of what your regulations you're trying to deal with, and again just simply your own policies, like trying to actually live up to your own policies.

And I do want to say, just echoing what has already been said, interoperability is extraordinarily important to the Department of Commerce, has been working for the International Trade Administration on this issue, on both with Europe and through the APEC CBPRs, and we want to ensure that anything we move forward will continue on that path.

MR. KERRY: We have got Dean's question, but we are winding down,

as a “Wait, Wait, Don’t Tell Me” fan, I like to wind up with a lightening round. The lightening round question: what's the easiest part of putting together a Privacy Framework? What do you think is the toughest challenge?

So, I'll go to Dean for his question, while you guys are thinking about your answer.

MR. GARFIELD: I’ll reply to the second question, so as we drive to interoperability, what are the particular issues that you think have to be addressed to achieve that? There's been some discussion about definitions of personal data; or, Michelle, you made the point about company accountability, and I'm just curious what elements do you need to be there?

MR. HALL: Well, there are two different types of interoperability that we are kind of talking about the interoperability of the framework versus the interoperability of the laws, the interoperability of the framework, I think goes to what Michelle was saying, of making sure that it's actually useful, regardless.

That it's agnostic, that it's not tying its string to a single regulatory framework even if it's the United States. But in terms of interoperability of laws, that is a bigger, harder question of trying to ensure that we move towards a situation where we understand that different sovereign nations can have different priorities, and different laws, and that's okay, that's how we work.

But that that doesn’t mean that we can't still have the data flow that is required to ensure that the Internet continues to function the way that it functions as a global digital network.

MR. HOFFMAN: I would just add to the thing, I think that's most critical would be future proofing, whatever is going to be done to make sure that it's flexible over time. Let me give you an example, that Peter touched on, which was the use of

metadata for cyber security purposes.

I think 15 years ago, if you asked a bunch of privacy people they would have zeroed in right on, we have to go for data minimization; we've got to make sure we are processing as little personal data as possible to accomplish the goal.

If you look at what Peter's organization, and other organizations are doing, they're processing data that could relate to individuals, depending on how it's done, and I don't know how Citrix does -- that actually is protecting privacy, because it's increasing cyber security.

So, if we had driven down just into the nature of data minimization and how it was done 15 years ago, and not providing an opportunity to flexibly assess risk and benefit, both the privacy we would have made a huge mistake, and I think that's what we have to guard against here.

MR. LEFKOWITZ: You're hired. (Laughter)

MR. KERRY: So, Peter, we'll start at your end.

MR. LEFKOWITZ: Okay.

MR. KERRY: So, how hard is it?

MR. LEFKOWITZ: So, quickly. You know, there's the story about the rabbi that everybody goes to see, and before he answers anybody's questions, no matter how tough, he looks at a little piece of paper that's in his desk and he closes the desk, and he nods and he gives these answers, he gives these absolutely brilliant answers.

Finally one day someone then seeing him, and he goes out to the bathroom, and he'd run over to the other side of the desk and they look. And the paper says: Hebrew reads to right to left. (Laughter)

The key here is to go back to basics. The FIPPs are incredibly simple, the Fair Information Practice are incredibly simple, but in the world we live in today, the

analysis of them, the discussion of them, how do you deal with collection? What are the factors that go into security? What does destruction mean? How do you handle risk management for reuse of data for fundamental, critical purposes?

Really, really, really basic fundamental things that will require a great deal of thought, and so my suggestion would be go back to the FIPPs, really focus, to your point, on what's really essential here, I would say, stick with the basics, because that's still going to be pretty tough.

MR. KERRY: So, we are going with the rabbi. You have the FIPPs, everything else is commentary?

MR. HOFFMAN: That's right.

MS. RICHARDSON: Well, I will say in answer to Dean's question, what has to be included, and what is going to be the hardest, is actually tackling collection use and sharing limits. I think it's very possible, if you look at some of the frameworks that have already emerged, and the conversations on The Hill, they're talking about everything but, right?

It's, well who is in charge of this system, what's the notice look like, can they check a box? And you never actually answer the question of: are we collecting the right stuff? Are we using it fairly? Are we not sharing it with people who just want to sell it for no other reason?

And it's going to be hard. There are a lot of, you know, very important uses of the data, but if we don't come out of the process with having this conversation, we have really missed an opportunity here.

MR. KERRY: Harriet, easiest, toughest?

MS. PEARSON: The hardest part I think is just that, which is how do you actually inject some of the values that are inherent to the discussion on privacy, into a

framework that's supposed to be the operational side of it? How do you actually do mismanagement without actually defining what the answer ought to be? And reasonable and good people will define that, and that's the debate the consultative process.

And the easiest part of this, is getting people interested, because we have a full auditorium, and it's a hot topic so, I think timing is everything, so this will be a piece of cake, from that perspective. (Laughter)

MR. KERRY: Travis?

MR. HALL: So, I think that folks have already touched on some of the difficulties, right? I mean, relative to cyber security it's a different political beast, and there are different understandings of the risk. I mean, from my part, I actually think it's fairly straightforward because you can just simply say that there is risk, and you can then talk about, in terms of flexible ways, how can you give in a broader, flexible definitions, depending on your regulation, depending on the values of the organization? How do you then mitigate those?

But it's going to be a hard conversation, particularly in context of the fact that there are actual political conversations going on externally about that, and how to incentivize that. But one thing that I do want to point out that I think NIST would definitely agree with, because I learned it from them, is that relative to cyber security as well, there isn't as many explicit standards, and so this might also be something of a gap-filling exercise.

And recognizing where there needs to be work done on actually developing standards for controls for outcomes, things like that, I think that that is something that is going to naturally arise out of this exercise. Like you did with cyber security, but for cyber security there was just a greater body of that work. And again, I can't take credit for that.

MR. KERRY: David, last word?

MR. HOFFMAN: Easiest, start with the OECD/FIPPs, as my former colleague, Paul Bruning has called them; they're the global common language of privacy. If you want interoperability globally, start with the OECD/FIPPs.

Hardest, getting arms around what's the societal benefits and societal harms are from the use of data and how we include them in a risk management exercise.

MR. KERRY: Everybody, please, thank our panel.

(Applause)

We'll now take a 10-minute break, and then back for the second panel.

(Recess)

MS. LEFKOVITZ: All right, we're going to go ahead and get started. I'm Naomi Lefkovitz, Senior Policy Advisor with NIST. I just want to say thank you to Cam and Brookings and staff for hosting this terrific event and helping NIST get started and convening stakeholders. So, we can develop this consensus driven framework and use it as an opportunity to demonstrate how in the U.S. we can promote both privacy and innovation. We have no preconceived ideas about what this privacy framework should look like or how it should function. Other than that, it should be a tool to help organizations of all kinds manage privacy risks. So, we want to hear from our experts sitting here as well as you, the experts in the audience, about what would be beneficial for your organizations.

So, the thing about voluntary tools is if they don't provide value then they're not going to get adopted. So, that' means that this framework has to be robust enough to help organizations provide meaningful privacy protections but also accessible and scalable to many different types of organizations as you've heard already. I mean, I don't know, piece of cake right, I don't know why everybody is saying it's so complicated.

In all seriousness, this panel is going to get a chance to dig down a little deeper and begin to think about what models or other tools currently exist that could help inform this framework and what privacy practices it should cover.

So, with that, let me introduce our experts and get things started. In the interest of time, I'm just going to stick with names and titles but you can read their impressive bios online. Let's start with Jenn Behrens, Partner and Executive Vice President of Privacy at KUMA. Kevin Gay, Chief of Intelligent Transportation Systems Policy, Architecture and Knowledge Transfer with the Federal Highway Administration at the Department of Transportation. Harley Geiger, Director of Public Policy Rapid7. Zoe Strickland, Managing Director and Global Chief Privacy Officer at JP Morgan Chase and John Verdi, Vice President of Policy, the Future of Privacy Forum and former colleague at the Department of Commerce.

All right so let's get this started. So, to help us better understand the context for your perspective on tools and practices, let's just begin by hearing how each of you are approaching the issue of privacy risk management. Jenn, do you want to start us off?

MS. BEHRENS: Sure. I'd like to echo Naomi's thanks and appreciation for this wonderful event and for inviting me to participate in this panel, this is really exciting. I work with a lot of different clients across government and industry sectors. One of the things that they are leaning more towards is moving out of that reactive privacy compliance stance and more towards a risk management approach.

So, I work a lot with my clients and well what does that mean, how do you make risk informed decisions regarding privacy. One of the questions I often get when clients come to me for risk assessments or privacy assessments is well what privacy framework is out there, I know there is this NIST CSF. Is there a privacy version and I'm like well,

kind of sort of bits and pieces. And then what we end up doing is compiling and hodge podging a lot of different tools together. I love the question in the audience about you've got High Trust out there, we've got SOC, you've got PCI. You've got some things that kind of you can pull different components from and do like a compliance assessment with 853 and then sometimes I hybridize and slap on the taxonomy of privacy implicated risk for individuals. But there is not one overarching framework that we can hang our hat on with any confidence, I think, in working with clients and really putting forward that this is a mature model that you can represent going forward that you have any level of organizational maturity in your privacy program.

That's definitely one of those things that I look for in working with clients to make informed decisions regarding the evolution of their privacy practices. But then also how to operationalize those kind of squishy Phipps that are beautiful but they are hard to put into the technology stack if you've got to build something or how to demonstrate compliance against transparency and beyond just simple, here's a privacy policy that you can read. I'm very excited to see this work effort coming out NIST to be able to support the risk management within organizations that are trying to put more meaning behind just a policy statement or just saying we do privacy.

MS. LEFKOVITZ: Great thanks. Kevin.

MR. GAY: I think I would echo a lot of the comments that you just said. So, a little bit of background is at the Department of Transportation earlier this year, we released our 2018 through 2022 strategic plan which outlines the Secretary's priorities for achieving a mission of safety at the Department. So, one of the four goals in there is innovation. As a part of that goal, it was identified that we want to encourage the adoption of the NIST cyber security framework for the transportation ecosystem. So, as a part of that, we've actually been working with the experts at NIST over the past year to

take the NIST cyber security framework and apply it to deployments of intelligent transportation systems around the country. We hope that developing this profile with our colleagues at NIST will provide a model for future deployments of an intelligent transportation systems and lead to further innovation.

On the privacy side, we would very much like to follow the same kind of model. Where, if there is a privacy framework that's a voluntary framework established by the folks at NIST, then we could make sure that that supports the transportation needs and that it would be something that we could work with them to modify or to customize for specific transportation technologies. Things like connected vehicles and automated vehicles and other developments that are just revolutionizing how folks move across the country.

So, we've been doing it sort of in a one-off approach now working directly with our deployers. When they have concerns, we certainly work with you on the privacy risk assessment methodology but I'm happy to participate in this and see how this develops into potentially a framework that could be utilized by all of the state and local agencies and other deployers of ITS.

MS. LEFKOVITZ: Great thank you. Harley.

MR. GEIGER: Thanks, and thank you to Brookings for having me here. So, Rapid7 is a cyber-security company. So, we are pretty squarely focused on helping organizations strengthen the security components of their privacy efforts. So, the way that we are approaching this is recognizing that security is fundamental to the privacy implementation. It is the shaded portion of the vin diagram between security and privacy that we're focused on. Privacy's control and awareness of how your information is collected, accessed, used and data security is making sure that unauthorized access, use does not happen. So in some ways, security is implementing or enforcing the

privacy framework.

In our opinion, many of the risks, the privacy risks that organizations and end users are worried about are, for example, leak of data to identify thieves or general public. In a lot of ways, these are also security risks because these are things that are not intended, not authorized by the data controller, the data processer. This concept is reflected in many privacy frameworks. GDPR, for example, APEC, the PHIPS of course, HIPAA, the California Consumer Privacy Act and several NIST publications which blends security and privacy to show organizations how they align.

I think it is also worth noting that the consensus around this issue, there are 17 states that have data security laws focused on the protection of personal information and many things that we consider to be privacy risks. So in our view, the motivations of protecting consumers, getting organizations on the same page with regard to their privacy practices and also helping organizations to comply with what is, as was recognized earlier, a growing patchwork of privacy law. All of those motivations must include security if we're going to be serious about privacy.

There is an important distinction though that gets lost and that is the unshaded portions of that vin diagram of security and privacy. When we are talking about security in the context of privacy, we're talking about security of personal information. Not necessarily the security of systems that deal with business assets that have nothing to do with personal information. Now, I recognize that those can be included indirectly with privacy because those types of systems can still route a cyber-attack whose target is personal information.

But for purposes of a privacy framework, you don't want to shoe horn the entire NIST cyber security framework into a privacy framework. It would just be impractical so we have to cut it off at some point there. That distinction may seem obvious to the folks

in this room but I have definitely learned not to take it for granted. I've been in several legislative discussions, for example, where data security is viewed as somehow completely separate from privacy and we really don't view it that way.

Lastly, I would just say that we have the utmost respect for NIST's work and expertise and their diligence. You've done tremendous work in this area and so we're really excited to see how the privacy framework will develop. Thanks.

MS. LEFKOVITZ: Okay thank you. Zoe.

MS. STRICKLAND: Sure. Well, I want to start as well thanking Brookings and Mr. Kerry. I think this is an excellent opportunity and a wonderful time to be looking at these issues. I really value the first panel. For those of us who have been doing privacy for a while or even if you haven't these have been issues that have been vexing us for several years. So, we've been talking about interoperability for a long time, we've been talking about the fragmentation, we've been talking about being forward looking. So, from my perspective if we say we should do it then let's do it. I think that the timing is right and the momentum is right in terms of the attention to this issue.

So, I'm going to focus on the management part of the question particularly for large companies and talk a little bit about how we do privacy governments at JP Morgan. Part of my role besides being the lead privacy person for the firm is also to build out the privacy infrastructure. Very large company what does that look like. So, we now have privacy focal centers within compliance and every line of business, every region, and we also have executives in every line of business and region who are responsible for execution and accountability and advice. And being a bank, we all govern this under what we call operating models so that we don't have folks doing things that are not connected to an overall approach. So, a lot of conversation about what that means, what does that mean in different lines of business, what does it mean in different regions,

because there are variations to these core principles that we've all talked about.

As we think about a risk-based lens, we always think about it in two levels. One is you do have to do the basic compliance with laws that have been passed and these tend to build over time. When we have these new issues in privacy which is one reason I really like it. There's always that new frontier, there's always that new technology, there is always that new way of using data.

How do you think about that, how do you provide and apply a risk-based lens to the existing laws to make sure you're really getting to that compliance with the spirit of what the intent was. And how are you thinking about a little bit too what was talked about in the openers with Walter and Dean about that risk-based lens, what does that really mean. Because we are all trying to be very forward looking about how we're gathering data and merging data and things like that. We hear a lot about when all the appliances in your house are talking to the internet and then there is some intermediary that's sharing that with companies, what do we think about that.

So, I'm very excited about what both Department of Commerce and NIST is doing. In my mind, it's a little bit of the glue which is we've got principles. We talk about this too which is in companies, there is a lot of principles and policies and training and then you have the engineers on the ground. There has been a lot of conversations including IP and elsewhere, FPF is leading in this which is how do you put those things together. So, there's a lot of conversations in industry about how do you start making that more systematic when you build privacy into various product designs and things like that and what does it mean.

I think that is what NIST is trying to do which is how do you take what is being developed through Department of Commerce with a deeper set of principles that people can actually understand and can implement. And then you have things like NIST

where you can have those tools, that code of conduct that is very popular in policymakers' minds. So, I think it will be a very important component to how we both articulate and resolve these things for the future.

MS. LEFKOVITZ: Great, thanks Zoe. John.

MR. VERDI: So, that's a bit of pressure, Zoe, you apparently were leading. So, I'm going to have to say something leaderly and I'll do my best. I very much appreciate the kind words. I also appreciate the invitation from Cam and the folks at Brookings and from the folks at NIST. Naomi, I always enjoy working with you and your team.

When I think about how the FPF community, the companies and the advocates and the academics and others look at privacy risk. There is, of course, the conversation around risk of physical harm, risk of financial fraud, risk of loss of opportunity based on data processing that you didn't consent to or expect, risk of embarrassment. There are those kinds of taxonomies of risk. One of the really interesting things that I see driving some of this conversation is risk but risk meant in a different way from those kinds of risk. I'm specifically talking here about enforcement risk. So, when companies in the United States think about risk, many of them start, they don't end but they start by thinking about what the risk of enforcement is.

So, if an entity like the Federal Trade Commission articulates through rulemaking, through other enforcement actions, through settlements, through other means, that a particular data category or a particular behavior is going to be subject to investigation and enforcement. Companies as a baseline matter, I think, their legal departments pay a great deal of attention to those sorts of risks. So, if the FTC says, children's data needs to be protected and there is a rule. Because exposure of children's data or handling of children's data in particular ways are risky, that enforcement risk or

investigation risk drives the definition of risk within an organization.

Now at most organizations like Zoe's and others, that isn't the end of the conversation but I think that's the beginning of the conversation. And a slightly different conversation happens in Europe. You look to Article 35 and you look to other articulations of what particular risks are. Whether it is automated processing or whether it's large scale processing. I think that one of the really meritorious things that NIST effort in this area might do is start from the basis of pooling and collecting all the risks that have already been flagged or acknowledged in statute or rule around the world. Like kids' data or the processing of information that can have really concrete negative legal impacts on folks. Like the sort of decision making that can impact somebody's eligibility for public benefits for a job, for example.

Once you kind of see a consensus view there, you can build on it. You can say well there aren't a ton of laws out there that outlaw use of data that leads to humiliation. But nonetheless, users really care about that so let's see what we can do to try to capture that as well. Or there aren't really laws out there that capture precisely this idea of loss of opportunity or things along those lines. Maybe we need to go ahead and capture some of those things to put it on top.

But I think if you start off with a really solid basis on where the consensus risks are right now, financial fraud, physical harm, kids' data, a variety of other things, you're going to get a ways down the road where you're going to probably have broad consensus. I think that that's probably a helpful way to think about it that can bridge the conversation between policymakers, business leaders, advocates, academics and other stakeholders.

MS. LEFKOVITZ: Great, thank you. So Jenn, not to put you on the spot but you work with a variety of organizations. So, how do you see that, what do you think

is driving them, non-compliance or concerns about whether people abandon services or products?

MS. BEHRENS: Yeah so, I think a couple of years ago definitely it was more compliance based. I've had CEO's hire me and say, I don't want to have to look over my shoulder so just fix it, do what you need to do to make sure we're compliant with everything or we're not right of any major law.

What I've seen in the market and what I'm consistently now hearing from clients and we work with, for example, the County of Santa Clair government and seating their chief privacy officer. They're building out a really comprehensive privacy program but then we also work with a lot of tech startups, also healthcare organizations from clinical research to medical to health information exchange networks.

What I'm consistently hearing, especially over the last 18 months is what they're hearing from their consumers, their patients, their customers that they want to know that the organizations are tackling privacy. Everyone has been burned by the big breeches that are out there. I joke all the time and say customers are not necessarily more sophisticated about the backend handshakes that are happening with all the solutions and how technology is integrated but they are more savvy these days. So, they do know that organizations should be protecting those backend handshakes. They start asking questions of the client organizations, what are you doing with my data, where is it going, how are you managing my risk. They know enough to be savvy to push back on the client organizations and so I'm having conversations with my clients now that they are needing to meet the consumer expectations not just regulatory or standard compliance frameworks.

For me, that has been really exciting because now I'm starting to hear organizations say yeah, I want to do a privacy risk assessment because we see this as a

market differentiator for us. That's super cool because then you start to get people who are being more proactive and innovative and thinking about how can we embed privacy. Not just in our great 36,000 privacy policy word count but also what can we do about really understanding, and this is where I think the framework is going to be helpful. Really understanding where your privacy risk sits based on knowledge about where your data resides and then how do you tackle pulling apart the threads of standards and regulations but also then privacy enhancing technology components.

You become aware and that's what I think I also heard that making these things more meaningful and approachable for organizations is very critical or else it is just going to stay some very high-level framework that no one touches. I think that's one of the things that the CSF does really well. It breaks things apart for organizations to use very succinctly and in a manageable way. That would be my hope for the privacy framework that as organizations are starting to really advance their privacy posture in a proactive way, it can be utilized as a tool to manage that risk in an informed way. So, that's what I'm seeing more from my compliance. They still want to check the compliance box but they're looking for a little bit more these days.

MS. LEFKOVITZ: Great. So, with that sort of segue you sort of mentioned the CSF as a potential model or framework that can inform the development of this NIST privacy framework. What do others think? Are you aware of, are you using, you can add on about the value of the CSF as a model or there are other tools or frameworks or models that you're using that could inform the development. Whoever wants to jump in.

MR. GAY: Well, I guess I can jump in actually and say while we're not using other frameworks for privacy, we are taking privacy seriously in the research programs in my office. One important thing that I'd like to call out is that make sure as

you're moving forward with this, think about transportation as sort of unique. It's a little bit different in some respects because we are conducting research in areas around automated vehicles and data sharing. State and local agencies are looking at collecting more data to improve transportation system operations. So, less crashes out on the road, more mobility, just the system performing better. Geolocation data and work zone data and other data about the transportation systems are really important to ensure that both automated vehicle deployment can happen and that the system can function more smoothly.

So, in some of the research we've done we've looked at ways to basically provide some protection around the collection of geolocation data and how that data can eventually be strung together to create trips. And then combined with other data that's out there, start to pull back and identify things. So, I very much encourage you as you think about developing this framework to think about how transportation users would fit into that. So that once you have a framework we'd be able to again move forward with a profile or do something that helps state and local agencies deploy in this technology think more about how can we do this up front. And make sure we're covered and the deployments that we're doing are going to improve and continue innovation. Rather than have them pull back and say no, we don't want to deploy this technology because we're concerned about cyber risk or privacy risk or other things that may sort of stifle that innovation and that deployment of technology in the transportation sector.

MS. LEFKOVITZ: Thanks. Harley, one second. So, it sounds like is it fair to say then you think the concept of profile is something that could inform the development of this?

MR. GAY: I think it's a hopeful way to think about it. It has been helpful on the cyber security side because again, transportation agencies are putting things like

smart street lights and Wi-Fi routers and other things out on the roadside in the infrastructure. And then they have traditional infrastructure like message signs. So, as it is moving forward it is sort of a different environment in that it is a little bit more exposed, it's not in the enterprise level and that you're in back office systems.

Now, they certainly tie into that but the technology that's being deployed within the vehicle and on the highways are a little bit different than what we see with our mobile phones and our enterprise systems. Some way that we can pull out and identify what would be of interest to transportation stakeholders, very much whether you're going to call it profiles or whatever else is we're okay with that.

MS. LEFKOVICH: Great thanks. Harley you were going to say something.

MR. GEIGER: Yeah, I comment on an implementation tool and then on existing frameworks. A tool that we have found helpful in cyber security like for cyber security risk management for our clients is a risk matrix. Relatively common for compliance, not necessarily for best practices but it can be adapted for that. The risk matrix is often a five by five graphical representation of risk. Five by is kind of arbitrary. It can be four by four, six by six. And then the row is the likelihood of risk and then the columns are severity of risk.

You can also map control implementations on there to see whether or not your controls and how effective they are, are in fact, attaching to the risks that are most likely and most severe. That would probably be separate from a list of privacy controls. But if there is a section helping to illustrate for organizations that are using a privacy framework, how to in fact, incorporate into the risk management processes, that is one tool to consider.

On existing frameworks, I'll say I'm very glad to hear that businesses are

responding to consumers privacy concerns beyond compliance and that they view it as a market differentiator. I think those things are crucial for privacy to really move forward in a sustainable way. On the other hand, I think the privacy framework really ought to take into very serious account, existing frameworks from regulators specifically the FTC and State Attorneys General. Businesses, I think, although like I said, I'm very pleased to hear that they are doing privacy as a right to be protected in and of itself. I think that the framework will not be as useful for companies or will be overlooked by companies that have limited time and resources if it is not also going to help them get to compliance.

MS. STRICKLAND: Yeah, I want to come at it from a slightly different angle because I think NIST has a lot of expertise in thinking about how to do these sorts of frameworks. I think what is going to be interesting for them is how do you marry it to something like privacy which can be a little bit more diffuse or variable. So, we'll have to think but I want to make a general comment first and then give some specific examples.

So, there will have to be some way of saying okay, what does it even apply to and it can't just be is this sort of like no one can define PI so there needs to be some commonality there. Or you can tap into people's classification standards because most companies have that, that's an option. There will have to be some way to think about what are those risks and how do you manage through them because that's what the rest of the document does. There are a lot of good models out there that talk about privacy risks. You can look at some of the government act things, you can look at GDPR but that will need to be theirs. That sort of funnel about how the rest of the document works will need some attention.

There is a lot of good privacy expertise that can be tapped into. Definitely we'll need to be partnering which I think is happening with things like the principles from Department of Commerce because those should align in some sort of

way. We're very involved with the business roundtable in terms of what privacy principles could look like. As these things evolve, how do they partner up.

A couple of specific examples where I think that this could be particularly helpful and it did come up in the first panel. One is around the identification. There is a lot of good material out there across many countries or industries to think about how you do that. I know some are very defined like HIPPA but the rest of the time, not so much. So, that would be a very useful area. Because typically if you identify data then it is not subject to the same rigor as an SSN, as an example.

Another area is how you do these sort of risk assessments and there has been really good work done around privacy impact assessments. I think the E-Government Act was a front runner. There is a lot of good material at GDPR. So, I think there are some things in the privacy space that can help create that sort of entry funnel as the rest of the tool gets built out.

MR. VERDI: I would echo what Harley said about risk matrices. We use those sorts of tools when we worked with the City of Seattle to try to assess the relative risk of some of their open government data sets. So, Washington State has one of the most robust open government laws in the country and the City of Seattle was quite naturally worried about the sorts of data they were releasing, for example, from maybe their 911 call database. They were much less worried about the sort of data they were releasing from air quality sensors in their parks. And being able to sit down and work through a process on a risk matrix helped them operationalize those sorts of concerns that everybody had in their head but they didn't necessarily have a way to make it programmatic within their organization. So, I would echo Harley on that, super helpful.

The second thing I would say to kind of tag on to what Zoe raised, I do think the NIST effort is a crucially important effort and I appreciate the fact that you folks

are working with folks over at NTIA and with the National Economic Council with the administration. I think there is a risk here though, no pun intended. That risk is if the NIST process is perceived as a way to define privacy risk for a legislative proposal, it is going to be subject to a lot of pressures that are very different from a process that is explicitly articulated as something that is intended to define privacy risk in an operational way that is going to be consistent with perhaps a legislative proposal.

It's going to be consistent with U.S. and European and Asia Pacific laws but is much broader than that. And that the intent is not to impose legal liability on all categories defined as risks but rather to identify categories as risks that ought to be managed and weighed against benefits. I think a clear articulation of that will be helpful in terms of fending off some of those pressures or increasing some of those pressures depending on where it goes.

MS. STRICKLAND: Do you mind I have a quick follow up to the point on the privacy versus security which I others might want to comment. I think that's right, I think their goal is looking at analogy to a code of conduct that can allow the pieces to fit together. I do think there is a very interesting part now as privacy and security interface even more with each other than they have before. There always was a healthy relationship but I'll give you an example from several of the large companies I worked at.

Security folks will often be like, well how do I have security that's appropriate for the type of data. Security is a good value, it's just a question of how do we achieve it. With privacy, you'll have people with very different opinions and I'll give you an example that's been in more than one company I worked at, which is birthdays. You'll have employees come to you and say, I'm really upset that I recognize everyone else's birthdays and I didn't get that and how do we share each other's birthdays with each other so we can celebrate. This is something I really care about, it builds these

connections in the workplace.

I also have employees coming to me going, I can't believe they celebrated my birthday. They put balloons at my desk, I don't celebrate birthdays, how did they know it was my birthday. They were actually really upset and I'm look, they really weren't trying to upset you because I told them last year. So, people look at it very differently and I think that's part of what privacy can do in a principle base.

Which is like, how do we understand the data, how do we understand the right uses of that data, what does that look like, how do you understand it. Which, I think, also makes it a good and a fun challenge for folks like NIST about how do we frame that up and then say what are the right controls attached to it. You might have other folks too as well as how they think about these two things fitting together.

MS. BEHRENS: I'm going to pull on the risk matrix thread that a couple of my colleagues have discussed. It is actually one of the things that we've converted our assessments that we provide for our clients. Again, I drive hard on the risk side of it and this also gets to the original question about are organizations seeking more than just a compliance-based privacy effort these days.

What I'm seeing, especially with utilizing some sort of risk matrix or risk criteria is that organizations can then more proportionately manage the risk from an operational perspective. It's not just, I'm compliant or I'm not compliant and we hand in the report and then they can turn it to someone, their auditors. What we've started doing and I've been hybridizing a lot of different tools to get to a risk assessment.

So, for pension fund I did appendix J plus a taxonomy of privacy for a major ride share organization that I've been working with recently. I did the GAPS, Generally Accepted Privacy Principles then mapped those to the PHIPS and then did the NIST 862 adapted taxonomy of privacy for implicated risk. That covers your grounded framework,

your compliance but then also your implicated risk and you can give a risk criteria score.

Then what each of those organizations have been able to do is go forward to their internal audit committees to their boards and their C suite as well as their investors and make informed decisions on where to apply resources and allocate funding. Instead of just saying we're good, they can now make intelligent decisions based on risk profiles about what aspects of the organization they need to change or enhance or remediate in order to have a more privacy informed and balanced organization.

So, I would concur with my colleagues about that necessity to drive towards that risk criteria or scoring or matrix or whatever language we ultimately want to call it. That's one of those important things I see out of the CSF that I think would be really important for the privacy framework in order to help pull organizations out of that compliance-based kind of route that they have gotten into in the last several years and more into the privacy risk management.

MS. LEFKOVITZ: Great thanks. So, I feel like we could probably talk about this for a long time. I want to get to the other half of the title which is practices. Kevin, I felt like you were starting to go there with certain practices around the type of collection and how you're going to manage that kind of data. Are there other practices that should be covered. You think about the cyber security framework. They sort of have these categories and subcategories which even though you can do a profile and figure out sort of the outcomes you're trying to get to, they sort of holistically give you a sense of hey, these are the different areas of a cyber security program. Is this something that we would want to follow in the privacy framework in terms of thinking about, hey there are these different outcomes that you might be trying to get to, what should that cover, what kinds of practices should that cover. Anybody want to jump in?

MR. GAY: Well I can definitely follow up a little bit from the research side in the Department of Transportation. So, some of the activities that we have started are looking at ways for transportation agencies to collect data and then be able to share it openly with users of the transportation system. So, that's a really important process. One of the things we've done now is we've worked our colleagues at Oakridge National Labs to be able to prototype sort of a privacy algorithm.

We actually operationalized it into an open source module that transportation agencies are able to collect real time data from vehicles that are instrumented and broadcasting what is a called a basic safety message. Which identifies basically their geolocation, speed, position and transportation agencies collect this data because it helps them improve the operations of the system and they want to be able to share that openly with some of the users of the systems.

So, one of the areas we're working with is in Wyoming. They've got an I 80 corridor that has a huge amount of weather issues there. It causes untold delays and fatalities every year. So, finding a way for the State of Wyoming to be able to share that data more openly and address privacy concerns was vitally important to us. We worked very closely with them on that.

Again, I feel like if there are tools that NIST is able to develop to help standardize that and make it so it is not a one-off process for every state local agency that we try to work with. That's where I'm really come at it from the Department of Transportation side. I think some of the stuff we've done would be informative but we're also looking for lots of help.

MS. STRICKLAND: So, I think we talked about in the first panel as well about how do we think about what actually we're going to cover here. I do think when you look at some broad-based privacy frameworks out there like APAC, OECD, they're

all good and they've got the right hot topics we're going to cover. We certainly want to modernize them with things like notice and transparency and things of that nature.

I think there are three areas that really merit a deeper look. One is accountability. A lot of conversation about what does that actually mean and how do you demonstrate that. Particularly you're going to have a tool, how do you do that. How do you say hey have you got the right roles involved in this, it's not just the privacy office doing this and signing off on it. That is not going to be baking it into the organization so how is that covered in a tool like this.

A big issue that is showing up in a lot of the privacy laws now are individual rights. So, what does that mean, what sort of rights are we going to be giving to the individuals whose data we're collecting and how does that fit into a framework. Are we going to say, well whatever rights you've deployed here's how you're going to track that and tool around it. So, that's definitely a major activity now in the privacy space. I think is one where there's a lot of different ways of thinking through it because often individual rights are when people can submit a request for whatever. Access deletion, don't process my data, but now we're hearing things like transparency is a right. So, that's less of something you request so how do we think about this piece of it.

Also, in my mind the one that is the most tricky is this business about choice and controls in the individual's hand. This is something that we need to be, especially for something like a tool, has to be really, really clear. Like when is it that we actually think that individuals are going to apply controls or choice because that is a specific activity. That's a request where you're either getting implied or expressed affirmation or acknowledgement or consent or whatever you want to call it. There has to be thought about what exactly that means because otherwise it is going to be very hard to deploy and measure.

MR. GEIGER: So, three, four, depending on how you count them, specific practices. One, an asset inventory. So, figuring out where the personal information is supposed to live, like where it's authorized to live and where it's not authorized to live. Because you do get a lot of companies that have personal information that are held in emails or external hard drives or a box and so forth. Second, setting controls on employees on essentially who on the inside has access to that information. So, who has administrative privileges, who has baseline access, those policies should be set and enforced.

Third/fourth is data protection. So, encryption, hashing, some sort of process rendering the data indecipherable, unreadable. The reason why you can split it up into two is because you've got data at rest and data at transit and there are different processes. We view those three/four as fundamental for privacy.

MR. VERDI: And I would say yes and to what Harley has said, there are also very complex and effective edifices depending on what the company's environment is and what their interaction is with outside parties that have to do with legal controls as well as technical controls around some of that data. So, it's not just the question of how is that data obfuscated or who has administrative rights on this particular system but also what are the kind of legal commitments that follow that data to try to mitigate risk as it moves through its life cycle.

I think that one of the things that has emerged over the past five to ten years has been this concept of privacy obligations traveling with the data rather than the data simply going out there and finding its way into the world and growing wings and going off and becoming its best self. We hope it's its best self but at the same time we hope it does so consistent with the privacy protections and the expectations that were attached at the beginning.

MS. STRICKLAND: This is why a conversation about privacy risk is so important. Because first of all, that scopes the whole activity but if you don't do that, then you have things like, well here's the way you have to approach it. I don't think that's necessarily what we should be doing here as an example. Things around where is your PI; a map is one way but it's not the only way to solve whatever the risk happens to be. I know a lot of companies have a different opinion about how do you tackle that risk. So, once you define the risk, you can say here are the different ways you can address that that will mitigate the risk without saying you must do this, you must do that.

MS. LEFKOVITZ: Okay so I am going to open this up to the audience who may have some questions.

MS. FAZZLE: Thank you. I'm Marina Fazel, an Afghan American journalist. I wondered if you could please tie up all of your fascinating insights about this very complex arena for mutual future. To bring it back to the U.S. elections, how would you rate the performance for electoral systems. How safe are they before the November elections?

Also, you've talked about how the different sectors come together or we would wish for them to come together, if we still in a planet where the different nations compete openly for resources and other things. If an election gets hacked, is there a little bit of non-aligned wishes here? How can we expect laws to emerge globally that would actually ensure for all global citizens that their privacy can be protected when on the level of this potential breech to our electoral laws we could go on forever before we get to the bottom of whether or not a breech happened? Was it a small player or was it a new era of political competition? Thank you.

MS. LEFKOVITZ: If you want to speak from the SEER to CSF point of view, that's fine too. Maybe just how does the framework sort of help support improved

security and privacy.

MR. VERDI: Sure. I'll just say, I mean the core of that question seemed to be elections. I'm not an elections security expert. The people who are tell me paper ballots, physical security, full stop.

MS. LEFKOVITZ: Now that that's answered.

MR. GEIGER: That was largely a cyber security question as opposed to a privacy question. I think that maybe that's why Naomi referenced the Cyber Security Framework. I think that it's important not to conflate the two.

One way that you can be within the security privacy diagram is if we're talking about hacking confidential voter information which certainly would be catastrophic for trust. But I think that hopefully the 2016 elections and the controversy surrounding it, regardless of whether or not you believe that there was, in fact, a cyber security breech, there has certainly been plenty of controversy. It has gotten the attention of state, local election officials who already do care about the integrity of their systems.

I think that it would be very difficult to just generally grade such a diverse and decentralized set of operators. In some ways, the decentralization is a strength because it is difficult to impact something systemically because it is so decentralized and because a lot of the systems end up being quite different from each other. I think that the cyber security framework, in particular, probably more than the privacy framework would be a very valuable tool for election officials to use in shoring up their systems. Not just voting machines, there is a lot of attention paid to voting machines, but also their backend infrastructure.

As John said, I think there has been a lot of consensus around the use of physical voting systems as opposed to electronic. I don't know whether or not that's the world we're moving into but it certainly the world I hope to see, personally.

MS. NEWTON: Good morning, Elaine Newton with Oracle. I wanted to comment that this panel has talked a lot about individual privacy and in the write up it's talking about benefits to individuals by protecting personal data. As we heard this morning and I'm sure is on everyone's minds, there is societal aspects to this. I was wondering if I could get your reactions to the framework covering not just personal privacy but harm to that can happen to society and if you think that's too broad a scope for the framework.

MR. VERDI: So yeah. So, one of our very smart lawyers at FPF put out a document a few months ago related to harms and mitigation strategies around some algorithmic decision making. It is not comprehensive to the issues that a privacy framework might cover but it is a big part of it as folks move to algorithms to process data more robustly. It actually splits those risks and those mitigation strategies into exactly those buckets. Risk to individuals, risk to communities, risk to society in general and, of course, the counter veiling benefits. The benefits to individuals, the benefits to communities and the benefits to society.

I think that's a critically important decision to make and I hope it is something that the privacy framework reflects. In the same way that I think the cyber security framework applies to not just personal data but it also applies to corporate data and secrets and confidential information and stuff like that. It applies to individuals and organizations and non-profits and government agencies. I think we probably want to have a broad scope here for what the real privacy risks are and what the real privacy benefits are in all those categories.

MS. STRICKLAND: Yeah, I agree. I think that that's what we've been talking about which is how do companies and agencies and other people will be using the tools and think through it. In terms of not just the impact to the organization itself but the

impact of the individuals and to the larger community. I think one thing that comes from these is we've done some privacy impact assessments is we've always had these conversations about risk versus benefit like they're two different things, you've got to balance them out. That in some degree is true but also you can mitigate some risk.

You could say, well if I don't need to collect this data, I don't need it to achieve the benefit or we can make sure that there are controls around it so that it won't be used by people downstream who don't know what the original purpose was. So, there are controls that you can put in place that mitigate the risk, get those benefits that can avoid this sort of like it's either or. I think we all think that's how it should work.

MR. WEITZEL: Dave Weitzel from Miter, Olson, American Bar Association Privacy and Computer Crime Committee. I want to speak in praise of connective tissues and interfaces. Especially from the CSF, we go five, we go about 30 and then we go down to 108 subcategories. What that does is connect the C Suite to the geek suite. Now we're going to need interfaces and how are we going to manage them between the cyber security framework and what is this. So, how do we get that connective tissue from risk analyst down to the geeks and then from the privacy folks over to the information security folks.

MR. GEIGER: NIST has already started that very process with the risk management framework for security and privacy. It was updated in May 2018 and it has a number of privacy controls. It is not formatted the same way that the cyber security framework is but part of the update was listing the specific controls in the cybersecurity framework that map to the risk management framework for privacy. There is a fair amount of overlap.

To your point about the taxonomy of the branch effect, it was down to the specific controls so that the geek suite would be able to reference the two very easily.

I'm not sure if that type of overlap is appropriate for the first draft of a privacy framework but I do think it will certainly be useful in further iterations because of the close similarities between the two.

MR. GAY: I'd have to agree with that. On the transportation side they're going to have the same questions. They're going to say okay, well we've got this profile from the CSF, how does this relate to what you're doing on the privacy side. We know they're related but in a lot of cases, the folks we work with are either cyber experts and aren't privacy experts, they're at the local state and transportation layer and they're asking a lot of questions about what should we do. So, I think having an easy to explain way to link those two and explain why we're suggesting that they should look into these is important for the work you're doing on the framework.

MS. STRICKLAND: It's another reason why it's good that NIST is in space because they can be expert in both and help that. Because there is that bridge that needs to happen and there are a lot of people, at least in my companies, who want to be able to understand and do both.

QUESTIONER: Just to go back a question and go back to the question of risk a little bit more. Because the first panel did identify those three categories, the organization, the individual and society. When you're all talking about risk are you talking about anyone of those or all of them together. When you talk about the middle one, I actually perceive that as having three subcategories. The risk to the specific individual user, the risk to the average user or the risk to the marginalized user, the person who has maybe a little bit more risk because of some aspect. The first one being clearly the hardest one to measure, the last one probably being the most important.

How would you get to being able to measure that risk because I don't think we can do that right now, especially not at scale. How do we maybe move a little bit further in

that direction and what is needed in order to get there.

MS. BEHRENS: So, I can take a stab. Actually, I have a little bit of a piggyback on the last one. One of the things that I think NIST has done with publishing, for example, the NIST 862 and their methodology really articulates the need for the discipline of privacy engineering. I think that's a big way to make that translation between the C suite and the geek suite if you have people who can actually articulate privacy and the technology stocks not just the policy which is traditionally where its lived.

So, being able to get with the engineers and the back-end doves and those guys and be able to sit down and articulate privacy in those controls, I think is very important that it can be carried up to the policy level and the macro level. I think that gets to your point, often times I come in and work with organizations.

So, I get seated, as much as I try to tell them I'm not security, I've been thrown into the security world so I've learned it by fire. I get seated with SSO's and CPO's to help at that strategic level but my passion is actually privacy engineering and I learned it because of this woman because she put me on a pilot and then through me in and said do this.

So, one of the things that I often work with clients is when they call me in to help them build out their technology solutions or do assessments is they're almost always focused on themselves as the organization. Using the pram methodology, for example, or probably what I'm hoping is going to come out of this framework is in privacy engineering discipline it forces you and, in my role, I advocate for the thought and considerations about the individual throughout the system. But them also the societal and cultural impacts. Not only on the individuals and users who are using those and in my first career I was a foster care social worker for 15 years.

So, I'm constantly thinking about the vulnerable populations and that was how

privacy made my natural crosswalk, in my brain anyway, to protect the vulnerable populations information. But you start in the privacy engineering discipline really invoking that thoughtfulness and consideration about how individuals and cultural entities in society is going to be implicated by privacy that is either being enhanced or revoked through the systems. And then it is your job as the trained privacy practitioner to articulate that into the work with the people who are developing your systems but then also the higher-level stakeholders that are then in charge of making business decisions. Navigating that balance between when do we invoke privacy controls and we need to satisfy the business (inaudible) so we're going to assume this risk.

So, I think that's one of the things that I've really enjoyed and certainly my work with Naomi. I reach out to her every so often and I'm like tell me something new about this. It's because this is what's pushing the privacy profession forward. We're not getting left in the dust anymore, we're starting to get budgets and resource allocations and have important sessions like this because we're starting to understand how to control for the risk, not of just organizations for privacy but those individuals and society. It's not easy and it is usually a constant reminder feedback loop that I have to engage with that great, we can do an assessment for this.

The other interesting side of that is the workforce members of that organization often get left in the dust also when organizations are looking at their privacy profiles. They think about what is the product or what is the service I'm offering, they don't think about, with the birthday thing, they don't think how their workforce are impacted by the privacy decisions they're choosing to develop in their solutions. So, it's a constant conversation and a session to remind. Having those individuals who are trained and educated and are part of a professional organization like IUPP or some greater organization, that you can learn how to utilize those tools is going to you to more

of the focus and shift off of just organizations or corporations but also to the individuals and society.

MS. LEFKOVITZ: So, I'm going to let our panelists have and John, maybe you can wrap this in because I know you wanted to have a conversation about this too, have one final word. So, just maybe talk about any other challenges, how can we measure outcomes, how are we going to measure the outcome of this framework, create incentives. So, just give us a last word.

MR. VERDI: Sure. So, very briefly on incentives, I think that this is one of the areas where the framework can interact with the legislative whether state or federal or any of the other proposals that are out there. The truth is that the Cyber Security Framework is succeeding for a variety of reasons. The quality of the framework itself, stakeholder buy in, the process by which folks got there, but it is also succeeding because of incentives. When you have federal agencies using the framework and speaking that language and holding federal contractors to certain obligations that creates incentives.

I think in the privacy framework, we're going to need to figure out a way, either through state or federal law, that doesn't exist today to bring some incentives to bear for uptake on this. We could have the greatest product in the world, we could have stakeholder buy in but if the incentives aren't there it becomes more challenging to sell within organizations.

MS. STRICKLAND: So, was your question incentives or outcomes or both?

MS. LEFKOVITZ: Both, I think any last word.

MS. STRICKLAND: Okay. What is our goal and what do we want to achieve. I do think that the space has really improved in terms of how do we do metrics

and reporting are some of the key features of a program and how can you show that it's actually working. I think that's what we're trying to do at large here, not just within a company but what does it mean. I think it will be when we can have some way of demonstrating all the work that's really going on in this space, how do we do that and what does that look like in terms of what you articulate to the public.

And then also, having less unanswered questions in the press about how do we deal with this, how do we deal with that. I'm like well, we've got these frameworks and approaches, they make sense. They do work on a global stage. There are areas where we can demonstrate some really forward-looking ways in thinking about privacy that can be useful for the rest of the world. So, I think that's really going to be what shows the success of these efforts.

MR. GEIGER: I think I would concur largely with what John said. There are, and we were joking about it at the outset of this event about the number of privacy principles and number of privacy frameworks that are out there. They've been around for a very long time and there are real questions about what is different this time. NIST has produced a lot of documentation on privacy controls and privacy.

I suspect that the controls that have come before are not going to be that different from the controls that ultimately make it into a privacy framework. You could write it probably by the end of the week and have it polished up and formatted by Halloween but the process is different this time. It's a multi stakeholder process, it's a yearlong process. It will involve workshops and public comment. Not that different from some of the work that came before also. A lot of the privacy frameworks that have come before also had public comment. There were also workshops for a lot of the big ones.

I'm hoping that this time and where the conversation seems to, particularly in the private sector, seems to have moved to a place where there is greater acceptance.

Perhaps that we need to do something nationwide on privacy in part because of forcing functions like GDPR and California. That this framework will ride that momentum in the format of the fact that it is a multi-stakeholder process will lead to something that is more easily useable, understandable for implementation for a wide variety of organizations. But I agree with John that without incentives in place, this could die on the landscape like so many other privacy efforts before it. And measuring adoption is, particularly in the absence of incentives, I think will be one of the challenges that the privacy framework faces.

MR. GAY: I would just say I really applaud the effort. I hope that it does take into account, all the diverse stakeholders out there. The diverse sectors, transportation has a lot of diverse users from public safety and first responders to private citizens through mobility, providers and shared services, state assets even and public transit agencies. So, finding something that will be able to be customized and address the needs of those diverse users, I think, is important to ensure adoption of it. Because if they can't really differentiate between those it is going to be hard for state and local agencies to use it to address the challenges.

MS. BEHRENS: I just would reiterate everything that my colleagues up here have said and again, express appreciation for participating on this panel. Towards the Brookings Institution, I think this is a great vehicle that NIST is building in order to help organizations of all types figure out how to negotiate risk as well as organizational business decisions that's grounded in some semblance of a cohesive framework. I'm really excited to see this move forward.

MS. LEFKOVITZ: Great. I'm going to thank you and thank Brookings and thank everybody here. I know we started with, it's complicated, but I actually think we started a good conversation to figuring it out. I look forward to seeing everybody

participating as we go forward with this. Thank you.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020