

Center for Strategic and International Studies

TRANSCRIPT
CSIS Event

“A Conversation on the NIST Privacy Framework”

RECORDING DATE
Wednesday, February 19, 2020

WELCOME AND OPENING REMARKS

John J. Hamre,
President and CEO, CSIS

KEYNOTE SPEAKER

Walter Copan,
*Undersecretary for Standards and Technology, U.S. Department of Commerce;
Director, National Institute of Standards and Technology (NIST)*

PANEL SPEAKERS

Chris Calabrese,
Interim Co-CEO, Vice President for Policy, CDT

Naomi Lefkowitz,
Senior Privacy Policy Advisor, NIST

Michael Cronin,
Vice President for Ethics and Policy, IBM

Jason Matusow,
General Manager for Corporate Standards Group, Microsoft

MODERATOR

James A. Lewis,
Senior Vice President and Director, Technology Policy Program, CSIS

Transcript by superiortranscripts.com

JOHN HAMRE:

Good afternoon, everybody. My name is John Hamre. I want to welcome you. I'm the president here at CSIS.

And when we have events, public events like this, we always start with a little safety announcement. I am responsible for your safety today, so if we have an emergency – we haven't had one. We've been here seven years. We've not had one. But sadly, we're living in a time when goofy things happen, and so if something does happen we'll hear a voice and I will ask you to follow my directions. We'll go out this exit over here or we can use this one. This is the one that's closest to the stairs that'll take us down to the first floor. We'll go out to the exit in the alley; we'll make two left-hand turns, a right-hand turn; we'll go over to National Geographic, and I'll buy everybody a ticket to see the Jane Goodall – the evolution of Jane Goodall show. It's really pretty good. You know, you'll enjoy it. Nothing's going to happen, but please be ready in case we do have to do something.

This is a – it's a real personal privilege for me to welcome Dr. Walt Copan here today. Walt is the head of NIST. I would guess it's probably a little bit different crowd. You probably know what NIST is, you know? But an awful lot of Americans have never heard of it. And since there is a television camera back there, I'm going to give them just a little bit of background.

You know – and it traces back to the very founding of the country. When George Washington is first – delivered his first message to the Congress, one of the things he said we need to do is to establish a regular system of weights and measures. Well, if you're going to buy a pound of nails from New York and have them shipped to Virginia to build something, you want to know it weighs the same, you know? Or if you're going to sell a gallon of grain alcohol, and you want to take it to Pennsylvania, you want to make sure that you're getting the same volume. I mean, it's a pretty natural thing. If you're trying to take 13 different states, and they were considering themselves sovereign at that time, and turn them into one nation, you needed to have a normal framework for commerce. And of course, that was the starting point for NIST.

You have – you don't realize it. Probably 30 times today each of you have been touched by something NIST has done. You know, something that's been important, establishment of standards that make your life better, safer. You know, the fire-retardant standards that are put in cars, for example. This is all foundational. And NIST does that. It's a real gem. NIST is an unusual organization in that – especially for Washington – because in NIST they don't really care if they get any credit, you know? They just want to get good things done. And that's the reverse of Washington, you know? (Laughs.) Everybody here – they don't care if they get anything done, they just want to have all the credit. So this is an unusual organization.

And they stepped into a very important role. And that is to deal with a great question unresolved in America right now. And that's privacy. You know, all Americans have two demands. They want the government to protect them and they want to be protected from the government – everybody. This is in our nature, you know? And so we've been confounded to develop a real coherent strategy for privacy in this country. NIST decided to step into the breach, and with a different philosophy, which is to say: I cannot reconcile these two competing goals, but we can hold up and develop – we can

develop and then hold up the highest standards, and encourage our best companies to aspire to it – lifting us all up.

And I think that what we're going to hear today is some insight into that, and what does it mean for us. So it's a very, very important session today. NIST is doing for the country things that right now our politicians can't do themselves. And we're lucky to have this organization taking the lead for all of us. So could ask you, with your very warm applause, welcome to the stage Dr. Walt Copan, who's the director of NIST. (Applause.)

WALTER COPAN:

John, thank you so much for your kind words. Thank you all for being here. I'm grateful to the Center for Strategic and International Studies for their hosting this event, this conversation today. And we are thrilled, indeed, to be talking about one of the key initiatives for building a stronger foundation of trust in technology, products, and services in the United States and globally. And we believe that the Privacy Framework now issued as version 1.0 has the potential to shape not just individual organizations, but to shape the approach to consumer privacy in the United States and internationally.

It can be easy to dismiss privacy as simply a cybersecurity issue. And certainly we know that cybersecurity and privacy are interlinked. However, privacy is much more. Privacy issues don't just arise from data breaches. For example, data collection for business purposes, such as smart meters, fitness trackers, your cellphone, could leave people feeling like they're giving away too much information, ultimately making them just reluctant to use a product or service.

The impact of a privacy incident can be devastating to an individual. They could suffer embarrassment, discrimination, or economic loss. And it can also be devastating to the organization that fails to protect that privacy, whether it's governmental or otherwise, in terms of reputation and, in the case of a company, genuine business loss. A Privacy Framework lead, Naomi Lefkowitz, from whom you'll be hearing a little bit later today in today's panel, likes to remind people that if you violate a customer's privacy but assure them that you are compliant with all relevant laws, they'll still probably be very, very angry with you.

NIST, of course, is a nonregulatory federal institute rooted in research and measurement science and standards, as John said, going back to the foundation of our country and so our focus is not on developing laws. This framework is actually intended to be agnostic to any particular law or regulation. But it can help organizations create the building blocks for the privacy outcomes that they want so they can meet their privacy obligations to their customers, boards, or regulators.

The approach in the Privacy Framework reflects our mission to work with industry and to support innovation. NIST has an incredibly broad portfolio of responsibilities including everything from building the world's best atomic clocks, including those that are synchronizing your mobile devices right now, to developing the standards for robotics and manufacturing systems to helping firefighters predict the behavior of wildfires, and so much more.

A challenge that we face in all of our R&D efforts is to be truly effective we must anticipate the measurement and standards needs of science, technology, and commerce. As we look constantly to the future, even as the pace of change accelerates, we at NIST have an obligation to America to be at the leading edge. In our cybersecurity and privacy work we find it's best to keep an open mind to possible solutions and approach each task with respect for all stakeholders.

NIST also brings our expertise and perspectives to the table to this entire process of framework development. It means that we consult early and often with the public and private sectors because we know that we need their inputs on how we select and implement broad programs and specific projects, and it includes both formal as well as informal consultation so that we can have regular reality checks along the way.

NIST, as an institute, is highly trusted within the United States and globally as committed to transparency, traceability, and openness in the development and the application of all our work. We know that the kinds of collaborations such as those to develop the Privacy Framework result in higher quality, more appropriate, and more useful products and services and that these collaborations themselves create buy-in for adoption by the community of practice.

We know that they help cultivate trust among those like you who are depending on the work of NIST. The Privacy Framework is a good example of this approach, which utilizes a multifactor approach and facing a broad and multifaceted issue that matters to all of us as individuals requires us all to help solve it. We all have a role in protecting privacy whether we're in the public or the private sector. Whether we're lawyers or engineers or senior executives, we own this. But with so many aspects to privacy and so much attention on it these days, we face a daunting challenge to find more consistent ways to communicate about it. Just developing a common lexicon is essential.

That's why a diversity of perspectives in the United States and abroad has been so critical to the development of the NIST Privacy Framework. We sought to bring that diversity into a shared lexicon and practical toolkit that establishes privacy as a key component of enterprise risk management. It is a tool for aspirational performance and not a checkbox exercise.

And at NIST, when it comes to cybersecurity, we actually spend a lot of time talking about risk and we've been pleased to observe amid the sea of worrisome news about threats, vulnerabilities, and breaches that cybersecurity risks are no longer considered the domain of the IT specialist or cybersecurity professional alone. Cybersecurity risk-management issues are becoming increasingly familiar topics at C-suites and at boardrooms. It's true for businesses and it's true for federal and other public sector entities.

At NIST, risk management is a common thread through many of our activities and we understand that it's pretty much impossible and, certainly, impractical to eliminate entirely the cybersecurity risks that organizations face every day. That's why organizations hire risk managers and not risk eliminators. With that in mind, we aim to develop and deliver technological and organizational tools and solutions to help understand and manage risks.

Historically, this has been around two frameworks that we've developed for cybersecurity risk management. You may be familiar. Initially developed with a focus on critical infrastructure, the NIST Cybersecurity Framework has become popular in the five years since it was first produced both across the United States and around the world. Hardly a week goes by where we don't hear from someone about yet another Cybersecurity Framework use case, whether from large organizations, technology companies, financial institutions, entrepreneurs, or from even other governments.

The key to that framework's success has been the active engagement of the private and public sectors in the beginning of the development process through to today. That development process brought up many questions about privacy risks in an increasingly connected, data-fueled world. And at risk – at NIST we began to ask ourselves whether the risk-based approach that we took in cybersecurity could work for privacy. The question spurred the launch of NIST Privacy Engineering Program, and it focused on understanding how a risk-based approach could help organizations make better decisions, and more effectively integrate privacy needs into their products and services, and look after the needs of their customers – the individuals that they serve.

Getting privacy right will underpin the use of technologies in the future, including AI and biometrics, quantum computing, the Internet of Things, and personalized medicine. And these technologies all will be a big part of our future. According to one industry estimate, the biometrics market alone will be worth more than \$59 billion by 2025.

And of course it's not just about the dollar value, is it? There's the genuine value to the human spirit of living in a free and democratic society. Getting privacy right means enjoying the benefits of innovative products while upholding our country's founding values.

Back in the summer of 2018 major privacy breaches and multiplying laws and regulations around the world dominated the news. Fairly quickly, NIST heard from industry stakeholders – and IBM was a leader in these conversations – asking whether we could replicate the success of the Cybersecurity Framework for privacy.

Before we could figure that out we needed to learn more from the community of stakeholders, so we issued a formal government request for information – RFI – and the results were absolutely essential for our next steps. We heard that compatibility with existing laws, regulations, frameworks, and standards is extremely important, and depending on the sector and the mission objectives that organizations must already comply with multiple internal policies and external regulations. So the framework had to address this head on.

Stakeholders also made it clear that they wanted a framework that was at least compatible with what they were already working toward, and ideally would facilitate not only the compliance process but organizational excellence.

Our stakeholders also confirmed that they wanted a framework that would be risk-based and focused on outcomes. An outcome-focused approach would allow the

organizations to innovate, to refocus their resources on where it made the most sense for their privacy practices and business operations.

We heard from organizations genuinely invested in protecting individuals' privacy beyond simply complying with regulations. They wanted a tool that could support their organizational goals and aspirations, and ultimately to build the kind of culture of awareness in security and privacy.

Likewise, multiple organizations told us very clearly, very forcefully in some cases, that they needed a flexible tool – something that could identify and manage privacy risks to individuals in the context of their specific organization, their privacy posture, business objectives, and with customers.

So as a result, the Privacy Framework is not a checklist of requirements. It's a tool to allow organizations to prioritize, to design the most effective privacy solutions for their business environment and for their customers' needs.

Just as with the NIST Cybersecurity Framework, they said that the key value of the Privacy Framework should be the extent to which it can foster communications within and between organizations. They told us they'd like a framework that could help them to communicate with privacy professionals, non-privacy professionals; get cybersecurity professionals and privacy professionals actually really working together; and with five simple words – identify, govern, control, communicate, and protect – that the organizations can quickly convey how they are managing data to minimize privacy risks.

NIST itself had a larger goal, to bring privacy into greater parity with security considerations, which goes well beyond the Privacy Framework itself. For example, we are revising NIST Special Publication 800-53, which is security and privacy controls for information systems and organizations. In its fifth version, privacy controls are actually fully integrated into the set of the security control catalogue, creating and consolidating a unified set of controls for information systems and organizations.

As I've been reminding this team, despite the sprint to get to this point, we are truly only at the beginning of our privacy-framework journey. Now that we have a completed version 1.0 in the hands of the people for whom it was developed, we want to work collaboratively to further understand how organizations are using the framework, how they are seeing the value of use cases, and ultimately what lessons we can learn, what our next steps should be to continue to advance this work so that it could evolve to meet the needs of stakeholders.

We encourage you all to contribute to our online repository of resources as well. It includes framework correlations with key privacy laws, regulations and standards, as well as common profiles, guidance and best-practice tools to help organizations better use and implement the framework with benchmarks.

Our new online privacy engineering collaboration space is going to allow us to keep these conversations going also. In the public online venue that this has been representing, practitioners can discover, share, discuss and improve upon open-source tools, solutions and processes that support privacy engineering and risk management.

In providing all this openly available, our goal is to encourage the development of more effective and accessible solutions to help organizations achieve their privacy objectives and to implement better privacy protections for individuals.

When we developed the Privacy Framework together, we also developed a companion roadmap that describes the key challenges to achieving privacy objectives. These challenges are going to drive our continued focus and further research-and-development thrust, advances, the evolution of the framework, promotes a well-functioning data-processing ecosystem, and to expand the body of standards, guidance, practices and tools that support privacy risk management.

Two of the initiatives that we're working on in the collaboration space include de-identification, such as differential privacy techniques and privacy risk-assessment approaches. We're also following the model of Cybersecurity Framework by considering supporting materials that we can develop with stakeholders to provide further clarity on how to use the Privacy Framework.

So I'm excited to announce today one such project, which is a guide to help small and medium-size businesses build in privacy as they seek to become the trusted big businesses of the future.

Over the next few months, we'll be reaching out to these innovative smaller companies, with their resource constraints understood, to better have a sense of how the Privacy Framework could help enhance their work and their operations.

So again, I'm very, very grateful to the many stakeholders that have joined with us in this journey, who have taken time to work with NIST and the broad stakeholder community over the past couple of years. And I look forward to hearing from some of those today who are already adopting the Privacy Framework. There have been some announcements made, including from governmental organizations, about their commitment to the use of the Privacy Framework.

And we all know that the benefits of the framework are only going to be realized once organizations actually start to use it, to put in practice and to move their organization cultures forward with this as a guide. And that's why I want to encourage all of you to review the framework, spend some time to understand it, work with NIST in helping apply it to your business or organizational situation, and also to demonstrate privacy leadership by becoming early adopters.

So, once again, we're at the beginning of the journey. It was only issued last month. A tool is only as good as the results that it creates. And our focus is on the outcomes, ultimately that will be generated by the Privacy Framework. We want it to be an essential part of every organization's toolkit for success in the United States and abroad. And we're delighted at the place where we are today.

Thank you to CSIS for hosting this event, for your leadership for the nation in our seeking for appropriate policy solutions for the future. And we look forward to working with all of you to achieve the great goals of the Privacy Framework.

Thanks so much. (Applause.)

JAMES LEWIS: Thank you, Walt. I think we have time for a couple questions if they're nice questions. (Laughter.) But do we have any questions in the audience? No? Go ahead, please. And could you please identify yourself?

Q: Sure. So my name is Ainga (ph). I'm with Hong Kong Phoenix Television.

So I'm just curious, will this framework that you're suggesting have some effects and relates to U.S.-China trade relations?

MR. LEWIS: So would you actually mind repeating the question so that we can all hear that?

Q: Oh, OK. So my name's Ainga (ph). I'm with Hong Kong Phoenix Television.

So I'm just – thanks for the wonderful speech. So I'm just curious if the framework that you suggested might have some impact on the U.S.-China trade relations.

DR. COPAN: Thank you so much for that question about trade relations between the United States and other nations, including China. Our goal is to really utilize these types of tools to open up positive dialogue. And so whether it's with China, whether it's with Europe, whether it's with other parts of Asia, and other nations of the world, we do believe it's a tool to develop common understanding, a common language around privacy expectations. And we trust that that will result in positive relationships to ensue, as well as a combined approach to address the challenges that we all face globally, recognizing that different nations around the world have different perspectives on matters of individual and other privacy challenges. But this is a toolkit to allow us to actually get to a common understanding so that we can achieve common goals. Thank you.

MR. LEWIS: Others? Yes, this is your big chance. I can't believe you're not taking it.

DR. COPAN: The panel is coming.

MR. LEWIS: All right, great. Well, please join me in thanking Walter Copan, please. (Applause.)

DR. COPAN: The panel's going to get the rough question. Great, thank you. Thanks for being kind.

MR. LEWIS: Could I ask the panelists to come up?

My name's Jim Lewis. I work at CSIS. Let me introduce the panel. We'll have them each talk for a bit. I'll ask a couple questions. And then we'll give you a second chance of asking questions. So start thinking of them now.

To my left is Chris Calabrese, who is – his real title – he used to be the vice president for policy, but you're now the interim co-CEO, is that right?

CHRIS CALABRESE: That's right.

MR. LEWIS: Got it right. At CDT, while they go through their executive search. So, Chris – I was telling Chris when he came in that when we sort of unanimously, when we went through who we want to have speak, he was – he was at the top of the list here.

MR. CALABRESE: Oh, that's very nice.

MR. LEWIS: So to his left is Jason Matusow, who's the general manager for a corporate standards group at Microsoft. We're very grateful for Jason for showing up and doing this. He's got a lot of responsibilities under his hat, including some with China. So you may get a chance to talk about the China question.

To Jason's left is another old friend, Naomi Lefkowitz, who's the senior privacy policy advisor and the lead for the Privacy Framework. So if you have mean questions send them right there. (Laughter.) Naomi's done tremendous work in helping shape the whole process here of how we approach cybersecurity, privacy, a lot of the things that NIST has made tremendous progress in. And last, but not least – that was an old one, wasn't it – Michael Cronin, who's the vice president of ethics and policy in IBM's chief privacy office. So he focuses particularly on AI and on privacy issues. We're grateful that he could come down and speak today.

What I was going to do is give each panelist a chance to make brief – I told them three to five minutes – brief remarks to open things, and then we'll go to some questions. So, Chris, should we start with you? Let's just go down the line.

MR. CALABRESE: Sure. Sounds great. I will try to be very brief and set a good example. So just for folks who don't know, the Center for Democracy in Technology is about a 25-year-old advocacy organization. We're focused on individual rights and putting the individuals' needs and rights at the center for the digital revolution. So that includes, obviously, a lot of work on privacy, data, free expression, and surveillance.

We've worked really closely with NIST on this framework. We're really excited that it's – you know, the first version of it has now been put forward. We think it's a really useful tool for coming to a common understanding about what we mean when we talk about privacy, what it means for a small or medium or big enterprise to actually go through a process of weighing privacy risks. And we think it lays out a really useful framework for doing that.

There's a couple of things that I think we all need to keep in the center of our mind. The first is that this is a tool. It's only going to be as good as the person wielding the hammer or the screwdriver, right? If a company is a good company that wants to engage in good data practices, this tool will allow them to do a good job. If it's a company that just wants to sort of check a box, or worse, maybe would like to obscure practices that aren't good, this is not a magic fix; it's a voluntary process. So at the end of the day it's not a substitute for a legislative approach or a regulatory approach, but it is a very useful supplement.

I think the second thing is that there is a real benefit to consumers from doing this. There's a real benefit both to going through a Privacy Framework, but also a Cybersecurity Framework which NIST is really well-known for as well. Consumers benefit from strong, concrete understanding of how their data is used, and the only

way they can really get that is if the people who are holding their data have it and can communicate it to them. And so that's something that the NIST Cybersecurity – or excuse me, the NIST Privacy Framework spends a lot of time focusing on.

And then the last thing is that this is a real benefit for industry as well, not just for consumers, because – you don't have to trust CDT. You can go to a much more expensive source. Deloitte & Touche published their tech trends for 2020 and they said something that I think is really very smart, which was, every adoption of new technology is a chance to either gain or lose trust with a consumer. So every time you apply something, you have an opportunity to make a consumer happy and excited about a product or worried and not want to use your product. And really, that goes back to how you're using data and how you're applying privacy principles effectively. NIST has done a really – has made a really good start at helping companies do that well.

MR. LEWIS: Great. Thank you, Chris.

Jason.

JASON MATUSOW: All right. Well, to start with I'd like to just congratulate the NIST team on producing an excellent first document. Naomi, sitting here to my left, has been committed and deeply thoughtful for a long period of time. We greatly appreciate it. We also recognize the work of Adam Sedgwick, who led a(n) open and transparent process. And between the two of them, really the results show.

The Privacy Framework is valuable for organizations of all sizes as they seek to protect individuals' privacy rights, but also to be responsible stewards of data. We do believe that privacy is a fundamental right and the framework can provide a foundation of behaviors that lead to consumer trust, as was just mentioned, and which is critical to enabling advancements in innovations and data-driven technologies. We've long supported and sought to advance privacy protections both in our own technologies and through the development of laws, regulations, and standards globally, and the framework is yet another item in the toolbox that organizations are going to use.

I think there are a few key elements to highlight that are really positive here. First, the framework is forward-looking and it has been designed to be flexible such that emerging technology trends can be accounted for. Privacy is not a destination. People have said this about security for a long time. You have to carry that over into the privacy discussion as well. And certainly as new technologies come onto the market, new technologies bring about interesting dynamics to assess, the framework needs to evolve with them.

Second, during the workshop process there was consistent feedback from industry that the framework be interoperable with laws around the world. And that was achieved, and I think that's an enormously important outcome.

The third element that I would highlight is that the design goal for alignment with the Cybersecurity Framework was also met. Dr. Copan mentioned something that I think is really important. Our experience even within Microsoft, but we've certainly seen it with customer engagements around the world, is that security individuals and privacy individuals in companies frequently don't work well together in the sandbox, right?

You have some conflicting objectives and there is a sense of overlap that creates organizational tensions at time(s). Having these two frameworks so tightly linked together is a really practical outcome that helps achieve a more effective privacy practice.

And then, finally, the document recognizes the importance of mappings, what we would call internally; the Privacy Framework refers to them as crosswalks. But this idea that there are so many different privacy regimes out there; how do you line up the different requirements? How do you map one set of behaviors against another? And there's more work to be done on this. The framework has started with some – with some basic work and there are some items that I think need to be dealt with in the future.

So looking ahead, while many might wish to debate the relative merits of differing legislative and regulatory approaches, the practical truth is that any organization operating in multiple jurisdictions has to deal with mappings as a matter of course. To that end, NIST has created the Resource Portal – am I getting the name wrong?

NAOMI LEFKOVITZ: Repository.

MR. MATUSOW: Repository.

MS. LEFKOVITZ: (Laughs.)

MR. MATUSOW: I was so close. The Resource Repository. Microsoft will contribute mappings to ISO/IEC 27701, which is – sorry, standard geekery; it's the Privacy Information Management System – which is an international standard that is, we believe, important on the path to global certification harmonization. The framework is not a certifiable standard. It's not something where you would have a third party audit you against it in a way that some governments are looking at. If you're a particular follower, for example, of the GDPR, Article 42 would be the one that you would care about in this regard. But as we think about cross-border data movement, the importance of certification will be necessary.

And then, finally, we think it's important that work still needs to be done on in-depth guidance and thought around privacy risk assessment and balancing the idea of organizational risk against individual risk. And there's still room to grow. And that's the whole point of getting out there with a V.1, work with it, look at it, and think about how to improve it and head towards future versions.

So with that, I'll say thank you.

MR. LEWIS: Great, thank you.

Naomi, please.

MS. LEFKOVITZ: OK. Well, first of all I'd like to echo Walt's thanks for hosting us and all the kind words that everyone is saying. And you know, it's a tribute to your work that the framework turned out the way it did and your collaboration – you know, I mean, I think at NIST our

goal is to help organizations, and to be able to do that really makes it worth getting up in the morning for me.

But I was recently reading this law review article that was claiming that we're at a constitutional moment for privacy, which possibly is a slightly overused trope but, you know, I take the point, but – because I do think that we are a significant sort of technology and privacy inflection point with the advent of AI and machine learning. And we have this opportunity now to chart a course on privacy that can impact people and societies around the world for many years to come.

And I think that, you know, our views on privacy for the last few decades have been sort of, you know, originating from these early days of computer databases and this idea that you manage the individual's relationship with data and privacy will come. And I do think that managing data and people's choices with respect to that data is an important part of privacy protection, but I don't think it's sufficient. And so, you know, that's why the Privacy Framework is really founded on a risk-based approach to privacy protection.

And it's built around this model of understanding privacy risks – specifically, you know, the problems that people can experience arising from how systems and products and services process data. And understanding these risks can really allow organizations that build the technologies that shape our world, like the companies here, to make better decisions about protecting privacy when they're designing their products and services, before individuals ever even touch them.

And you know, so it's from this understanding that organizations then can use the Privacy Framework to consider the types of policies and capabilities that will be most effective in addressing the privacy risk specific to their business environment and specific to their product-development processes.

But I don't want to imply that as a community we shouldn't create norms or areas of no-go or moratoria on specific types of data processing. You know, we make those judgments in other areas all the time. But we do that based on a discussion of risk, not on sort of static proxies of one – you know, one-size-fits-all rules for everyone.

So the Privacy Framework is a tool for individual organizations, but it's also, we hope, a model for how we can shift this important and necessary conversation that we need to have around privacy and technology.

MR. LEWIS: Great, thank you.

Michael. Well, let me – I might want to come back to the process point, but Michael, please go ahead.

MICHAEL CRONIN: Well, I'm going to start with some more kind words for NIST. We, at IBM, strongly support the framework. We think it's a terrific tool that can be used for companies of any size throughout the world and the work that was done on it was just terrific. As I said, we strongly support it, and particularly in this day and age, you know, you don't have to look too far to find consumers and others are concerned about their privacy.

In fact, we commissioned a study recently that found that 71 percent of the respondents – it was U.S.- and EU-based people we polled and 71 percent of them rated data privacy concerns as the top-rated concern, tied with climate change. So it goes to show that this is an area that everybody is concerned about and tech companies should be concerned about it as well, obviously, because in order to stay in business and to do things you have to do it in a responsible way and you have to be concerned about privacy.

Now, the Privacy Framework came out at – couldn't have come at a better time, really. We know that things are fragmented, as people have talked about. There are laws all over the world, and the framework is great because it does several things. Jason alluded to it a little while ago. It's global in nature so it can interoperate with other laws, help you to comply with other laws.

It builds consumer trust through accountability and it's accountability through the entire organization from the senior management all the way down to the operational level. And then it's also simple. It's easy to actually apply, and that means you don't have to change your operational models and so forth. You can overlay it and incorporate it into it.

There's another thing that I would mention, too, that I think is important and it's – the NIST Framework can't do this.

The framework will only work if you have the skills in which to operate it. And so to that extent, one of the things that I think is important in the whole area of privacy – cyber is true as well; AI is another area – is having a – building skills and that's skills around the world to be able to do these new jobs, do the risk assessments, do the mapping and so forth.

And IBM has always been a very strong advocate of creating new skills in these areas, of helping to build and advocating others to do the same, and that is an area I think that not only it's building skills, finding ways to hire people with those skills, changing the model of how we educate people. So that's – and what NIST is doing as part of their roadmap that Walter had mentioned earlier, they're going to work with NICE on the skills area to try to come up with sort of skills profiles that are necessary in the privacy world to work on the framework and in other areas, a taxonomy for describing exactly what privacy is and so forth. And we applaud that and we'd be happy to help in any way we can in terms of – in terms of working on that with you. But that's another area that we think is very, very critical.

And then, finally, I would say that, you know – it was mentioned before – we believe that all companies, particularly technology companies, have a responsibility to create products that protect privacy, that protects, you know, help with cyber and so forth. IBM is – they're built into our DNA. We've always been doing that. It's an ethical underpinning in addition to compliance.

We think that's critical. Companies will not stay long in the world, we think, if in fact they don't pay attention to these areas, not only because the laws may comply it – may apply – may require you to comply, but also it breeds trust and trust is the thing that

keeps companies' customers coming back to customers – to companies and, of course, it's the right thing to do.

The last thing I will mention is that – is we think, we see the framework also helping to inform legislation as it comes through is that it's a great way – a great way of informing policymakers in governments to come up with legislation that uses that as sort of an underpinning to take into account. We, at IBM, support U.S.-based consumer legislation. We think it's necessary at this point in time to avoid any fragmentation and consumers don't and companies don't need multiple rules to deal with in order to comply with law. So having a single law that deals with that would be a wonderful thing to do, and we see NIST actually helping in that regard. So with that, I would just thank you for letting me be on the panel.

MR. LEWIS: Great. Legislation is actually my second question, so we'll wait to come back to that one. (Laughter.) But let me start by saying, could each of the panelists give us an idea of how they see the NIST framework mapping to GDPR? I mean, in many ways GDPR is the central iceberg in the privacy ocean. That's a weird metaphor. (Laughter.) How does it matter? Michael, do you want to start?

MR. CRONIN: Well, I can see it in two specific ways. One is that both GDPR and NIST are based on accountability. It's one thing. And secondly, it's a risk-based framework. So they actually work very well together because the – sort of the philosophy is the same, the underpinning philosophy's the same. And what the framework will allow you to do is to be able to do some of the how of how you comply with GDPR, to apply some of the things within your organization. It's not just GDPR. I think it will apply across the board for all laws that currently exist and will exist in the future.

MR. LEWIS: Chris then Jason, go ahead.

MR. CALABRESE: Well, I mean, I would just echo that in terms of the pragmatic nature of it. I mean, I think we hear a lot phrases like privacy by design. Well, this is – this is giving you a way to actually do that design work. And I think that's really powerful and important. There's also, I think, some – as we've already noted – some sort of impact assessments for high-risk situations, where you're going to have to do precisely this type of analysis under the GDPR. So again, it's a practical way to go and say: "All right, I've identified a high-risk potential privacy arm. How am I going to go about processing that within my organization, mitigating the potential harm, and grappling with it as sort of an institution?"

MR. LEWIS: Naomi.

MS. LEFKOVITZ: Sure. So we were just in Brussels, actually, talking about the framework. And we were talking to our counterparts, and commission, and so forth. And one of them asked – one of the gentlemen asked me, he's like, well, where is data minimization? Like, where does it say, you know, not to collect certain information? And I said, you know, it's not – we're not – we're replete with principles. Everybody knows the principles. What we're doing is providing sort of the policies, and the capabilities as building blocks that help you get the data minimization. And you know, we can let, you know, the principles stand, and they're well-understood. We fit underneath.

MR. LEWIS: Great. Jason.

MR. MATUSOW: So I think that a point was made earlier that is important to keep in mind, that the framework is a starting place for organizations that already have a desire to achieve privacy. The GDPR is a prescriptive regulation that says there are obligations on any organization for responsible data practices. And we actually endorse that quite strongly, the idea – and this was actually just said by my fellow panelist – that we are in a situation of consumers want to trust what's going on. They're going to not only – it's not about notice and consent anymore. It's going to have to be about – in a sense that organizations are under obligation to act responsibly as well.

What the framework does, is it allows for the mapping. And it's going to go right back to this crosswalk discussion. The importance of the mapping is to be able to say – something like data minimization would be a great example. There are explicit mentions of that in the GDPR. Guess what? There are also explicit mentions, but in a very different way, in the Australian privacy law. And if you have customers, or supply chain, or partners in both places and here in the United States, you are going to have to think about how do you address that same concept, but under different regulatory regimes? And the framework is going to give you a way to look at those in a flexible, forward-looking manner. And so I think that was as design principle of the framework.

I would also point back to the mapping that I just mentioned before. Something like an ISO standard, where you have 30-plus countries at the table, plus regulators, working on a document that established a set of controls that can act as a Rosetta Stone on a per line item basis across the regulatory regimes, and allows you then to up-level that into something like the framework, which is about turning it into a practical operating practices in a company. So I think that there are relationships, but I really think you need to be careful in separating the implications of a prescriptive law, which places obligations on organizations, and a framework, which is about voluntary good strong behaviors.

MR. LEWIS: Sometimes when you talk to people from the EU you get the – they're very pleased with GDPR. And they see it as a model for legislation in other countries. And I think I'm probably making this up, but I think one official told me that the California was probably GDPR's lovechild. (Laughter.) What – something like that. What does the framework say for American legislation? We can talk about, you can talk about, you know, what the chances are that we'll see legislation. I think it's inevitable, but when we look at the framework how does it shape that move towards what might a federal law at some point, probably in the next couple years.

Chris, do you want to start?

MR. CALABRESE: Sure. So I think that we – we are certainly very, very supportive of the federal baseline comprehensive privacy legislation in the United States. I think it's crucial, not just to protect consumers and to protect, you know, all the various uses of data, but also for companies to build trust and to allow a framework for innovation. So I think it is a good thing all the way around. This framework is both very useful to that process, and only has a limited role in it. So I'll speak to the limitation first.

As I kind of said at the outset, this does nothing – this framework does nothing about bad guys, bad actors of all sorts, right? They can continue to be bad actors. They could put their thumbs on the scale and weigh their risk assessment in a way that I think a lot of consumers wouldn't be comfortable with. So NIST is aware of that. It's – you know, and there's only so many things you can do with a voluntary process. At some point, we need laws and regulations that are going to set rules for everybody.

And that's where this framework I think has done a really good job of providing some guidance, because in fact there are some pretty clear and well-understood concepts in privacy law and regulation now. It is possible to pass regulation – or, to pass legislation that has limitations on how data is used or puts obligations on data holders as to how they're going to process it, that big entities are already grappling with. They're grappling with it as part of this framework. So we're not, in fact, sort of creating some new and onerous regime that no one has ever thought about before. But rather, merely creating a floor that the bad actors are going to have to get above. And I think that's a really crucial role.

So I hope that we'll see privacy legislation. Maybe not this year, but I do feel that in the next couple of years we have a real opportunity. It's something that is being discussed in a bipartisan way. It's being discussed in both chambers. And you know, and that's exciting. You really can't say that about a lot of things in Washington right now. So I think we're excited. We will be really interested to see the direction that it goes. Frankly, I've been really impressed over the two-plus years that this has really been discussed in this latest iteration in Washington, how sophisticated the discussion has gotten. It's about data processing controls, but it's also about harms, it's about civil rights, it's about the ways that this data is going to feed into artificial intelligence and machine learning.

So it really is a central conversation for how we are going to proceed with information technology over the rest of the century, honestly, the latticework that we're going to build. So I think it's an exciting time. And NIST is really helping to sort of set that piece of the latticework out here.

MR. LEWIS:

Before we go down the row, I wrote down something that I think you said in your introductory remarks, which is that it's not a substitute for a regulatory approach. Do you want to expound on that a little bit, then go to the others?

MR. CALABRESE:

Sure. I mean, all I would say is that you can't – regulation is not fundamentally about good guys. It's fundamentally about bad guys, right? The good guys – and the people on this stage are going to do good things. And I think they appreciate having a framework that helps them do that. But at the end of the day, Microsoft is going to come up – and IBM are going to come up with approaches that work, that benefit their users. Not everyone is like that. And I think it's crucial that we have penalties for people who don't want to use this or, frankly, maybe just need some convincing organizationally that this is somewhere they should spend resources, and something they should focus on, because in fact it's the law and they have compliance obligations.

And so that's what I mean. I mean, we're not going to – we're not going to – this isn't going to solve a privacy problem. What it's going to do is give us a pretty good sense

about some of the various issues that we're going to have to address. And then it's going to be up to the policymakers to enshrine those in law.

MR. LEWIS: Jason, please.

MR. MATUSOW: I'll be very quick on this. I largely agree with what's been said. You know, if you look at California, the California law does not place obligations on organizations. And we believe that there should be federal legislation that does that, for all the reasons that have already been stated. So I endorse what's been said and would reiterate the same.

MR. LEWIS: And you'd expect to see that, or you'd hope to see that, in some federal legislation?

MR. MATUSOW: We would hope to see that. We have been extremely active in California and in Washington State and, you know, the folks that are more deeply engaged with this than I. I'm on more of the practitioner side of the house. But the folks that are working on the policy side are deeply active on it.

MR. LEWIS: Was it you that said – we had a little lunch beforehand – was it you that said that you had similar thinking about data-breach laws? When California would be – it may not have been you then.

MR. MATUSOW: No, it was not me.

MR. LEWIS: California had a data-breach law a few years ago, and the idea was, well, you'll have federal preemption. And now that we've finally reached the milestone of having 50 state data-breach laws, we're still waiting for federal preemption. So it might be something to think about it, whether you – yeah, go ahead.

MS. LEFKOVITZ: So I think the thing that we say when our opinion is asked – (laughs) – is not to underestimate the power of process and the ability to have a consistent way to talk about privacy risk. I think that's done, you know, wonders for cybersecurity. Organizations may not assess threats in the same way or the impacts, but they are actually able to talk with each other because they have that same language around threats. And I think that's, you know, what we have been trying to do with the framework and as a model to how we can have a consistent conversation in privacy.

And, you know, on that point of process and on the point of the bad actors, which, you know, having, in my prior life, been at the FTC, there is certainly a spectrum of bad actors, from those who are outright fraudulent to those who are maybe, you know, legitimate but indifferent, perhaps, I guess you could say. (Laughter.)

And, you know, we were doing these grants with these pilots. And I would say that we had a spectrum – (laughs) – of grantees who ranged from very enthusiastic about privacy into those who, you know, thought they had it or, you know, maybe were a little more indifferent. And, you know, driving a privacy risk assessment methodology and a process with them, even with that sort of more indifferent organization, forced them to have this conversation. They actually learned some things. They came out. They identified some privacy risks they hadn't really thought about and were able to come up with solutions that they hadn't contemplated before. And I just – you know, it really taught me what the power of process is, so.

MR. LEWIS: Legitimate but indifferent may be the quote of day here.. (Laughter.) That one's hard to top.

Before we move on, you mentioned privacy, too, in your opening remarks. And one of the things, you know, I was thinking then is the NIST process, which has tremendous credibility. And you sound like you're talking more about the process within companies. Is that right? Do you want to talk a little more about process?

MS. LEFKOVITZ: Yeah. What I say about the Privacy Framework – I think people have been talking about this in different ways, that it's culture-building and it's developing processes because of the way we've structured it from – you know, starting with sort of identification of your data processing and then governance around the policies and the practices and the training of your workforce and, you know, working your way down through different capabilities and that – so you can have that conversation from the C suite down through policy and legal and business management and all the way down into the engineering.

You know, and we – you know, we actively put in things like, you know, establish privacy values; but not only establish them, because I hear lots of companies talk about privacy values. And then you look at their products and you're, like, what happened, right? (Laughter.) And so, you know, we actually said, all right, have privacy values. Now have processes to embed your privacy values in your products. And it's that kind of process that we think is so critical.

MR. LEWIS: Great. Thank you.

Michael, please.

MR. CRONIN: Yeah, I think there's – when it comes to legislation is that the – we believe it's important to have legislation in the United States to avoid the fragmentation or the confusion associated with – (inaudible) – legislation. But the issue really, I think, is having legislation that's balanced. You want to protect privacy. On the other hand, you don't want to chill technological advancement. And so getting that balance is important.

So prescriptive legislation tends to – you know, getting to the point of bad guys, do you get it so that you get that one bad guy who's going to do things all wrong, or is there something on the spectrum so that you're trying to get – prevent certain people and penalize them without putting too much burden on companies to either comply or to ultimately innovate. So that's the tricky area, I think, in that.

And the thing I would mention is I think there's room, if you have risk-based legislation, there's room for also the ethical systems in the frameworks like the Privacy Framework to guide people so it works hand in hand. So you've got the private sector and the public sector both achieving – you know, working together to achieve the same result, protecting and also protecting innovation.

MR. LEWIS: I'm glad you brought that up, because one of the things that's changed in the debate over, say, the last 10 years at least is that there's now a link between your privacy rules

and your ability to innovate. And that link might very well be the treatment of data. So it turns out, it is important what you do in privacy because it will affect future economic growth, future technological development.

Michael, I don't know if you want to add anything to that.

MR. CRONIN: No, I think that's absolutely right. It's – and it goes back to the – you have the consumers, government, and the companies. And they all have to work in concert. For the companies to stay in business, they have to have the trust of the consumers and the trust of the government, frankly, because they don't – if government doesn't trust technology sufficiently, they're going to overregulate.

So I think what it then comes down to is making sure that you have things like the framework. You have a culture that you build into your companies and to organizations so that they will do – most of the people or all the people will do the right thing. And that way you'll end up with the ability to continue to innovate, because you're not going to be spending a tremendous amount of money on compliance and/or be afraid of going into areas for fear that you'll fall foul of particular laws.

MR. LEWIS: One of the fundamental trades of the internet is you trade data for services, right. So to the extent you can, how will the framework affect that business model that underlies a lot of the commerce we see? So I can see Chris is looking skeptical. A good example: Google, right? You use Google. And we all use Google, right? You've got Google Maps. You've got Gmail. You've got Google Search. In exchange, Google gets some of your data, your PII or some of your transactional data.

It's – we've been trying to do a little work here on the value of that trade. It's really a good deal. But I don't know if other people have. How will the framework affect what is this business model that dates back really to the dawn of the commercialization of the internet?

I didn't prepare them for this one, so –

MR. CALABRESE: I mean, so I'll say, I mean, my skepticism is not disagreement. Obviously we see this transaction of data for services every day. I think there's an overreliance on that argument. Sometimes it argues that then, therefore, you can never restrict the transfer of data because you'll somehow cut off these services. And I think there's a lot of middle ground there.

So I'll be very concrete, right. Google offers a tremendously popular service and one that I think almost everyone here uses, either this or Apple, which is Google Maps. And obviously everyone understands that when they use Google Maps, they are sharing their location data. It is sort of crucial to many of the most useful things that one uses Google Maps.

Now, that requires the sharing of location data persistently in real time, and often even maybe when your phone is not on, depending on your settings. So you can make that educated and informed deal as a consumer. That doesn't mean that you feel comfortable having that location data used for some other purpose.

And, in fact, one can imagine a legislation that said something to the effect of, if you are opting to use a service that you know requires location data, that is as good as consent. We don't need you to check a box. You get it. The company gets it. But what we will not let you do, for something sensitive like location, is use it for third-party purposes. It won't – you know, you will not be able to, in fact, convert it to another service.

That's a deal that CDT is comfortable with. That's a legislative line. Others may not be. They may want to move the line a little bit. But my point is, that's very much a legislative, you know, line-drawing exercise. We are saying there should be a law that says sensitive data cannot be used for third-party purposes.

So what this framework will help you do, I think, and do very well, is do an assessment of what kind of information do you have, how sensitive is it, what might the guidelines look like, and then the internal actors can make assessments about how they feel comfortable doing that, and I think helps to clarify, for a policymaker that might want to say how do I adjust the dials, right, how do I adjust the – you know, the framework says, well, here's some natural points that we thought we had to – we had to assess as an internal entity about whether we felt comfortable taking it to this point and then, of course, the lawyers get involved about how you write it into law, and that's a separate question. But I think the framework has a lot to say about helping to kind of commit very concrete some of those various decisions and do them in a way that's very informed by how data is being used.

MR. MATUSOW:

Yeah. I would add that it's not mutually exclusive that you would have protection of data and responsible data practices and innovative business models and new technologies. I think that one actually begets the other in important ways and you have to be thoughtful about how you do that. I think there's an active debate coming around secondary use of data because there's huge value in that and it's societal value, it's – companies can profit from it. It's individual value.

You know, if I can, you know, take someone's search results and the music they downloaded and what they bought at the store and diagnose pancreatic cancer, that's a really interesting outcome that has incredibly profound results. But you would have a really hard time making an argument under the classic GDPR sense that your legitimate use – that your original collection of the data of someone's song traces was to diagnose pancreatic cancer, right. That's a – that's a leap. And the whole value of where we're going around combining datasets is really about unexpected learnings and where that can come from.

And so I'm not purporting to give you an answer, you know, from this point. But I would say that this is a societal debate that's still to come, that you've had a movement in privacy to say you collect data for a specific use and that is then determined to be legitimate and, therefore, you would operate, you know, your business practice around it. But now as people are moving into this idea that there's going to be huge economic value or innovations from secondary uses of data there's a – there's a big debate, I think, on the horizon around that and I think it's an important one and one that has both, as I said, you know – not both. It has three elements: societal, business, and individual implications.

MS. LEFKOVITZ: I mean, I think that's really where the risk-based approach is – you know, has its strength in terms of, you know, understanding, weighing those different risks and benefits without sort of, you know, having these kinds of rules that, you know, everybody sort of chafes against.

That's sort of why, you know, inherently privacy is sometimes seen as a sort of obstacle as opposed to, you know, a support, an enabler of trust. And having that, you know, risk-based discussion sort of furthers that, you know, and it keeps, I think, organizations focused on actually innovating on their privacy solutions, right. I mean, when you tell everybody do X that's exactly what they focus on and usually not much more. But when you say use, you know, measures commensurate with risk, now they have to think what might those measures be. Hey, can somebody come up with a better measure, right, and that's where, you know, research both at NIST and other institutions can play a role in saying hey, you know, 10 years ago we couldn't do, you know, homomorphic encryption.

Now, you know, we're beginning to have some applications and, you know, you're still going to make money off the data but it's going to be a little bit more privacy protecting. It's not a huge shift in your model but it gets – you know, we still may have our model and we still get a little bit more privacy. Maybe it's not as much as some people would like but maybe in 10 years we'll have another technology that we'll do research on and it will improve. And so we take an attitude of, you know, more similar to sort of health care where we're constantly trying to improve our medical treatments. You know, I just would like to see that for privacy.

MR. CRONIN: You know, I agree with almost everything everybody said earlier. But I think the only thing I would add is that I see the framework as being not only technology but also business model agnostic and it should be – it'll work in any of these things. There may be slightly different issues, different risks, depending on the use, on the user. But the fact is the framework will help in all of those areas.

MR. LEWIS: We have a really toy research project trying to put a value on data, and so it's been interesting, and it's lower than you would think. Is that a market failure? Is that – does it – or are we not catching something? So stay tuned for that one.

Maybe a final question for the panel: What does this mean for consumers, both now and in the future? And you can decide when future is. But the framework is out there; what should consumers look to see change in what they do now when they interact online? What might change a few years down the road?

I did warn them about that one, but – (laughter).

MR. CRONIN: Well, I would say that what you would hope to have is that if everybody applies the framework, that consumers will be better protected and they will understand that they're better protected, because a lot of this is – there's a lot of mistrust with consumers, and a lot of it is lack of – perhaps some is lack of education. Some of it's lack of really the companies doing what they should be doing. So therefore, if you have everybody working the framework or many people doing it, at least the companies that are using the framework could reassure consumers that their information is being protected and in appropriate ways. And that is an evolving standard, frankly, because

as time goes on you'll have – Naomi pointed out there's new issues coming up all the time. There's new technology, new ways of doing things. And so that should be creative over time and improve and enhance.

MR. LEWIS: Anyone else? Does this mean we – oh, go ahead. Naomi, please.

MS. LEFKOVITZ: OK, or Chris or –

MR. MATUSOW: Well, I guess where I would start with on consumer is just to keep in mind that consumers depend on the power of branding relative to trust – relative to trust. The NIST brand is a trusted brand I think more within the business community that's aware of it. I would say that your average consumer may not be aware of the NIST brand.

The consumers start to look for, you know, it's got the seal of good approval to say, oh, I'm trusting it more or not. Or as I noted before, if there's, you know, prescriptive regulation, that that would obviously have a real say in overall consumer trust.

It's important to note the framework is not a certification, nor was it intended to be one. And there are privacy certifications, as well, and there will be varying degrees of that. And one of the challenges that I think everybody is potentially faced with is somewhat of a vulcanization of the certification space around privacy where you might have 25 different marks that are suddenly floating around and say, which one's better, you know? Which one do I – do I need to trust more or less? So that's a whole conversation in and of itself.

But I think that it's really important to note that the framework will have an effect on consumers if businesses are acting more responsibly, but in terms of consumer trust, I think you have to recognize that consumers look for a brand. They look for something that they can – you know, the seal of good approval or the Consumer Reports or the – you know, the ISO stamp or something like that. That's what they're going to respond to. So I think that we have to look at this as a spectrum of different activities and the role that different elements play.

MR. LEWIS: Great.

MR. CALABRESE: I mean, I would completely echo that. I mean, I do think that – to very concretely answer your question, I mean, I don't think it's going to have a dramatic impact on consumers by itself. I think that what it is is a way for us to get to a place where we can create rules of the road so a consumer can really feel some confidence that there are, in fact, laws; and those laws actually govern how their data are used; and that, you know, companies that are following those rules are being responsible and they can have a sense that their sensitive information is just not flying out there willy-nilly to be used by anybody. And I think that's where they are right now.

And there's a little bit of a – of a learned helplessness, if you will, where it's like, I've checked the box, I know I've given – done something and I don't like it, but I want the service. And I think that's a place where – I suspect everybody on this panel wants to get beyond that place. They want to get to a place where consumers are really – actually feel OK with the benefit and they feel like they're actually making a reasonable

benefit. And I think this framework, if done right by the right companies, is a way to actually begin to kind of lift up that value proposition.

If it's a checkbox exercise, then it won't do that. But you know, our hope is, of course, that they'll have policymakers and lawmakers come up behind and say, well, now you're going to have to, we're going to make you. And this is a step in that process.

MR. LEWIS: I was hoping that somebody would say that it means we wouldn't get those things that say, have you read our 4,000-page – (laughter) –

MS. LEFKOVITZ: I was about to say that. (Laughter.) Like, if we got to a place where in three years my sister did not call me up and say, why am I suddenly getting all these notices of consent – (laughter) – it would be a great place.

MR. LEWIS: Good. That's a good metric for progress there and easily to – easy to verify.

Let me see if there's questions in the audience. Do we have – we've got – oh, we've got a few. So why don't we start on that side and work our way over? Can we get a microphone over there? And please identify yourself.

Q: Hi there. Dan Vasquez, vice president for East Asia for Fornetix.

What can we do to encourage faster adoption of NIST standards internationally? There was a company in Japan that I was talking to last summer that said that the new NIST 800-171 standards were great, especially how they applied to encryption, and we were trying to help them with this billion-key encryption management system we have. But the company told us that they have to wait till the Japanese government approves it and it enacts it, which creates kind of a one-year lag of adopting the standard. So what can we do to try to get companies involved earlier instead of having to wait a year to implement one of the NIST standards? Thank you.

MR. LEWIS: Why don't you start?

MS. LEFKOVITZ: So I'm not sure I fully understand that exact example, but you know, certainly from, you know, our publications, you know – so like our special publications, you know, might have some requirements for federal agencies, but they are always available voluntarily to any organization to adopt at any time, so.

MR. MATUSOW: I'll take that a bit further and say that industry has been pretty vocal with NIST in encouraging them to internationalize some of their work. So the NIST Cybersecurity Framework has been adopted now by the ISO/IEC community and that's been extremely helpful. We also have heard people around the world say: fantastic piece of work; it's got a U.S. government stamp on it, I can't adopt it; and if it's got an ISO stamp on it, I'm more comfortable adopting it. And so that type of thinking and that type of work is important.

There's also NISTIR 8074 – I'm looking over at – all right, thank you – which encourages the U.S. government to work with international standards where possible and to take their work internationally where possible. As U.S. industry, it behooves us to have that level of thinking and international acceptance because of the obvious reasons of doing

business in multiple jurisdictions. And I think that there are – you know, the Privacy Framework, we don't know yet. We're just not there to know if there is a future path for it as the Cybersecurity Framework took. But certainly I think it behooves everybody to think about it on a globalized basis.

The other point I'll make is the framework's not a standard per se, right? I'm a standards geek. I happen to swim in the world of standards geekery way too much. But we have to be really careful. The framework will, in fact, reference many other standards and point to them as useful guidance, and that's what the mappings and the crosswalks are going to be all about. And so that's an important relationship to keep in mind. That's why it's called a framework, because it's not a standard.

MR. LEWIS: Anyone else on that one? No?

Well, let's take the other question there. And please remember to identify yourself.

Q: Hi. My name is Steve Perkins (sp). I'm from Dallas, Texas. I've been involved in data analysis and information technology for about 40 years.

And last year I was involved with a group that helped write a law in Texas or a bill in Texas on data privacy, and that bill was honestly run over and killed by a bunch of lobbyists, so we did not have a data-privacy bill that passed. Out of that, though, came the Texas Privacy Protection Advisory Council, which is now trying, again, to write a bill about privacy. I admit I am a real skeptic about there ever being a federal privacy bill, you know. It may never happen. So I'm wondering if the NIST Framework should be thought of as California does this version, Washington state does this version, New York does this version, Texas does a version. What do states do with the NIST Framework, basically?

MR. CALABRESE: What an interesting question, which is always code for I'm not sure I know the answer. (Laughter.)

MR. MATUSOW: But you're going to answer anyway. (Laughter.)

MR. CALABRESE: Well, that's what they pay me for. That's what I get the big bucks for.

MS. LEFKOVITZ: We'll be right behind you.

(Cross talk.)

MR. CALABRESE: Listen, I do think that it's important to understand, first of all, that the NIST Framework, it's not a set of substantive sort of rules. So that that's just – just – (inaudible) – that level set.

I do think that there is – there is some value in – because, I mean, many of the bills are crosscutting in terms of, you know, the types of obligations they put on data holders. And so I could see, in a universe where we had half a dozen states with privacy laws, an effort to use the framework as a way to sort of harmonize some of the obligations or, at least, understand the obligations and attempt to harmonize them. I just – and this is where I think it's a little different than data breach. I just think that's really hard to do.

I mean, there are times when there are very concrete obligations that may govern the same actions in different states but put different obligations on them. And that's a very difficult circumstance to put a – to put anybody in.

So that's why we continue to push for federal privacy legislation, even though I will freely admit it's a slog. So I guess my – that's my long and short answer, is I think it will help. I think ultimately we do need a federal push. And I – I guess the last thing I would say is that the states are playing an important role in making that happen, because that push didn't exist before CCPA. But now that we have CCPA we have Washington, we have Texas, we have New York. We're starting to see that build momentum federally.

MS. LEFKOVITZ: I mean, I think some things that we have heard from some organizations about, you know, how they're contemplating using the framework is, you know, to create sort of that base program that then they can use across different jurisdictions. And then they can sort of, you know, tweak on top of it, for this jurisdiction requires this little thing, and this jurisdiction require that, and so they can have this base program that then they can tailor as needed in different jurisdictions.

MR. LEWIS: Anyone else? No? OK. Oh, goodness, they keep coming. This gentleman here, please. And remember to identify yourself. I'm not ignoring this side of the room. I'm just near-sighted.

Q: Hi. My name is Peter Slort, Netherlands Embassy.

I have a question. There's a lot of discussion both in the U.S. and in Europe about facial recognition. Is that also a field in which the framework could work? And if so, would that – would that possibly lead to different outcomes, whether you discuss that in California or in other parts of the United States?

MS. LEFKOVITZ: So the framework is, you know, technology agnostic. So, you actually – you know, you won't see any terms around biometrics in there. But I think that both the process, in terms of sort of risk assessment as well as, you know, some of the more specific, you know, outcomes that we call for – for example, you know, having – embedding privacy preferences of stakeholders into algorithmic model objectives, design objectives, and then sort of evaluating against those outcomes are, I think, very good, you know, activities that can be applied in that kind of – you know, facial recognition and that kind of data processing to sort of assess and understand and figure out, like, what are the appropriate constraints and, you know, are our models actually working, so.

MR. CRONIN: Yeah, I agree with that. I mean, I think that facial recognition is just a specific use case. And it involves privacy, it involves other things as well. And the framework should apply as equally well to that as to any other use case that involves privacy – has privacy implications.

MR. MATUSOW: I would –

MR. LEWIS: OK – oh, go ahead.

MR. MATUSOW: I would just note that NIST did an additional process this last summer on artificial intelligence and sort of the role that NIST should play relative to that topic, the role of standardization, how to think about that. And I think that the important piece of that privacy is a necessary but insufficient element to discuss to get your head wrapped around that set of topics. So there's more to it. And I think that the framework is helpful, but not sufficient to say – to address the whole – it's a whole other domain that's worth talking about, but it's just we should be thoughtful.

MR. CALABRESE: I will actually just push back. This is the closest thing we might have to controversy on this panel. (Laughter.) I will just push back a tiny bit. I actually think face recognition is a good example of something the framework is maybe not as best positioned to handle, because face recognition is – there is a tremendous amount of disagreement, I believe, about the proper applications and use of that technology.

We have a wide range – everything from ban it altogether, to, you know, I don't understand what everybody is complaining about. And it's also a technology that is actually rapidly and has already spiraled well out of control of the individual or even the data collectors, right? Because you can scrape the entire internet for face images, build your own database, deploy your own algorithm, and use that technology against people in public. There are very few choke points, even for a responsible actor, to necessarily rein that in.

So that, to me, is an area where I just think it's asking too much of the framework to make some of those very difficult societal decisions about how facial recognition should be used, especially when even a good actor may not have the ability to rein in a bad actor's use – or, you know, I wouldn't call it a bad actor. Rein in an actor that wants to take – to use that data beyond the original collected purpose of the data. There's not a lot of room there to do – to actually control that. So I think that that's more appropriate to a policymaker stepping in.

MR. CRONIN: I agree. I think if you were to start from scratch, though, the kind of – the principles and sort of the processes that are used – you'd have to change them to a certain extent. It's a much more complicated issue, I agree. And for instance, with – at IBM we've actually advocated precision regulation in the facial recognition space. And I think we have to balance here, yeah.

MR. LEWIS: Yeah. We're starting a project, I think, on facial recognition here that looks at some of the applications you can use. And I would highlight, if you haven't seen it, some of the work NIST has done on facial recognitions and coming up with good ways to assess it. So probably among the most valuable reports on this that are out there.

OK, I wasn't expecting this. Why don't we start from this end and we'll go that way? So that lady there, please.

Q: Thank you all very much. Rachel Fefer, Congressional Research Service.

We referenced the NIST Cybersecurity Framework. It's been hugely successful domestically and internationally. But as you all have mentioned, we still have 50 different state, you know, data-breach notification laws. With the rollout of the Privacy Framework, and you're looking for federal legislation to come out, are you looking for

preemption of what is there at the state level? And should the – should any federal legislation take into account things like data breach or other data issues that maybe weren't specifically clarified in this particular Privacy Framework or maybe other efforts by NIST?

MR. CALABRESE: Well, I mean, I'll say, just to answer briefly, CDT is willing to accept federal preemption. And in fact, we think it may be necessary and appropriate, but only with a very strong data governance law. You know, it's – answering that question is sort of the last question we answer, after we have a piece of legislation in place that we feel confident is going to kind of protect consumers. So that's our sort of baseline on preemption.

MR. CRONIN: I concur. I don't have anything more to add.

MR. MATUSOW: Yeah, me neither.

MR. LEWIS: OK. Well, nailed it in one.

We're coming close to the end of our time, so why don't I take at least three questions and then we'll respond to them? Can you hold up your hands again, please? We've got one there, one there, and then the one – the gentleman in the back. And remember to identify yourself, please.

Q: Yes. I'm Tatiana Mesic (ph). I work in risk management for CareFirst.

I spent last two years working in Europe on GDPR compliance projects. So I can attest to what has been said before about how NIST work is extremely useful in GDPR compliance projects, especially when it comes to risk-based approach, right, because GDPR says all these things that need to be done, but then how it needs to be done is not always clear, or it wasn't always clear from the beginning, right? So all roads led to NIST when it came to many things that had to do with – not everything, of course, but a lot of the things that the GDPR compliance project would require.

And so I am both European and American. And so when I work there, Europeans look down on the U.S., and here people are, you know, saying how, you know, European have their noses up, and so on. And I think that Europeans have it right in terms of what needs to be done, but then Americans have this pragmatic approach to things, and showing how these things can be done. And so this framework, Privacy Framework, is going to be extremely useful. And I have already used in my work all the things that NIST has done in privacy engineering, and so on.

Now, my question is about the privacy-enhancing technology. So in the future, I think that technology is going to resolve a lot of the issues that we have in privacy today. And I think it's – the wave is going to, you know, of course, come from the United States. I think a lot of the innovation – technological innovations come from here. But I'm wondering what you think about the future of privacy-enhancing technologies and whether this federal legislation potential would entice people to come up with more and more solutions that actually would be profitable and, you know, not come from just general concern for privacy but actually have this profit and business impetus behind it.

Thank you.

MR. LEWIS: Thank you. We have this lady here and that gentleman back there, and then we'll close it out.

Q: Oh, hi. I'm Kelley Cox with the American National Standards Institute.

Naomi, I'm wondering how are you promoting this framework outside of industry? Because you've got great connections, obviously. And to Jason's earlier point, to get the consumer buy-in, are you doing outreach to the consumer interest groups? And, additionally, I would also think, because of the state issues like some of the big seven – National Governors Association and some of those groups that would have a keen interest in this.

MR. LEWIS: Great. Thank you. And then in the back there. The last one, please.

Q: Hello. My name is Jeremy Treadwell (sp). I am a technology consultant.

I've been focused on product for a while, and a lot of my executives have been asking questions about privacy and how do they ensure the data that they're collecting is complying with different – you know, upcoming GDPR and CCPA. Kind of simplified this the best I could: In a world with constant data breaches and the eroding trust relationship between consumers and organizations, how can organizations educate consumers on their efforts to both secure the company and the consumer data and minimize the individual exposure as well?

MR. LEWIS: Great. Thank you. That's a good one to end on.

Do people want to tackle any or all of these? I mean, we had the privacy-enhancing technology, the consumer outreach, and then the – how do you get consumers to trust and to think. So I don't know, they're all good. So feel free.

MR. CRONIN: I think with the privacy-enhancing technologies is that I think part of the question was will legislation spur it, and I think with privacy-enhancing technology, technology companies should be getting out ahead of that. They shouldn't wait for it because that will ultimately – again, the whole idea is getting trust. If you have the technology that people can use that helps breed trust, then you may not need the legislation, I mean, or the legislation may be framed differently if you've gotten people to, you know, understand that you're protecting it.

MS. LEFKOVITZ: And, I mean, I'll follow up on that point, that the way you structure the legislation I think would impact the –

MR. CRONIN: That's right.

MS. LEFKOVITZ: – you know, incentives for developing different types of privacy-enhancing technologies.

MR. MATUSOW: Yeah. I would point to the fact that, you know, the GDPR is so strong on privacy by design as a genuinely aspirational step that was taken, and it does – has driven lots of behaviors. It also gets to the gentleman's question in the back.

There is this mix between privacy-enhanced technologies and that which you're doing by design and how consumers can get educated because, A, the products that are coming out are going to be more aware of privacy issues and will be marketed as such, and that's important. At least there will be education in that. But also go back to the – to the – you know, the Ronald Reagan concept of trust but verify. People want to trust but, ultimately, they're asking for, OK, prove it to me somehow, and that's where they're going to get to marks and bugs. You know, if I hold up the back of this physical device and you all have different physical devices you'll find 25 bugs on the back of it that say UL, CE, triple-C – you know, all these different marks. Those are all ways that consumers get that piece.

And so education is going to come, I think, in a number of ways. But the legislative push and then the aspirational push of companies to actually deliver privacy-enhanced technologies, I think those go hand in hand.

MR. CALABRESES: And I – and I guess I'll just finish by echoing that. You know, I would be very concrete. If I was telling the executive I would say, listen, you should support privacy legislation in the United States. I mean, there's – the reality is that it's not going to be crazy. This is not going to crush innovation. There are plenty of forces who are well aware of the need for enough elasticity in regulation that we're not going to see rigid data uses.

But what we do need is a universe in which we can tell consumers that there are laws on the books that are going to protect them. And I think for most executives in mainline businesses they're starting to use more and more data, and I think most of them understand that they work best in a regulated environment that they – where they have rules of the road that they can comply with and then just go forward and do their business.

MR. LEWIS: I'm glad you ended it on a consumer note. But I don't want to lose the ANSI point, because when you were asking your question, I was trying to remember, what the heck did we do to get the Cybersecurity Framework? Part of it was well adopted. Part of it was it was incorporated by the administration at the time in a variety of regulatory and executive orders and other actions. Agencies picked it up. There was a broad – now you have an industry that works on promoting the Cybersecurity Framework and using it and selling services off it.

What do you see for the – and maybe, Naomi, we'll start with you, and others can pitch in. What are we going to do to answer the ANSI question? Because that will, in some ways, also address the consumer issue. I think consumers may not be aware of the Cybersecurity Framework as much as we might hope, but it does shape their lives and their business activities.

MS. LEFKOVITZ: So that was absolutely a focus. As my boss said to me, like, now the easy work's done; now the real work starts – (laughter) – now that we've developed it. And so it is very much a focus of socialization and, you know, thinking not just about the U.S. but globally how we get that adopted. So we certainly have, you know, many plans for

conferences and presentations and so on. But, you know, I absolutely think that everybody becoming an evangelist – so, you know, we are looking for privacy leaders, right, who are willing to stand up and say we’re using it, and this is why. And that was – we found very valuable with the Cybersecurity Framework.

MR. CALABRESE: I do think the Cybersecurity Framework –

MS. LEFKOVITZ: Looking at all of you.

MR. CALABRESE: – helps a little. Sorry.

MS. LEFKOVITZ: I’m like, looking at all of you, all right? (Laughs.)

MR. CALABRESE: I do think, I mean, the success of the Cybersecurity Framework helps, honestly. I mean, I was talking to somebody in my office before this panel and they were, like, yeah, remember we started doing that thing, like, five years ago, and now it’s everywhere, right. So, I mean, there really is a sense that, like, if you build some of these products and they’re useful, that there’s going to be a value in adopting them and focusing on them and figuring them out.

So I think you’ve sort of laid – plowed some good ground there, and we just have to build on it.

MR. LEWIS: Any other final thoughts? No? Last words. We will have a signup form if you want to be one of those privacy volunteers that Naomi was talking about. (Laughter.) But that will come later.

MR. MATUSOW: And Naomi will call you. (Laughter.)

MR. LEWIS: And she will call you.

MR. MATUSOW: I wasn’t kidding. (Laughter.)

MR. LEWIS: Please join me in thanking what’s been a really – (inaudible) – panel. (Applause.)

(END)