The Joseph H. Alhadeff Digital Economy Conference Series Presents:
"A Decade of OECD Internet Principles: Policymaking in a Data-Driven World"

A Joint Virtual Conference of the USCIB Foundation, *Business at OECD* (BIAC),
and the Organization forEconomic Cooperation and Development (OECD)
May 25, 2021
9:00 a.m. - 12:30 p.m. EDT

Conference Transcript

Opening Remarks

BARBARA WANNER: My name is Barbara Wanner. I am Vice President of ICT Policy for the U.S. Council for International Business. On behalf of USCIB, I am pleased to welcome you to The Joseph H. Alhadeff Digital Economy Conference, "A Decade of OECD Internet Principles: Policymaking in a Data-Driven World." [agenda link]. This is our fifth event, which we have been holding every other year in collaboration with the Organization for Economic Cooperation and Development, or OECD, and Business at OECD. As the title suggests, this year's conference will consider how the OECD's Internet Policy Principles, which were developed in 2011, so 10 years ago, not only have informed consideration of some of the OECD's groundbreaking digital work but also how the principles may be employed to address challenges posed by the rapid pace of digital innovation and related changes to the digital ecosystem in which we now operate.

First and foremost, I would like to thank our corporate sponsors, whose generous contributions will continue to support our work on digital economy issues. They are Amazon, AT&T, EY (Ernst & Young), Facebook, Google, CCIA, and Walmart.

It is my pleasure to introduce USCIB President and CEO Peter Robinson and Hanni Rosenbaum, who is Executive Director of Business at OECD, who will formally open the conference. Peter, the floor is yours.

Introductions and Welcome

PETER ROBINSON: Well, thank you, Barbara, and good morning, good afternoon, good evening. I see some of the participants are from around the world to this fifth joint conference of USCIB, Business at OECD, and OECD focused on cutting-edge issues in the digital economy.

As most of you know, USCIB is the American member, Federation of Business at OECD, which is a relationship that we highly value, as it has enabled U.S. business together with counterpart federations from other countries to provide business input to, advice to, and help shape the work of the OECD across several disciplines, including digital economy, tax, trade, education, and labor, to name a few.

As Barbara mentioned, this conference will consider how the now decade-old OECD Internet Policy Principles not only have been reflected in some of the OECD's most recent groundbreaking work but also have served over the years as a guide for our consideration of a host of digital economy issues.

The focus of this conference would have been near and dear to the heart of the late Joseph H. Alhadeff, for those of you who know Joe would appreciate and for whom this conference series is named. Joe,

formerly of Oracle and before that our colleague here at USCIB, served for many years as chair of Business at OECD's Committee on Digital Economy Policy, or CDEP. In his capacity as chair, Joe worked tirelessly with business colleagues back in 2011 to help shape the OECD's development of the Internet Policy Principles as well as to build consensus within Business at OECD to support the IPPs.

As we will learn, the process was not easy. Indeed, it was fraught with disagreements between and among all stakeholder groups. However, the final product, the 14 OECD Internet Policy Principles time and again has served as the basis for building consensus on digital economy issues in the OECD and other multilateral forums, between stakeholder groups, and within an increasingly diverse business community. History will likely show that the IPPs were one of the OECD's more noteworthy contributions to policymaking in a digital economy world.

So, while I have the floor, let me just take this opportunity to thank Barbara Wanner and Erin Breitenbucher for their intrepid work in putting this conference together, and as you settle in for what promises to be a substantively rich discussion, I'd like to turn the virtual podium over to Hanni Rosenbaum, Executive Director of Business at OECD. Hanni?

HANNI ROSENBAUM: Thank you very much, Peter, and let me also start by thanking everybody at USCIB and OECD for all the support you've offered in making this conference happen. We are really excited to be part of it. Special thanks to our co-chairs Julie Brill and Makoto Yokozawa and also our vice chairs who worked a year with us on today's program, including Ellen Blackler, Rich Clarke, and Barry O'Brien. We would also, of course, like to express our thanks to our OECD colleagues and friends. I'd like to mention Andrew Wyckoff and Audrey Plonk and, of course, their teams for the excellent working relationship that we've had on digital issues for many years and which for us really makes the OECD the go-to organization for digital policy.

Now, as you all know, over this past year with the COVID-19 pandemic, we have witnessed an incredible acceleration of the digital transformation which has made our cooperation with the OECD all the more important.

Let me also mention that just last week at our annual General Assembly, we issued our Economic Policy Survey, where member organizations cited the digital transformation, data governance, and data protection among the five top reform priorities for 2021, underlining the important roles that digital technologies have played in the COVID-19 pandemic.

Now, this past year, therefore, even further reinforced is the critical importance of OECD work and global standards. I'd just like to mention for privacy, digital security and safety, connectivity, and digital infrastructure. Let me also mention the cross-cutting digital policy work in key areas such as trade, taxation, competition, health, employment, education, to name just a few. Let me just say that we believe that this cross-cutting approach clearly underlines the unique role that the OECD plays in the digital field where we need to connect the dots with other policy areas.

Looking ahead from the Business at OECD side, we are really excited to be engaged in the third phase of the OECD Going Digital project, addressing data governance for growth and well-being. We clearly see this third phase of the digital project as a key opportunity to advance, among others, secure and globally interoperable policy frameworks for responsible data sharing and collaboration on cross-border data flows with trust.

As far as today's conference is concerned, we are excited that the meeting revisits the famous OECD Internet Policy Principles and looks at how the principles remain relevant to issues that we are currently addressing, such as AI, government access to data, policy for secure internet, and new and evolving business models and technology. We firmly believe that working together, the cross-sectoral and the multistakeholder process holds the key to success for an inclusive recovery from COVID-19, which we are all aiming at, and recovery with data-driven innovation will be key driver of success.

Now to conclude, let me again express our deep appreciation to USCIB for organizing this conference series commemorating our past CDEP chair, Joe Alhadeff, and I can confirm that Joe has been one of the most active chairs we've ever had. Let me also express special thanks to Barbara and Erin from USCIB who have spearheaded the organization of today's event and, of course, also my colleague, Nicole, who leads our CDEP work at Business at OECD in Paris with great talent and enthusiasm. So let me close here and wish you all a great discussion and an excellent conference and thank you very much.

OECD Internet Policy Principles: Their Enduring Value in a Rapidly Evolving Digital Ecosystem

BARBARA WANNER: Thank you very much, Peter and Hanni, for getting us off to a great start. As we move to our opening session entitled the "OECD Internet Policy Principles: Their Enduring Value in a Rapidly Evolving Digital Ecosystem," it is my honor and pleasure to introduce Danny Weitzner, 3Com Founder principal research scientist, founding director of MIT's Internet Policy Research Initiative; Julie Brill, corporate vice president, deputy general counsel of Microsoft, and co-chair of Business at OECD CDEP Bureau; and Andy Wyckoff, director of the OECD Directorate for Science Technology and Innovation, which leads the OECD's consideration of digital economy issues. [Link to biographies of all conference speakers.]

Danny, you served on the White House National Economic Council as Deputy Chief Technology Officer during the 2010–2011 period when the Internet Policy Principles were being developed and played an active role in shaping their development as a member of the U.S. delegation. It would be helpful if you could provide us with some background concerning the economic and political context that influenced their development.

DANIEL WEITZNER: Barbara, thank you so much, and my thanks to the USCIB Secretariat and the OECD Secretariat for organizing this. I'm delighted to be here with my colleagues, Julie Brill and Andy Wyckoff, to have this chat with us, and I just want to also mention, not with us, but essential to the Internet Policymaking Principles, Ambassador Karen Kornbluh, who was the U.S. Ambassador to the OECD and my partner in crime when I was in government working on this, as well as Anne Carblanc, who played such a critical role in the passage of the principles.

It's great that we're here remembering Joe Alhadeff. I think he'd be delighted that we're looking back to try to understand how this process worked, but he's probably also remind us that we ought to be looking ahead because that's what he'd be doing. And I'm pleased to have the chance to remember him. I know that his memory is an inspiration to all of us.

So, Barbara, you asked about context, and from my perspective, what was so significant about the Internet Policy Principles, that they really marked the kind of maturation of what I think of as the second phase of internet policymaking. I want to just remind us what I think of as the first phase, which was

essentially the mid-'90s until about 2000, and we could characterize this first phase particularly in the United States and the EU and other OECD countries as a period of excitement and emergence.

There was, contrary to the kind of Wild West myth of the internet, actually quite a lot of lawmaking that happened early in this first phase. The United States passed the Communications Decency Act, which was both the occasion for the U.S. Supreme Court to strike down censorship provisions and declare that the internet was the most participatory medium for speech yet developed and therefore deserving of the highest level of constitutional free speech protection. That, I would say, was very important for establishing the political and economic environment of the internet as well as the passage of Section 230, which is much discussed these days, the regulatory framework that really made possible internet platforms like YouTube, Twitter, Facebook, Google, eBay, and others. The U.S. also passed in this time the Digital Millennium Copyright Act, which was kind of a detente on copyright issues between the intellectual property holders and the internet service providers, and the U.S. enacted a series of internet tax limits, which were important as well.

In the EU, there were parallel developments. The Information Society Directive, which addressed intermediary liability limitations, was enacted, and the Data Protection Directive, of course, came into force in the late '90s.

Globally, also in this first phase, there was a very important shift from reliance on *de jure* technical standards from UN organizations, such as the International Telecommunications Union, and the related International Standards Organization (ISO), to *de facto* voluntary global technical standards from the Internet Engineering Task Force, the IETF, and the Worldwide Web Consortium, and really a struggle that occurred for quite some time between those *de facto* and *de jure* standards. And in the case of the internet and much of digital technology, the *de facto* standards environment really won out.

I would also just say that in this first phase, I remember particularly that the public reaction to the internet was really quite enthusiastic. In the United States, there was large-scale survey that was done by the Pew Foundation, I believe, that asked how did people understand the internet, and they said it was more like a library than a mall. And I think that was telling in the way the public thought about the internet environment then.

I think the second phase, though, was really quite different. It coincided with when I arrived in government along with Julie Brill and others, and I think it was a phase in which there was a recognition that the internet and related technologies were really vital to the global economy, to our political process, and even to our social lives, and that we were facing somewhat of a global governance challenge.

I think there was, first of all, a recognition in OECD countries writ large that the policy discussion had to broaden considerably beyond just the expert telecom regulator to include economic ministries, consumer protection authorities where then Commissioner Brill was, and the issues became significant at the highest political level. There was also a recognition that the traditional treaty-based governance process was not likely to work for the internet. Our colleague, Dick Baird, who for many years led the U.S. presence at the OECD from the State Department, would talk about the decline of the Westphalian order, and in fact, that is what we saw.

So the IPPs came at this critical moment where we had to reaffirm what was important about the internet, what had led to this 15 years of extraordinary growth, but also deal with the fact that countries had many, many legitimate public policy interests from economic and social policy to national security policy issues. We had, of course, in a tactical sense, moves by some countries at the ITU to try to reassert control over various parts of the internet economy. So the IPPs had kind of a big role in affirming the basic principles reflected in the IPPs statement, principles about privacy and intermediary liability and innovation and open networks and also a tactical role in rallying the OECD countries and many others around the view that we should not re-enclose the internet, if you will, in the more traditional telecommunications regulation from which frankly many of us had spent many years trying to liberate it. So that really was the context, I would say, for the work that went on, on the Internet Policy Principles.

BARBARA WANNER: Excellent, Danny. That's so helpful as background, and I think also what I heard in your comments, that this seemed to set the stage or usher in an era in which it was recognized that all stakeholders have a seat at the table in terms of talking about internet governance issues.

So, to delve into this more in depth, we had asked Danny to moderate a virtual fireside chat with Andy Wyckoff and Julie Brill. Danny, Julie, and Andy, the floor is yours. Thank you.

DANIEL WEITZNER: Thank you, Barbara. Great to be with you, Andy and Julie. This is just an absolute pleasure. So the audience understands how we're going to roll here, I'm going to ask Andy and Julie a series of questions. We'll have a discussion, and we'll also then hope to be able to take your questions at the end.

Andy, could I start with you? You've been a leader in global technology policy since the time that it was really nerdy and saw the OECD through issues such as the cryptography guidelines, which were I thought very important but perhaps not front-page stuff, and involved a lot of experts. You saw the OECD through the Internet Policy Principles and now obviously beyond. But, as you look back at the adoption of the Internet Policy Principles, what do you think has been the important impact, both in OECD countries and maybe even more broadly?

ANDREW WYCKOFF: So thanks, Danny. I just want to compliment you on setting the table here with that background, which I thought was a really good—you know, to know where you're going forward, you need to know where you've been. So I think that history lesson is important here.

For me, the IPPs did really three really important things, and one of them, we're celebrating today and celebrating with the life of Joe Alhadeff. It's the multistakeholder ethos that went behind them and were how the IPPs got developed. It's moved, I think, from that time. If you remember, just in 2008, we were the first committee that had really institutionalized broadening multistakeholders beyond just BIAC, who is hosting us today, which I really appreciate, and TUAC, which is organized labor [Trade Union Advisory Committee] to include civil society and the technical community. To have those four different stakeholders sitting at the table is to this day, unfortunately, a little bit novel at the OECD but has become the norm and one which I think governments really welcome, and I see that norm now in the G7 and the G20 and in other bodies. So I think that to me was one of the most important things.

I would point out that Joe —and Peter Robinson referred to this—didn't have the easiest time of getting businesses to all consolidate on those principles, and at the end of the day, civil society decided not to

sign. But, to some extent, I think that represents the strength of the relationship that people can disagree, but there can be sharing of views and practices.

With that comes a second thing that becomes a mantra lately, which is kind of like-minded values. It was less important then, but it's in the principles, and it's interesting how many times they're in the principles. I think it was really important in the beginning to underline that this is important. It's more than just technologies and making money. It's about human-centric, democratically based values, which we all hold dear, and with that the respect of human rights and the rule of law. That's in the principles, and we care a lot more about that today. And we'll probably get back to that.

Then the last thing for me, a little bit nerdy, is it began to underscore some dimensions of the "internet economy," what we called it back then, that are now central in the economy, and it began to flag these. Policymakers started to attach greater importance to them, one of which is what we called the "digital divide," just connectivity. That's really come to the fore, I think, with the COVID pandemic. It's about promoting creativity and innovation and how that happens and how you keep that going—it is the lifeblood of the economy and growth—and with it, strengthening—and I'll leave this to Julie, but strengthening the consistency and effectiveness of privacy of personal data collection.

And then the last thing is just about maximizing individual empowerment. These are all principles that are there. I think that they become even more central and have gone, as we would say at the OECD, kind of horizontal and mainstream.

DANIEL WEITZNER: Andy, thanks. It is interesting, as you point out, that it was actually some of those basic principles that I'd say we had the easiest time with getting consensus on. There were some that were hard, but some of those principles that you call out that are really important were table stakes for everyone. But now it seems important to actually have said them, so yes.

So, Julie, I want to take you back a little bit. You've been in the United States, both a state regulator and enforcer and a federal regulator and consumer protection and enforcer. I've heard you call yourself a "law enforcement official," and indeed, you did have significant law enforcement authority. But you were doing all this in the context of this growing global environment, and I'm just interested in how you see the Internet Policy Principles either having been shaped by that increasing global focus on enforcement and consumer protection or how it contributed to being able to work in that arena.

JULIE BRILL: Sure. First of all, thank you, Danny, for, as Andy said, laying out some of the background in history of the IPPs so well, and I also need to thank USCIB, BIAC where I am a co-chair of the CDEP committee, and of course, the OECD, Andy and your team, and so many people who've really dedicated their lives and careers to really advancing an open global internet in which people can participate. And, of course, I too was a good friend of Joe. I believe it's the second time we're honoring Joe, and it's my second time participating to honor Joe. It's just such a wonderful time to remember him and all that he did.

So, actually, Danny, for 17 years, I carried a badge. I was in law enforcement. I worked in state attorney general's offices, and I led consumer protection and competition enforcement. And when you are an assistant or deputy attorney general, you get a badge. So it was serious stuff.

Then, of course, I spent 6 years at the U.S. Federal Trade Commission as a commissioner in the Obama administration, got to work with you, got to work with Andy, and got to work with so many others on these critical issues.

When I was a commissioner, I would say that the IPPs were very important as—I'll call it "organizing principles" around which regulators and all sorts of stakeholders could think about internet policy, and I'd say that there were three important things that I used as part of my organizing principles that came out of the IPPs. One is that internet policy is not just one thing. You can't just think about privacy or the free flow of data or intermediary liability. In order for the internet to really be a thriving ecosystem for speech, for the economy, and for so much more, you actually need to think about a lot of things together. And the IPPs in a remarkable way that we don't see that much anymore brought together a lot of different domains into one place and allowed us to think about internet policy holistically.

I think the second thing that I took away as a pillar in terms of driving my work at the U.S. Federal Trade Commission is that internet policy needs to be global. It is a global platform, and as a result, as regulators, as law enforcement, as other kinds of stakeholders, we need to interface with our global counterparts. We could devise all sorts of rules in the United States if we had wanted to, but the effectiveness and the impact of those rules that we would devise would always rub up against and bump into what was happening around the globe. So we needed to have a perspective that was global.

I would also say, just to sort of echo a little bit of what Andy said, I think the third pillar for me was how human-centric the IPPs have been and continue to be. You think there's a lot of discussion about individual empowerment. There's discussion, of course, about privacy but also about security, which is deeply important to individuals. There's discussion about trusted flow of data globally. How prescient to be thinking about that back then because it's obviously top of mind now.

Then the last thing that I think was deeply important—and you could think of it as a pillar. You could think of it as substantive, but that internet policy will not work without the participation of lots of stakeholders, not just government, not just business. Labor, as Andy pointed out, NGOs, civil society, we all need to come together. We might not agree, as we pointed out, but it needs to be a multistakeholder discussion, again, in order to be effective and impactful.

DANIEL WEITZNER: It's such a great point, and I think it really bears stressing. I know that my own first interaction at the OECD was in 1996 and '97 when we were having the first global debate about encryption policy, and the OECD took this on. I remember I was an advocate at the Electronic Frontier Foundation, and I was invited to be part of the U.S. delegation. I remember saying to Scott Charney, our mutual friend, "What are you doing inviting me on the U.S. delegation? I don't agree with any of the U.S. policy on encryption." He said, "No, but you're an important part of the discussion," and I do think that the OECD has always stood for those principles, very important.

I would say, not to be pessimistic, but it's not clear that we are seeing more of that. It seems like we may be seeing less of that globally as the polls of the policy debate become more nationalized, I would say, or associated with particular countries.

JULIE BRILL: Yes.

DANIEL WEITZNER: It does suggest there's a lot more to do in this forum.

Could I ask you, Andy, what do you think has changed? I know that you're working very hard now on AI policy generally. The OECD put out, I think, a very important set of initial policy principles on AI, and you've got, I think, a very important effort with the AI Observatory now. Between 2011 and now, what do you think is different, and how are you functioning differently, given those changes in the environment?

ANDREW WYCKOFF: Wow, Danny! I have a hard time getting my head around the last 18 months.

[Laughter.]

ANDREW WYCKOFF: There's huge changes we've seen and particularly back 10 years. I remember 2011 was the rule of analog. We had tsunamis in Japan and volcanoes erupting in Iceland but a huge amount of change. Let me just give you maybe my top three.

I don't remember China really being on our radar in 2011. It was more, as you were discussing, differences across the Atlantic, a few countries, but I don't think Chinese inserted the firewall until late 2000s and then got serious about Deep Packet inspection in 2012 or so. That's one. Clearly, they are a big player in physical economy policy, however you want to cast it, and that's a big change.

The second is another big change. You know, I was just looking up the market caps of some of your favorite U.S. big tech companies today, and wow! That's indicative of a couple things. It's indicative of credible innovation and foresight, being at the right place at the right time, and it's indicative of, I think how the economy has swung towards a digital economy more. So now you've got the top five plus you've got to include Microsoft, you know, over $8 trillion this morning. That's three times the bottom five of the top ten. That's a huge change. In 2011, it was just Microsoft and Apple barely coming in at No. 10. The economy has changed a lot in those 10 years.

To me, I'd love to pick your brain, Danny. The techy thing, I think that was really important. To me, it was that smart phone in 2007 or thereabouts, which really didn't start to penetrate, and really, it's a smart computer, isn't it? It only had 35 percent of adult household in 2011, and now we're way up to 85. It's ubiquitous, and I do mean ubiquitous computing because when you pair that with high-speed mobile broadband, which is available nearly everywhere, it's a much different environment. So it was really our first Internet of Things, a little bit throwing off a fair amount of data and changing people's daily routines. It's now become a constant product that everyone, right down to teenagers, must have, and so I think that changes things.

And maybe the last thing—we talked about it, but I got it so wrong in 2008. We did a big ministerial in Seoul, Korea, and it was really celebrating the economy as the internet economy. They were the same thing in my mind, and clearly, I was in a rarified group that thought that. It really took until several years later that it began to take hold. I think it's really only until—at least if I judge the OECD as a proxy, there was one committee dealing with these issues in 2011, the digital economy policy. Now fast forward to 2021. Nearly every committee at the OECD has a digital policy item, and to me, that is really reflective of how governments have changed. And it makes our job a lot harder in some ways, but it has really changed the environment of the whole digital economy policymaking.

DANIEL WEITZNER: Yeah. You know, you've both made the point in different ways, Julie in pointing out the substantive breadth of the Internet Policy Principles and that you can't just pick one and say that's

how I'm going to decide any given issue. You can't just say, "I'm going to do what's right for privacy" or "I'm going to do what's right for copyright holders." You have to hold them all in your head somehow at once and make whatever tradeoffs you're going to make amongst them. I do think that's part of why we ultimately lost civil society is they were in the middle of too many copyright fights around the world, and to accept this, quote, "compromise" or this kind of middle-ground position just was not something that was tactically possible.

But nevertheless, as you both say, both substantively you have to keep this range of issues in mind, and institutionally, certainly, I found—and Julie, you could speak to this—coming into government in 2009, we were frankly not organized to deal with the internet in the horizontal way, that you just couldn't stick it in one agency. You couldn't stick it under one category of regulation alone.

It's interesting whether we're going to find that pattern or not with AI. I tend to think some of AI policy may be taking us back more in a sectoral direction, but maybe we'll come back to that one.

Julie, Andy kind of took us to the modern-day internet economy, that the market cap tables have flipped almost upside-down from where they were 25 years ago. I know you've spent a huge amount of time in the last year at Microsoft wrestling with the challenges that the COVID economy and the COVID society and the COVID public health crisis puts in front of us. Digital technology has been at the heart of that. I'm interested in whether you think that the IPPs get us ready enough. Did it provide us enough guidance to deal with in facing the challenges of COVID?

JULIE BRILL: So I don't think anyone could have really prepared for the challenges that the world faced. This crisis—I mean, look, I've been on the planet for quite a time, as have both of you. I have never experienced a crisis like this, and I think we'd have to go all the way back to 2017, 2018 in order to come up with a comparison in terms of a crisis created by a disease in terms of its global impact and then just the number of people impacted.

Where I think the IPPs were prescient and had we had them top of mind as we were grappling with the pandemic, I think we might have been a little bit more agile in terms of dealing with the crisis, and here's my perspective and how I see it. The world went through more digital transformation in the past 18 months than it had in the prior 5 years, and that amount of digital transformation was expected more or less to happen in like 3 to 5 years and instead, boom, it was compacted into just a few months.

And the world, to the extent that people could work form home, they worked from home, and they did that through digital technology, largely speaking. To the extent that people could socialize online, that's what they did. To the extent that people could go to school, that kids could go to school or adults could go to school, they did that online. Lives transformed in many ways to have digital interaction as opposed to what had been, in many circumstances, more of an in-person or hybrid interaction, and this kind of digital transformation was enormous and had impact, both very, very good—of course, it kept society together in many ways. It allowed many, many people to participate who wouldn't have otherwise been able to, but it also pointed out some of the real gaps and problems that we had. And some of these were identified in the IPPs back many years prior.

So, first, I'll identify a few of them, the gaps that we saw that came out of the COVID crisis that I think the IPPs are designed to address. The first, I think Andy referred to this a little bit earlier—connectivity. Connectivity is so critical to participate in the digital economy or to go to school, to work, to socialize

through digital technology, and we learned. We had known this before, but the extent to which the digital divide and the connectivity in broadband gap became obvious just grew in terms of enormity and importance, particularly for those people who didn't have the ability to connect with good broadband, who had to drive their kids to sit outside a Wi-Fi hotspot in order for them to go to school. These were always issues, but I think that just came to the fore that much more. The UN and many, many other multistakeholder organizations, OECD and others, are really trying to drive a conversation around how to close this digital divide, the broadband gap, so that the world is connected when it needs to be and when it wants to be and individuals are connected when they want to be. The IPPs identified that issue many years ago.

The second issue that the IPPs, I think, identified—and again, we needed to pay attention to it. We, of course, at Microsoft were paying attention to all of these things, but I think the world needed to pay more attention to these issues. When you're talking about connecting digitally, you're talking about data, and when you're talking about individuals doing this, connectivity and engaging in school and work and socialization, you're talking about personal data.

And so what we needed to be thinking about was not just how to protect that data through privacy and security, which is, of course, always critical, but also the extent to which that data could be used to help solve some of the problems in the COVID crisis, some of the racial inequities that were being experienced, both in terms of the impact of the disease and also the mitigation efforts, the health care crisis that was starting to arise and developing a clear picture that there were certain communities that were just completely being left behind because of historical health care gaps as well as current health care gaps.

That means data actually could have been incredibly helpful. I'll just use the United States at the moment as an example. Had the United States had clear guardrails about how companies and governments and NGOs and academics, how we could have used data in a more robust way to dive in quickly and solve these problems—we don't have these guardrails. They're not that clear, and so people were not using data to sort of jump in and say, "We've got a hotspot here. We need to help in this other area. Things seem to be okay," and to really in a more agile and granular way deal with the crisis.

The last thing I'll mention—and I'll mention it quickly because it's something we've been talking about this entire time that we've been together—is the IPPs also identify trust and the need to build trust. As you're using these digital technologies, as you're using personal data in order to identify problems and really identify solutions, trust is the foundation upon which everything else is built, and that's where privacy and security and the kinds of things that the OECD is driving through continued development of these principals really was playing a critical role and will continue to play a critical role.

DANIEL WEITZNER: Julie, I think those last two points are so critical, and I know how hard you and your colleagues at Microsoft worked on them, but I think you're right. I think in the U.S. and maybe less so in other parts of the world, though, there was a struggle about how far we could go to use personal data to address the critical, really scientific questions, the scientific underpinnings of this crisis.

One of the incomplete to-do items from the IPP era, at least for the United States, was our passage of federal consumer privacy protection law, which you were very vocal about and which a number of us worked on, but we didn't quite get there. I will say that I think that we had imagined in 2011 that we would still be living in what I might characterize as a multipolar world, that obviously, it was clear that

Europe was going to remain a critical source of privacy thinking and regulation, but also that the U.S. would have a strong voice and be a center of privacy policymaking.

I personally think we've lost a lot in the U.S. from not being a center of privacy policymaking, and I actually think if you look at some of the data as an example in differential deployment of the automated exposure notification capabilities that Apple and Google deployed in order to warn people about potential COVID exposures, you saw much higher adoption rates in European countries than in the United States, much higher adoption rates in other OECD countries that have strong data protection laws. Now, obviously, there are many causes for that, but I can't help think that we are losing a lot from the lack of a globally consistent set of privacy rules.

Back to Andy, you drew our attention so importantly to the importance of a multistakeholder dialogue. Well, that's just not because you're going to have a better debate. It's because it actually means you'll involve more of society in any of these policy discussions, and I think somehow—I'm editorializing here, but I think it's wonderful that the EU has made itself a center of privacy thinking. And I think it's enriched EU society in many respects. I think we're seeing a lack of that in the U.S., and I think that translates into a corresponding lack of trust and probably just as importantly—so a lack of trust on behalf of individuals but also a lack of confidence and clarity on behalf of businesses who, as you say, Julie, just weren't quite sure what they could do or how far they could go.

JULIE BRILL: Precisely.

DANIEL WEITZNER: Barbara, I see your hand is up.

BARBARA WANNER: Yes. I think there might be a question from one of our speakers, Yokozawa-san, who is Julie's fellow co-chair.

DANIEL WEITZNER: Please. Yokozawa-san, go ahead, please.

MAKOTO YOKOZAWA: Hi. Thank you so much, and hi, Julie and Andy. It's very nice to see you here.

My question is very simple. The internet has to change to adapt to the recent modern issues like we are always discussing in the OECD, like the personal data protection and the cybersecurity and also the government access. Julie, you are quite right that trust is a very important element of the future internet policy issues. So it might be a time to think about a new structure or new design in any level of the internet. That's my basic question. How do you feel about this?

DANIEL WEITZNER: Thank you, Yokozawa-san. To summarize, perhaps, the question is: What are the new design imperatives and opportunities that we should be looking at in the internet environment? Who wants to start?

JULIE BRILL: Go right ahead, Andy.

ANDREW WYCKOFF: Thanks, Julie. I know we're getting close to the end of our time, but I think to me—and this won't shock anyone here—it's better understanding the nature and the use of data and getting a much better governance framework for data. I don't mean regulations always. I just mean a government framework because I think we still—there's a lot of misunderstood notions about it, but I

think it's just going to be resources, as Julie was just talking about. It is incredibly important for us to better harness with safeguards where we need them in the future, and so I think this will be an overarching kind of North Star, Southern Cross, whatever you like, for a lot of the digital policy going forward.

DANIEL WEITZNER: So, as a technical design imperative, better data governance to increase agility and flexibility. Julie?

JULIE BRILL: And I would say one of the critical elements that we need to maintain in our internet policy is its international interoperable focus. Danny, you were saying the United States, which I fully agree with. The United States has been left behind in terms of its ability to even participate in a global conversation around how we protect data because we don't have a national North Star.

So I think what I would like to see and what I think is necessary is that member states, members of the OECD, develop their own perspective on what is required in order to protect data and be clear about that and then come together and talk about the need to make sure that this is interoperable so that we have the free flow of data around the world.

What I worry about is if we try to rearchitect the internet in a way that does not allow for that interoperable free flow of data. We will lose so much. We do know how much we will lose, but we don't always keep that top of mind. And I think there's so many conversations now where that issue about the power and the importance and the freedom that comes from an interoperable internet really does need to be sort of at the center of any discussion around how we build to improve the digital ecosystem.

DANIEL WEITZNER: I think that's a wonderful forward-looking way to end. Better data governance to increase trust and agility, a continued commitment to global interoperability.

I will just say I cannot thank the OECD enough, Andy, your extraordinary leadership over the years, and all of the member states and everyone here who's participated and made the multistakeholder commitment a reality.

I think the wonderful thing about the internet environment is it really is always a work in progress. It has been from the very beginning. It has principles about it, both technical and organizational and public policy principles, but it also keeps moving forward. And our challenge is to all work together to keep it going in the right directions.

Thanks to the audience, and thanks again, Andy and Julie.

Session One:
The OECD's Artificial Intelligence (AI) Principles:
IPPs Inform "The How"

BARBARA WANNER: I would like to now introduce our speakers for Session One. These speakers will examine the development of the OECD's groundbreaking Artificial Intelligence Principles that you heard referenced during the opening session. Importantly, all of these speakers participated in a special multistakeholder experts group that was convened by the OECD for the express purpose of developing

the AI Principles. They are Audrey Plonk, who is director of the OECD Committee on Digital Economic Policy and who will moderate the discussion; Adam Murray of the State Department; Barry O'Brien with IBM Ireland; Dewey Murdick with Georgetown University; and Cristina Pombo of the Inter-American Development Bank.

Audrey, the floor is yours.

AUDREY PLONK: Thank you, Barbara. Hello, colleagues. It's great to see you all today, and I just want to thank USCIB for organizing this event. It is timely. I also want to take a moment to remember my friend, Joe Alhadeff, who I worked with for many, many years and who we miss regularly here at the OECD and beyond.

So we're going to dive right in. Our previous speakers talked about the AI Principles a little bit, and so I just want to first start by saying that all of you were in Paris at the time when the OECD developed the AI Principles. Looking back at that experience, I want to invite our panelists to reflect on how the IPPs laid the foundation for the OECD's work developing the AI Principles, which are now recognized as fairly groundbreaking or at least early in the sort of international community's work on forging a common view toward how to advance trustworthy AI.

The influence of these IPPs may have been conscious or unconscious in the making of the AI Principles, but given the extent to which the IPPs have influenced our approach to the digital ecosystem, which we heard a lot about in the last 45 minutes or so, we weren't even really thinking about AI when the IPPs were developed. I'd love to get the panel's reflections on whether and how the IPPs may have influenced your thinking or even looking back at the IPPs now, having been through the AI Principles with the OECD, how you think they kind of fit together. If you don't mind, Cristina, and you can kick us off.

CRISTINA POMBO: Thank you very much for having me today and for allowing me to share this panel with these amazing guys that I remember in so many of our meetings of the working group of the AI Principles.

So reflecting back when we started thinking about these principles—and I think I joined the group in February last year, and I think before me joining the group, some of, of course, the people in the OECD were thinking about those principles and were reflecting more on how to translate the IPPs in the principles.

I might confess, Audrey, that I was not sure how those things go along together. I think at the beginning, with the first conversation, I started thinking I have to read a lot after the first meeting, thinking how is exactly this going to fit in one to another. The one thing that I really like at the end of our conversations was the best way that these principles could translate into something that is real from principles to practices, it was getting the IPPs to inform and to really merge with the AI Principles. So it was time to do vis-à-vis work with the IPPs and the AI principles, and it was not easy. And it's not easy right now, but I think that is at least my way of thinking it, going through the definition of the principles.

AUDREY PLONK: Thank you, Cristina. Let me turn now to Adam Murray, who is the chair of our experts group, ONE AI, and was deeply involved in the development of the principles. So I'm curious, Adam, how you think the IPP shapes the AI Principles or vice versa.

ADAM MURRAY: Yes. Thanks, Audrey, and let me add my thanks too to the host for putting this conference together today. It's really a pleasure and an honor to join this group of experts here. As somebody who comes from a policymaking background and doesn't have a lot of technical experience with Artificial Intelligence, it really has been a privilege to chair the network of experts on AI and to work with folks like we have here on the panel today, always learning so much whenever we have our meetings.

I was really impressed and struck by the first panel, the fireside chat, about how many similarities and key words I heard between the IPPs and the AI Principles. Let me start with multistakeholder cooperation. I think that was really key to our development of the AI Principles. From the very beginning, it was a multistakeholder group with representatives from not just government and industry but civil society, academic, the technical communities, labor unions, and you might expect that it would be tough to get all of those actors together around a common set of principles. But we did it, and I think that was a really impressive feat to be able to move relatively quickly to get everybody on board. And I think that is, one, a testament to the power of the multistakeholder process but also, two, to the work of the OECD and the Secretariat for really herding all of those cats, so to speak, and laying the groundwork for us.

"Trust" was another word that came up in that first discussion, and just recall that these are the principles for the responsible stewardship of Trustworthy AI. So I think trust was another key component here in our AI work.

Lastly, let me just say that I think in many ways, like the internet, Artificial Intelligence could be considered a general purpose technology that really underpins so many other applications. In that regard, it was important for us to set the AI Principles at the right level and to make sure that we could, in a sense, future-proof them to see that they would have some staying power, and I think we were able to do that. I'll admit honestly that had a copy of the Internet Policy Principles on my computer that I would refer to often as we were going through the drafting sessions because I thought they really struck that right balance, and I'm hopeful that our AI Principles will have that same staying power, and maybe in 10 or 15 years, you'll be inviting me back to reflect on this process again. Thanks.

AUDREY PLONK: Thanks, Adam. You're always invited back, always invited back. Hopefully, you'll come back. That's the key.

Let me turn now to Dewey Murdick. Dewey you certainly were involved in our experts group. But perhaps you were less familiar with the IPPs when you dove into the AI Principles. So it might be interesting to hear your views, having done the AI Principles, looking back at the IPPs to see how they connect.

DEWEY MURDICK: Yes. I think from my perspective, the process in which I've integrated the insight to the IPPs has been through looking back and saying, "Wow! I'm really glad that these precedents were set previously," as opposed to being inspired by every instance. Looking back and hearing the previous session, which I thought was really interesting, Adam's comments are really important structure for what I'm going to say, but just adding one little piece, one of the IPP principles—I think it's No. 7 based on my notes—was to develop capabilities to bring publicly available, reliable data into the policymaking process. This is exceptionally essential for artificial intelligence, machine learning, and many other emerging technologies.

Getting this information available so that people can actually use it and now as part of the public discourse in a multistakeholder-inspired way, it is essential to what we're trying to do now as we turn the corner from the AI Principles into implementation. I think the precedent that has been set from the IPPs is essential, and we have benefited strongly from them opening the doors now we're benefiting and able to take the next step for the Artificial Intelligence context.

AUDREY PLONK: Thanks, Dewey. I'm going to turn now to Barry and get his reflections. Barry?

BARRY O'BRIEN: Sure. Thanks very much, Audrey, and also, thanks to USCIB for the invitation to participate today.

Like Dewey, I have to confess that the Internet Policy Principles weren't at the top of my dossier when we started the work on the AI Principles, but when you look at them today, I think it's striking how resonant they are. There's certainly a lot of parallels between them and the AI Principles that came out in the end.

But I think it's also clear that the IPPs have influenced a lot of the public debate around issues like data privacy and security and so on, and I think you could also recognize the fingerprint of the IPPs in the kinds of principles of many companies, including IBM have adopted, in relation to issues like transparency and fairness and accountability and that emphasize data privacy and empowering the individual. So, if only in retrospect, I think clearly their influence is very marked, and it's definitely there.

Like Adam, it was really interesting to hear the insights from the earlier speakers about the process through which the IPPs were created as well as the multistakeholder aspect, which I think is really important. The other one that strikes me is that I think both in the case of the Internet Policy Principles and the AI Principles, here is this group who came together to consider this new emergent technology that was perceived as holding enormous promise for societal good but also one where there were maybe risks and unknowns, and that, therefore, kind of a principles-based policymaking was appropriate. It was the right way to go, and that together with the multistakeholder approach, I think, is what led, certainly in the case of the IPPs, to clearly a very influential set of principles. I think in time, it will show the same in the case of the AI Principles.

AUDREY PLONK: That's an excellent setup for the next question. As the head of Division for Digital Economy at the OECD, I'm particularly interested how we take the AI Principles so that when we're having this conversation 10 years from now, we have speakers on the panel—all the speakers on the panels are like, "Yeah, I knew about those AI Principles 10 years ago," and so it makes me think, what did we learn from this experience?

Just moving forward, the principles and policy frameworks are great, and along with the economic analysis and the metrics, that is the core of the OECD's value proposition. But the rubber really hits the road when you try to implement principles.

The OECD has broken new ground by launching an important new follow-on process that has been digging into what it means to implement the AI Principles. You all participate in this work. You lead this work. You live and breathe this work. You're sort of an extension of our family here at the OECD, and for that, we're extremely grateful.

I wonder if you could, just at a high level, reflect a bit on what that has revealed. I think, unlike some other areas of technology policy, there is a strong agreement that the principles are a foundation, but that we have to go deeper, and we have to make them actionable and implementable, particularly for governments, but not just for governments, also for private-sector entities that are looking toward how to navigate this complex policy and regulatory and standards of technical landscape.

Let me go a little bit in reverse order. I'll mix things up, just to keep people on their toes in the audience, and I'll start first with Dewey, and then I'll put Adam on the spot and then Barry and then Cristina. So, Dewey, you're up first.

DEWEY MURDICK: Thank you so much for setting that up, Audrey. This is really quite an exciting space we're in right now where we really are trying to figure out. The principles are essential and important for the usage of this emerging technology. Now how do we apply it?

Think about Artificial Intelligence. To effectively regulate or govern Artificial Intelligence, you need situational awareness about how these AI systems are going to impact various contexts. Many of these AI systems, whether they be in financial systems or autonomous cars or AI-enabled trading systems or water treatment plans with AI-controlled systems or facial recognition, all of these contexts are slightly different, and trying to say, well, AI is obviously like this in all those contexts is not productive.

I think an important stage when you're trying to actually make an implementation is you need to have the situational awareness. You need to characterize these AI systems in a way that is quickly understandable to the policymaker community and then can help you differentiate between what kind of regulations are appropriate for that autonomous car system as opposed to the water treatment plant or the recommender system for child videos on YouTube or whatever platform your child uses to consume media.

So there's four characteristics —and I won't go into the great details because this will take too much time, but first of all, you need to understand the context in which the system is operating. Is this a critical system? Is this something that has life or limb associated with it? What sector is a part of it? You need to understand the data that's coming into it and the input that's required to fuel the AI systems that are involved in those contexts. You need to understand the algorithms like how did this AI system acquire its capability. Was it trained? Was it given human guidance, rules? And then what tasks are they actually executing? With this context in place—we've essentially laid out these four dimensions.

We've laid out a whole bunch of different choices. So we can basically provide policymakers a field guide. When we go out and look at birds or try to identify animals or mushrooms, we say, "Oh, look, it's tall. It's got two legs. It makes a really tweety sound," but now you do the same thing with this field guide for AI systems and you say, "Oh, look, it's processing images. It's trying to help people understand how to make decisions, but it doesn't make the decision itself. And it works in the medical context. With this field guide, I can say, okay, these are the questions that are relevant."

Anyway, this is an incredibly exciting process that we've followed, and I think this field guide, metaphorical meta-field guide, will be very useful as it matures.

AUDREY PLONK: Adam, what can you add to that?

ADAM MURRAY: Well, it's hard to follow up on the field guide. I love the analogy there. It's great.

You know, look, I think what's really important about the work that we've been doing through the network of experts is how we move from principal to practice because we all recognize the importance of establishing those principles as kind of a first step. But as everyone has alluded to, it really is the follow-up work that's so important.

Along with Barry and another colleague, Carolyn Nguyen, from Microsoft, we co-lead ONE AI's working group on Trustworthy AI. In that working group, we've been focusing on trying to find use cases or examples of what works in different contexts to promote responsible AI, to promote Trustworthy AI. This is going to be really important for helping policymakers to better understand and see what's out there, and not just policymakers but actually other AI actors, companies in the private sector or academics or even individuals who are impacted by AI. The Trustworthy AI working group is putting together a database that will pull all of these use cases together to identify some good practices. I'm sure Barry will talk a little bit more about that.

Let me just say a little bit as well about the working group on Policy Implications for AI. This is where international governments have come together to share their own practices in implementing AI or establishing their own strategies, policies, or regulations. Obviously, we've seen a lot of movement out of the European Union in the last month with new draft legislation on AI. In the United States, we've been doing quite a bit as well. We have guidance from the Federal Trade Commission. We have work on standards through NIST [National Institute for Standards and Technology]. We have guidance for public uses of AI from the Office of Management and Budget. All of these things that come together, I think, are really good contributions to the global conversation. The OECD provides the platform to bring countries together with other stakeholders to talk about these things.

Audrey, concerning your introductory point, perhaps what will set the AI Principles apart from the IPPs is that we have the OECD's AI Policy Observatory. That is such a fantastic resource, and my kudos to your team for putting that together because the amount of information that's available is just really stunning. It allows for both the history of the principles and how we got there, but also pulls in work from across the OECD, from the different policy communities. It links back to national strategies and examples. It has data available on it. It's a really valuable tool and resource, and I hope folks will go and discover it if they haven't already.

AUDREY PLONK: Thanks, Adam. We're very proud of the AI Policy Observatory, and I think it's an excellent point that maybe it sets the standard for how to move forward with implementation going forward when you have a strong set of principles.

Let me go to Barry and then Cristina to explore how we are moving into action, particularly in your experience in ONE AI but even beyond that.

BARRY O'BRIEN: Thanks, Audrey. So picking up on what Adam said, I can tell you a little bit more about the working group that I co-chair, which is exactly on this question: How do you help actors implement Trustworthy AI in accordance with the AI Principles focused the human-centeredness, transparency, accountability, and so on.

This working group set out to create a space for different AI actors to share information about their experiences with implementing Trustworthy AI, what approaches, what tools they used, what challenges did they encounter, etc. It turns out there are a lot of tools out there already to help AI actors rise to the challenge of deploying and building Trustworthy AI. But those tools aren't always easy to find, and in truth, I think it would be a challenge to many AI actors to judge whether and how it might help with their particular AI implementation.

The tools vary significantly. Some of them are software programs to help you detect bias. Others are procedural guidelines that you might use in how you organize developing an AI system or operating one. Others are educational initiatives, maybe for developers or implementers or business users. There's a huge variety.

This working group set out to gather examples of all those things and then create a framework that, again, classified those tools a little bit the way Julie was talking about classifying AI systems themselves. We're going to work towards a database which will allow AI actors to understand what set of tools are out there and to choose ones that are most appropriate to their particular situation, choose the kind of system to manage the stage and the life cycle that they are at. It's going to be, we hope, a very practical contribution to helping real-life AI actors implement the OECD's principles in the real world.

AUDREY PLONK: Thanks, Barry. Now, Cristina, your reflections on how we go from principles to action.

CRISTINA POMBO: I want to share with you what we've done with some of the governments in Latin America and the Caribbean, thanks to the work that all the team has done and particularly within the group that Barry is co-chairing, which is the one on which I participate.

A lot of Latin American governments are thinking about how we translate these principles. For example, a government may want to support a system for giving subsidies and helping people with the pandemic. So how does that principle have to do with the system that I want to build?

One thing that really helped me a lot in those conversations was to start thinking about specific questions. If you have the principles at the top of your mind, then what are the criteria that you can have to see if that is the principle that is present or not? Then, how are you going to measure the criteria you are applying? What is the indicator, and then how you do you prioritize that indicator? And the last one, the last question would be: What are the observable correctors that you will have?

For example, if you think about the principle of transparency and expandability, your criteria would be maybe you're going to show that you are applying that principle, disclosure of the original datasets or disclosure of properties of the algorithm of the model used. Then the indicators could be—you could think about if the data documents. Is it plausible for its purpose? Which data is being used? Has the model in question been tested and used before? Then you can start thinking about those observable characteristics and whether the model is right to use.

For me, working with the governments, the classification and tools that Barry mentioned were really tangible and handy to explain to them how to translate the principle into practice. So asking those four questions for me were very, very important.

AUDREY PLONK: Thanks, Cristina. So I'm going to move us into a quick round of wrapping up. I want to close by asking everyone if you could say one thing that you think the OECD should do on AI going forward in the next year. It could be something we're already doing, but it doesn't need to be something we're already doing. Barry?

BARRY O'BRIEN: Thanks, Audrey, and especially for the surprise question! What this really comes back to is it's relatively easy to get people to agree in the OECD's AI Principles or a slightly varying set of words but essentially the same principles. The real challenge is how do you get beyond that. You have to get into a fair amount of detail to actually understand these things in practice, and the same is true when it comes to regulation.

Again, we can all talk about the need for risk-based regulatory approaches and so on, and that's easy to agree to. But the challenge then becomes, how do you actually define those risks? Can we all agree on what constitutes a high-risk?

For instance, can we come up with a way that organizations, public sector, private sector, large and small, can all use to figure out, well, am I talking about a high-risk application; if so, what do I need to do about it? The devil is really in the details. I think it is important and there is a role for the OECD to help in that process of taking the principles down to a level of detail where they're actually, practically useful to all kinds of different people on a regular basis. I think the message for me would be keep going. That's the right direction.

AUDREY PLONK: Okay. Thanks. Adam, can I go to you next?

ADAM MURRAY: Sure. Well, thanks, and let me just follow on with what Barry was saying about the work and getting down into the nitty-gritty. I think that's really important, and sometimes, it's not the headline-grabbing work, and so my thanks really to all of the experts in ONE AI who have rolled up their sleeves to do that because it does lay the foundation. Really, it is about helping us to promote public trust in AI. I think that's so important in rolling out AI in a responsible way and making sure that it's adopted in our society so that it can contribute to all of these great things that we've been talking about.

I think the one piece of advice, if I could give to the OECD—and I think this is probably on your radar already, but as we heard in that first fireside chat. That is the importance of data and data governance. I know the OECD has launched a new horizontal project this year focused on data governance under the Going Digital III banner, and I think linking up the work between ONE AI and the Policy Observatory with Going Digital III and its focus on data is going to be really important.

We had this great recommendation on AI Principles a couple of years ago. We're about ready to have the OECD Council endorse a new recommendation on enhanced access to and sharing of data, and I think that's a really powerful combination. We really need to dig into that.

AUDREY PLONK: Amazing. Thank you so much. Cristina and then I'll let Dewey have the last word.

CRISTINA POMBO: I agree with what Adam said in the first question, having a multistakeholder body thinking ahead and having different voices, because the beauty of that is it's not only OECD countries talking about it. It's Latin American countries as well. There's a private sector. There are a lot of different voices with different perspectives, and it's hard to agree on risks, as Barry would say, but it's a

super rich discussion on how to advance. So I really congratulate OECD for that. It's an amazing space to move forward.

The only thing that maybe I would love to see and discuss more in the future—and it goes a little bit with what Adam was saying—is thinking about algorithm audits, and it's a little bit of what is the responsibility of this decision support system governed by algorithms. Some of our stakeholders at the IADB are asking us, "Can you recommend to us how to mitigate the risk of letting the algorithm govern a little bit more the decisions? Is there a way to recommend and do algorithm audits in a more systematic way?" I would love to have a conversation on how to move that forward.

AUDREY PLONK: Thanks, Cristina. So, Dewey, what would you put on the wish list for us?

DEWEY MURDICK: Oh, I'm really grateful to go last. First, it gave me time to think, and secondly, a lot of the people, like, for example, Cristina, what she was just saying was one of the things I was thinking of. Adam, when you're talking about data governance, my heart burst with things to talk about on that topic. So I'm going to save you the bursting heart discussion there.

However, let's be really practical. I'm going to ratchet the multiyear view into something closer. If Carl Linnaeus when he created the taxonomic structure for all of biological organisms had said, "Yeah, this is a great system, and here's five examples of animals that fit into this structure, so enjoy," it probably wouldn't have been nearly as useful.

Looking forward, we're taking all these wonderful frameworks, making them work at scale, actually populating them with hundreds of AI systems, many more tools than we have available. This takes the promise of "Isn't that neat?" to "Wow! Isn't that useful?" and I think that is really where we are for the next year or two to make that foundation of principles into a wonderful application framework, and then into a very useful tool because it is well populated. The sharp metal edges that catch you when you pass it every time have been filed off, and it becomes a very useful system. That is where I really encourage us.

The neat thing is the audience of this particular session actually has the opportunity to help file off those metal edges that would cut people and make them sad but now also make it even more helpful by adding features. Right now, for example, the AI Classification Framework is out for public comment. You can read it and say, "No, that's not quite right. I think it's missing something." Provide that feedback, and I think you can help OECD and the multiparty body working on the classification framework be that much better. That's really where I would suggest we go for in the near term.

AUDREY PLONK: Well put, all of you. Thank you for both the ongoing support and the excellent ideas. I'll just plug the classification system again. Please go look at it. Please comment on it. You will make it better. It's only through that public consultation and sort of a huge stakeholder community that we can make it the most useful going forward.

Thank you, Barbara. I hand the floor back to you.

BARBARA WANNER: Thank you, Audrey and speakers, for the rich discussion.

Session Two
Government Access to Data in a Post-Schrems II World

BARBARA WANNER: I would like to introduce our speakers for Session Two, which will focus on government access to data held by the private sector. It will be moderated by Christopher Hoff, who is the current U.S. Deputy Assistant Secretary of Commerce for Services. Our speakers will include Norman Barbosa of Microsoft, Lauren Bernick of the Office of the Director of National Intelligence, Dylan Cors of the U.S. Department of Justice, Greg Nojeim of the Center for Democracy and Technology, and Michael Rose of Google.

The OECD's work on this issue arose from concerns raised by members of the OECD's CDEP in late 2020 about government practices that compel access to personal data held by the private sector. The CDEP also observed that the absence of common principles for trusted government access to personal data may lead to undue restrictions on data flows resulting in detrimental economic impacts.

The OECD decided to convene a special governments-only group to elaborate a set of common and coherent best practices and legal guarantees from across OECD countries aimed at reconciling law enforcement and national security needs for data held by the private sector, with protection of personal privacy and individual rights.

This is a link to the CDEP statement about the need to address this work. Business at OECD, in collaboration with the International Chamber of Commerce and joined by 23 other business organizations, also issued a statement that details the economic and commercial ramifications of restrictions on data flows.

Deputy Assistant Secretary Hoff, if I may turn to you. Please lead us through the OECD member governments' work to date on this issue, drawing upon your colleagues, Lauren and Dylan, who have been participating in the governments-only group. In particular, how do these discussions break new ground in terms of the involvement of law enforcement and national security authorities in an OECD process, which traditionally has been dominated by government officials with an economic portfolio? Thank you. The floor is yours.

CHRISTOPHER HOFF: Thanks, Barbara, and that's absolutely right. This is an incredibly important initiative. To me, it fits very well with our priorities, and it's notable for its involvement of law enforcement and national security experts at the table, some of whom are here today. It's a conversation that is just critical at this moment in time. It is important to me.

The three offices that I lead at the Department of Commerce are all of the Services' industries offices, including the Office of Digital Services, and that office has long been focused on digital trade and data governance issues. We have always advocated for policies that support the free flow of data cross borders, which is essential to global commerce, as you all know. It's important that when companies are doing business globally, both American and companies around the world, that there be fair and transparent rules of digital trade.

The engagement with foreign partners and multilateral organizations like the OECD is critical to our work to support transparency and fair treatment when it comes to data localization, cross-border data flows, and just generally speaking, trust in the digital economy. The OECD is a key forum for us and the

other OECD member countries where like-minded governments, both democratic institutions can work together to share experiences and find solutions. And because the OECD requires full consensus of its member countries, that leads to a fair and transparent process.

OECD legal instruments end up being referenced in the development of classic legislation and regulations and international trade agreements, which leads to a global impact. For example, the 1980 guidelines governing the protection of privacy and transborder flows of data was the first internationally agreed set of privacy principles that define how data should be treated and protected around the world. In the 30-plus years since its adoption, the OECD privacy guidelines have formed the basis for privacy practice and data protection laws globally. That's why the work that is done in OECD is important.

Those privacy guidelines did not consider this particular topic -- government access for national security and law enforcement purposes -- which are areas subject to intense recent public scrutiny that affects global commerce. Part of that conversation is around the Schrems II decision[1], an action that my office is dealing with right now. The United States is working with like-minded partners right now on this OECD initiative to reframe that global debate on trusted government access to data held by the private sector. This project is really critical and timely for a number of reasons.

It means that governments must remain accountable to our citizens and protect our privacy and safety while doing so transparently. It allows like-minded democracies to come to an agreed-upon set of principles. It is not just the United States standing up for itself or European Union member countries standing up for themselves, coming to an agreement. The OECD initiative has broad volume and support.

Beyond being accountable to our citizens, we recognize that these privacy principles, as international best practices, help us draw a clear distinction between the conduct of democracies -- our democracies -- and that of authoritarian states like China in areas like protecting citizens' data, the rule of law, accountability, and transparency. Citizens must have trust in their democratic governments. Fostering that trust requires that we draw on common safeguards and constraints that exist in our governments when compelling access to data for law enforcement and national security purposes. Laying those common safeguards out for everybody to see helps citizens trust their governments and trust that they're protecting privacy similarly to each other. That way, they know that if data is transferred to another OECD member democracy, it will receive similar protections.

We have critical mass to do that right now and support. To date, there are 24 countries that have nominated representatives to the OECD drafting group working on developing these principles. You see some of them here. The drafting group is limited to officials from OECD member governments, including law enforcement and national security agencies, with that relevant knowledge and competence regarding the government's domestic laws and actual practices and policies. This group has been meeting regularly since February 4, 2021 as well as conducted stakeholder consultations. It has planned another stakeholder discussion in [late] June.

[1] In July 2020, the European Court of Justice (ECJ) invalidated the EU-US Privacy Shield Framework as a legitimate mechanism for transferring personal data between the United States and the European Union. This decision often is referred to as the Schrems II decision, named after an Austrian privacy activist Max Schrems, who brought two cases to the ECJ aimed at invalidating the (1) US-EU Safe Harbor Agreement and its successor (2) EU-US Privacy Shield Framework.

What will the outcome of all of this work look like? OECD instruments are non-binding legal instruments. Nevertheless, they carry great moral force because they reflect the political will of the member governments. As I mentioned earlier with regard to OECD privacy guidelines, OECD legal instruments do find their way into domestic legislation and trade agreements. And they often have a global impact that sets the tone for the conversation and the path into the future.

I wanted to highlight just how important this is to the U.S. Government and the long-term work that we're doing. Let me now turn to the U.S. drafting group representatives for their respective views on agency priorities. We have with us Dylan Cors from the Department of Justice and Lauren Bernick from the Office of Director of National Intelligence.

I'll start with you, Lauren. As Barbara mentioned, it's not common for law enforcement and national security officials to participate in OECD work. Please tell us why there is a need for law enforcement and national security representatives to be included in this discussion?

LAUREN BERNICK: Sure, and thank you, Chris, for providing all those helpful insights as background and context for this discussion. Before I address your question, I want to thank USCIB and Barbara for the opportunity to participate in this panel, but especially to share the importance and relevance of having these law enforcement and national security experts involved in this effort.

I think that importance has been echoed and supported by the OECD and the OECD Secretariat who encouraged, facilitated, and strongly recommended the involvement of these experts as well as the different member countries who have sent their experts to participate in this effort. Thank you to the OECD Secretariat as well to and our fellow delegates and our law enforcement, national security representatives who are not used to contributing to the OECD's work.

Chris, as you mentioned, this effort is really focused on identifying common shared principles, the constraints, the limitations, the safeguards that OECD member governments follow when they access personal data held by the private sector for law enforcement and national security purposes and to really understand our shared principles, our shared safeguards. That will allow us to build that trust, but to get to that point, we need to have the experts, the practitioners who know about this, to have this dialogue. It has created a unique situation.

Traditionally, OECD has focused on commerce and economics. So you have those [economic] representatives participating, yet now with this initiative, the success really lies in having and assembling the officials that have competencies in those areas to have these discussions, and having the law enforcement folks, having the national security folks is really going to allow us to identify the actual safeguards. They know the laws. They know how the laws are actually implemented. Having these practitioners is really going to provide the insight to facilitate development of principles that are meaningful and accurate with sufficient detail to show that we have these shared safeguards.

To date, much of the data protection debate has focused on transatlantic data flows, and for better or for worse, the United States has been at the center of the debate. Dylan, Chris and I, know the pain and joy that is involved in that, right? As such, we've had to really have our Department of Commerce folks involved. We've had to have our Department of State reps involved. We must have trade policy officials talking to our law enforcement folks at Department of Justice, and talking to the national security folks at the Office of the Director of National Intelligence. We've had to build this relationship in

collaboration and communication so that we could share the privacy protections and surveillance constraints under which the U.S. operates.

As you mentioned, Chris, the effort now with this OECD effort is shifting the debate to a global perspective, and thus, we need to bring those same types of players to the table, the players that haven't talked to each other for the most part before. The OECD effort is really promoting the discussion of these different players on a few levels.

You have promotion of the discussion with the different players in the individual countries. The U.S. has had that experience and that practice. I don't know how much that practice has occurred within the individual OECD members, but then they're bringing that discussion to the OECD meetings themselves. So there are different players talking among themselves and then also bringing the law enforcement and national security reps from the different members talking to each other. Having these law enforcement and national security reps explain the safeguards and the protections to the data privacy folks, to the trade folks, to the economic folks is really facilitating a greater understanding of among OECD member countries about how we protect the data access when we're accessing it for law enforcement and national security.

While I can't go into the actual discussions that have happened so far, Chris, I can tell you that the dialogue, especially with the law enforcement and national security experts, has been very robust and every engaging and then also featured the traditional OECD players coming in and pushing us to explain different things in a different perspective. That has been very exciting, been a very active dialogue, and I think that level of interaction is really allowing us to identify these shared safeguards in—and I think this is an important aspect—sufficient detail so that we could build the trust.

I think many of us—and this is just a personal experience -- have been surprised by the number of common safeguards that we are sharing. I think we're surprised because we haven't had this dialogue before. We haven't had these experts in the same room talking to each other. I think if you take a step back and pause, from the perspective of us all being democratic countries that are accountable to our citizens, it's actually not surprising that we're going to have so many shared principles and safeguards.

What we're seeing in this effort with this conversation with the law enforcement and the national security experts is that there are these common protections, and while some of these protections might be implemented or crafted or have different structures facilitating protections, the common safeguards are there. The commonalities are there, and they exist within our global law enforcement and national security environment. Being able to talk about those is going to allow us to create these meaningful principles and hopefully then create that trust that was mentioned earlier.

CHRISTOPHER HOFF: Very well put. You've explained it better than I could, but speaking from personal experience, having you and Dylan at the table right now in discussions around transatlantic data transfers has been critical. The way I describe privacy negotiations is that it's a whole-of-government effort, and you're involved in that. While I can represent Commerce and do my best to represent industry at the table, I do not have the expertise on national security law and practice the way that Justice and ODNI representatives have this knowledge. We must be able to communicate well with each other and understand each other and how national security affects privacy—and how privacy and commercial data transfers are affected by all of that. So thank you for being part of all those conversations.

Dylan, picking up where Lauren just left off, can you walk us through the overarching goals of the experts group. I understand there are common safeguards among the OECD countries as articulated in the Committee on Digital Economic Policy statement, yes?

DYLAN CORS: Thank you, Chris, and thank you to USCIB for allowing me to participate today. First, I would echo everything Lauren said about the robust and active discussions we're having and the progress we're making. Although we are spending a lot of time exploring each other's legal systems and the privacy safeguards that relate to law enforcement and national security data access, that is the substance of our work. We are tying that work back to the two objectives that are in the CDEP statement from December 2020: First, to engage in that discussion in order to identify principles that are common to OECD countries to distinguish the OECD countries from the authoritarian governments or any government that doesn't protect privacy at that high level; and second, to help build trust among the OECD countries to provide a basis for continuing data flows of personal data.

The outcome document will be one of the OECD legal instruments. We envision it to be fairly brief, setting out high-level principles that reflect the privacy safeguards that we identify as common. Because it's not a legally binding instrument, it won't overrule the ECJ [European Court of Justice decision] or solve Schrems II.

The purpose is to produce a reference document that is not prescriptive. It won't prescribe how governments should protect data or impose its obligations on them, but rather it will"describe." It will be a descriptive document saying what's going on now in OECD countries, what are the existing law and practices, and as a reference document, will inform the important discussions happening now in so many places about how to establish trust as a basis for cross-border data transfers.

Now, of course, this discussion is happening at the OECD, and there's such an important role for economic and business interests. We want to make sure the outcome document advances the objective, which is in the CDEP statement of reducing undue restrictions on the free flow of data among OECD countries and other countries that live by these principles. This raises a question for USCIB and the business world to consider.

As Lauren mentioned, the discussions at the drafting group for this project are being led by law enforcement and national security reps, like Lauren from our intelligence community and like me from our Justice Department. So we're equipped to work on identifying commonalities regarding law enforcement and national security investigations and related privacy safeguards.

A question for business to consider is: What should the OECD outcome document say about how those privacy safeguard principles relate to the commercial free flow of data? How should we relate privacy safeguards that are recognized as existing among OECD countries to the promotion of the free flow of data in order to advance that CDEP objective about eliminating undue restrictions on the flow of data?

We look forward to any input you can provide at the stakeholder discussions, which will take place in a few weeks.

CHRISTOPHER HOFF: Thanks, Dylan. You teed me up nicely to move over and ask Norman a question, in view of the Business at OECD comprehensive statement highlighting an erosion in trust in international data flows, and noting concerns that government demands to access data may conflict

with universal human rights, freedoms, privacy rights, or cause concerns and conflicts with domestic laws. And I also want to note that Business at OECD built a coalition of 23 business organizations that aligned with this statement. I would like to hear what the main issues of concern are for business, and to Dylan's point, what does businesses want and need to see come from this work -- the work of the special government experts?

NORMAN BARBOSA: Thanks, Chris, and thanks to USCIB for having us here today. We've outlined a number of concerns that are driving our interest in this process, and really, they go back several years, frankly to the Snowden revelations. We can't deny that the trust implications of that event have continued to reverberate for several years, and as global communications companies and internet service providers, we've seen that continue to be a drag on the digital economy. Most recently, as highlighted by the Schrems II decision, it continues to be a stumbling block for businesses, consumers, and even governments who are seeking to use the benefits of the digital economy.

We all recognize that law enforcement and national security authorities have a critical role to play in protecting public safety and preventing genuine threats to not just U.S. national security but global national security. There are common threats that people can agree on pretty easily, such as terrorism, weapons of mass destruction – and as we've all seen very starkly in the last 6 to 9 months -- massive cyberattacks that are impacting the global economy as well. But there continues to be a lack of certainty about what those rules are.

I'm really encouraged by what Lauren was saying about how this process is going. In many ways, I think the process may be as valuable, if not more valuable, than the end product. Seeing that global national security authorities and law enforcement officials are coming to the table with people from the trade community and privacy regulators and developing a common understanding of what like-minded democracies use to control these tools is really important, and in many ways, it's a belated conversation. As pointed out, this trust deficit has been growing since 2013, and we're now having these communications in 2021. And they need to move forward quickly.

What we are seeing in the business community in terms of the impact of this lack of certainty and lack of transparency about the rules are increasing calls for what is typically characterized as data localization. Really, this comes down to prohibitions on the use of foreign technology and trying to restrict technology to only local providers.

We're seeing an increasing demand from governments around the world that are seeking to use the benefits of the digital economy. We're seeing demands that we certify that we are not immune from other laws that may pertain to national security. That just is not a sustainable model as business tries to develop a global economy that is built on a globally interconnected network, which is critical to bringing economies of scale to the benefit of consumers, businesses, and governments around the world.

What we see from this [OECD] process is hope for a baseline of the key protections that are in place among like-minded democracies, and hopefully to draw out those commonalities. As Lauren and Dylan both pointed out, there are many commonalities. But we also want to draw out where are there areas that governments need to continue working.

I don't see the OECD process as the end of this conversation. In many ways, it's the beginning of a conversation that needs to lead to broader multilateral understanding of the appropriate boundaries and scope of public safety and collection from private-sector enterprises.

CHRISTOPHER HOFF: I appreciate all those comments, and I like that you point out that it's perhaps the beginning of the conversation and not the end. But it's a conversation that is important for all of us to be having together as government, business, civil society, and all of our like-minded democracies. Thank you for your comments about that.

I've got two more speakers to turn to. Michael, I will start with you. This is important to me because as the Commerce Department's lead negotiator for the Privacy Shield negotiations, this is something that I am dealing with for 10 out of 12 hours a day at least. Will you briefly review the issues caused by the ECJ's invalidation of the Privacy Shield Framework, and tell us what in turn you think would be needed from the OECD experts group to provide some legal reassurance to EU authorities and privacy advocates about personal data protections?

MICHAEL ROSE: Sure. Thank you, Chris, and thank you all for having me here. I get the fun duty of talking about Privacy Shield knowing that my other [U.S. Government] panelists largely won't be able to chime in. I think what I say gets to be the word of God in this space since they can't contradict me. [Laughter]

The challenges the ECJ raised in the Schrems II ruling funneled back directly to why not only is this workstream so important, but the OECD itself is probably the only place where it can be held in its first iteration. I agree with Norm that this is not the end of the conversation. But the issues that the Court raised can't be solved without international political agreements and conversations.

I'll briefly summarize these issues. The original case that the court ruled and struck down Privacy Shield in July 2020 was brought against standard contractual clauses[2] used by one American company in Ireland. That is the nexus of this entire case. What the Court ruled was not specifically about standard contractual clauses nor specifically about that one company. They targeted and ruled directly against the U.S. surveillance and judicial redress practices, but more broadly, the global lack of alignment and interoperability with European fundamental rights.

The Court critically didn't say that Facebook, the company that the original case was brought against, did anything wrong or could have done anything differently to address the Court's concerns. Rather, the Court itself ruled that certain surveillance authorities in the United States were overly broad and disproportionate. The Court also ruled that European consumers lacked sufficient judicial redress and oversight of their fundamental rights in the United States.

One of the key challenges for U.S. companies has been to try to understand what this ruling means going forward because neither of those provisions can be solved directly by us. There are supplementary measures that we have put into place to try to understand the ruling, even though there has not been finalized guidance by European Data Protection Authorities on what those supplementary

[2] Standard Contractual Clauses (SCCs) are aimed at protecting personal data that is leaving the European Union to countries that the EU has determined does not have a privacy regime deemed "adequate" and therefore may not afford the same level of security to personal data. The United States is one of those countries. SCCs, through contractual obligation, are aimed at ensuring that data is protected to a level required under the EU General Data Protection Regulation (GDPR).

measures should look like. Some companies have taken more extraordinary steps around commitments to combatting government access requests where they can and transferring or localizing data in Europe.

But there's very little we can do to solve these underlying principles. And because of that, I think we get back to questions such as what is the solve for this Privacy Shield dilemma and what is the solve for transfer dilemmas? Right now, the focus is on the United States. It is hard to imagine, however, given what the ECJ outlined, that any other country in the world will be able to achieve the level of what is being asked.

That brings us back to this process in the OECD. One of the reasons I stated that the OECD is really the only venue that can hold this conversation is twofold. First, the OECD member states are like-minded democracies that have fairly aligned principles and objectives, with an understanding of the need to balance domestic rights and laws versus international economic and business needs. The OECD is a unique venue for that.

Second, in this conversation, one often gets back to creating an equivalence with something like the European Court of Human Rights, but even that institution has its limitations. Russia is a signatory of the original treaty. It technically should be under the purview of the European Court of Human Rights, but Russia recently amended its own view of how it submits itself to that jurisdiction. In addition, Russia is an original signatory of the Council of Europe's Convention 108, which is ostensibly the first treaty on privacy. I don't think many would accept that Russia's national security laws and redress for European Union consumers is equivalent nor is it as good as the U.S. approach.

There is no clear venue for these conversations, except perhaps at the OECD. The fact that we have folks like Lauren and Dylan joining these conversations and their counterparts in other governments is in many ways historic to be sitting there with a trade negotiator and a commercial advocate, like Chris.

This is the first pillar of solving what is becoming a global dilemma, and there are a lot of positive steps that have been taken. As examples, the Korea adequacy determination and the UK adequacy determination were both done since the Court's ruling and have created a framework for what a future Privacy Shield will look like. But, again, that is just solving for one country's transfers. This OECD workstream can really start to actualize data free flows with trust and actualize a commitment by governments to recognize where data flows should be protected and where companies operate through transparency based on the country in which they're headquartered.

CHRISTOPHER HOFF: I appreciate keeping our eye on the global perspective because perspective is important in this conversation, so I appreciate that.

Turning to Greg, the Center for Democracy and Technology has participated in two OECD consultations on government access to personal data held by the private sector and has been a leader among civil society groups in articulating the human rights principles that ought to govern cross-border data demands. I would love to hear from you the main elements that civil society groups, such as yours, would like to see reflected in these high-level principles as well as hear a little bit more about your concerns.

GREG NOJEIM: Thanks so much for including me in this important conversation. It is certainly to the credit of the organizers to involve civil society in these discussions. I would submit that it might be a

good idea for the OECD to include either civil society or data protection authorities in the discussions as law enforcement has been included as well.

I think one of the main concerns that civil society has about the process is the risk that it will result in baseline principles that are acceptable to all countries in the OECD, even though many countries will have stronger principles, stronger attention to human rights and stronger surveillance laws than the baseline.

I guess I can say this better than other folks who are on the call who might be more constrained. When you look at the different countries in the OECD and their human rights records in the surveillance area, they differ dramatically. The concern is that there will be a race to the bottom in the sense of articulating principles that are acceptable to all the countries in the OECD, even though some of them have very poor human rights records in the area of surveillance.

There's a difference between having surveillance principles that are based on human rights, as the Schrems II decision was, and having principles of surveillance that are based on what countries are doing now. There's a vast gulf between those two, and the concern among civil society groups is that the gulf will be filled by baseline principles that are acceptable to all countries.

What happens when one country has a very strong rule with respect to one of those principles, and another country says, "No, we couldn't possible agree to that"? Example: Notice of surveillance by the provider. In the United States, notice is permitted in the particular circumstance, usually within the order authorizing the surveillance. In France, for example, notice is a crime. I am concerned about how the distinction between those two approaches on notice would pan out in these discussions.

I think the best articulation of the principles that civil society thinks ought to undergird government access to private sector-held data are the necessary and proportionate principles that came out a year or two after the Snowden revelations. Whatever the OECD comes up with is going to be measured against these principles, which have over 400 civil society signatories. They include principles like legality, legitimate aim, necessity, proportionality, due process, user notification, and transparency.

Again, what the OECD develops is going to be measured against these human rights-based principles as opposed to just against what countries that are OECD members are doing now. Thanks so much for including me in this event.

CHRISTOPHER HOFF: Thanks, Greg. I really do appreciate your perspective. I'm glad you're here as well.

I will ask one last question of the group in general, although you're welcome to mention anything else, if you'd like. Monitoring closely the progress of the drafting group, the OECD does expect to hold consultations with the stakeholders [in late June].

How can we make the most of this discussion, and in particular, how can we work to develop a greater level of trust in the digital ecosystem and realize the economic and societal benefits that stem from such trust?

NORMAN BARBOSA: I'll throw out one answer that builds on what Lauren was saying earlier. Lauren pointed out that this process has brought together experts in these actual practices and that they know the laws. What's important is that society knows the laws, that society globally understands and has some certainty in what those rules are so that can build trust. What is critical to the success of this is to bring transparency to how these rules are interpreted.

Also, I want to thank Greg for his input, too, because it is also critical that it doesn't become a race to the bottom. The deficiencies in various practices that may be common among several member states in the OECD process also should be called out and there should be a plan for progress on how to bring those standards up.

MICHAEL ROSE: I think high-level buy-in is critical, because the points Greg raises are very important, and Norm is entirely right. We need transparency.

One of the great aspects of the OECD doing this is there will be opportunities for principal-level conversations—involving Secretaries and Ministers—to acknowledge this workstream and acknowledge to their citizens that there is an alignment among member states. That goes a significant way in building and ensuring trust as well as demonstrating that the governments are committed to this and are behind it. Absent a new international mechanism or treaty, the most important thing we can ask for is the backing of the governments to showcase that they're all in this together and that they agree with each other that there are alignments on these principles.

CHRISTOPHER HOFF: I appreciate you saying that Michael; it is just a fact of the day. The next thing I must do is walk up to the office of the Secretary of Commerce for another call. I bring this workstream to the attention of Commerce Secretary Gina Raimondo every chance I have because it is really important to a long-term solution to some issues that plague us. Secretary Raimondo is well aware of this issue. And thank you very, very much, all of the panelists. Fantastic input from all of you.

Session Three
Changes to the Digital Ecosystem Present New Challenges to Business Policymakers and Regulators

BARBARA WANNER: I'd like to set the stage a bit for Session Three. One of those very unfortunate changes that has occurred in the online environment has been the rise of terrorist and violent extremism content, as exemplified by the tragic attacks in 2019 at two mosques in Christchurch, New Zealand. Shortly after issuing the Christchurch Call, the governments of Australia and New Zealand urged the OECD to undertake a project to develop a voluntary transparency framework through the so-called TVEC, or Terrorist and Violent Extremist Content Online initiative. This conversation will explore that effort as well as companies' initiatives to establish their own mechanisms for decision-making around taking down or leaving up certain content. Speakers will also consider the regulatory implications of these developments.

Moderating the panel will be Ambassador David Gross of Wiley. Our speakers include Sharri Clark of U.S. Department of State; Rich Clarke of AT&T; Erin Saltman of the Global Internet Forum to Counter Terrorism, or GIFCT—you may know it by that acronym – and Dina Hussein of Facebook. David, the floor is yours.

AMB. DAVID A. GROSS: Well, thank you very much, Barbara, and thank you to everyone for joining us today. Of course, because this is the Joe Alhadeff event, it is always bittersweet for all of us who knew and loved Joe. I have to say I'm a little conflicted that we're doing this on Zoom because I don't think anybody loved traveling and being in person with people more than Joe did. He loved the fact that he was constantly jetting off to various places, particularly the OECD. So, of course, in thinking about Joe, we think about both the substance and the personality, and of course, his loss is our great loss.

Barbara just outlined a little bit about what our panel is going to talk about. One other way of thinking about this is now that COVID is hopefully diminishing, and we are starting to get together with friends and family, I know many people have been wondering what do we talk about, having not talked to our friends and family for the last 15, 16 months or so.

If you were wondering what to talk about and you have a problem figuring out what to talk about, talking about terrorism, violent extremism on the Internet is always designed to get a rise out of everybody. Everybody has an opinion about it. Everybody is affected by it. So this panel is designed not only to tell you what's going on from the various perspectives but also to argue for that cocktail conversation that may otherwise be lacking.

To start things off, I'm going to ask Sharri to talk a little bit about what the U.S. Government's views are moving ahead on this very important OECD project, and what changes do we expect to see with the new Biden administration?

SHARRI CLARK: Thank you. I appreciate that. First, I want to thank the organizers for inviting us to speak, representing the Department of State, U.S. government, I have just finished a detail at the National Security Council. I wanted to start with that and also thank the OECD experts group for their important work on this project as well as the Secretariat.

It is fair to state the aim of this project, which has been undertaken over a fairly long period of time. The TVEC experts groups has been working on this for a while now. Noting a comment by one of the previous speakers that we can all agree on things like terrorism and weapons of mass destruction, I would say, yes, and agree that this is a priority for U.S. government and for other governments -- and for almost anyone. The devil is in the details. So how we address this is the real issue here.

It is also fair to say that most people agree that transparency reporting is an important step to better understand the problem. We have appreciated this project and its aim to basically develop a tool for voluntary transparency reporting -- a framework or a protocol for all platforms to be able to report what they're doing or what they're thinking about doing to build an evidence base for informing sound policymaking and also to hopefully avoid regulatory fragmentation.

Part of the impetus for this project is that we want to continue to focus on the voluntary nature of this effort. Also, a big part of this is encouraging all companies, not just the big companies providing online platforms and services. There is a huge variety of different companies involved, and I'm sure Erin and Dina and others will speak more to that shortly. But this has been a huge challenge, in a way, because of that.

Also, we think one of the greatest strengths of the OECD's approach is the multistakeholder approach. That continues to be critically important going forward. All of the stakeholders in this effort must be part

of the discussion and be heard, and their views should be incorporated into the final product. We've seen large platforms, Tech Against Terrorism, and GIFCT try to mentor small companies, realizing how difficult it is for very small companies with few resources to even think about terms of service.

We have argued for and think it remains important to start with a basic framework that everyone can utilize, which will hopefully encourage companies to use this framework. Also, another point we want to continue to make is the importance of respect for rule of law and human rights in this process. That needs to remain front and center in this effort as we go forward.

As you all know, identifying and addressing terrorist and violent extremist content for the United States is particularly complicated, as much of this content may be protected speech under the U.S. Constitution.

We also appreciate and want to continue to see the flexibility that this project has come to use, which allows the companies themselves to tell us how they define and how they will address what their policies are with respect to TVEC, how they understand it, and what they're trying to do about it. That leads us to the sort of basic framework that is going to be released publicly.

We think it absolutely is the right move to sort of release the framework into the wild and let companies try to use it, and then that will help us better understand what we got right, what might need improvement as we go forward, and continue this work in developing a more extensive sort of second-tier framework as we go forward.

The second thing for the future of this project is that we would love to see future analytical reports that quantify the extent to which this effort -- this kind of transparency reporting -- and other efforts, such as regulations, whatever national and international efforts are doing, to reduce the amount of TVEC online. We think that will help inform better policymaking as well as potential regulatory approaches.

In the long term, the United States has argued for and would support this as an ongoing effort after the OECD's great contribution and development. This as a foundation cannot be overstated. But as this goes into long-term development and use, we have thought and argued for the movement of this project to a counterterrorism-focused forum, for example, in the GIFCT, where there's already work going on and transparency reporting to include a focus on counterterrorism.

Those are the basics on the project. We again really appreciate this effort, and we've been very pleased to be a part of it, as complicated and messy as it's been at times, as so many stakeholders are weighing in.

In terms of the Biden-Harris administration's approach to this, President Biden has from the beginning made a priority of reassessing the U.S. government's approaches and efforts to counter violent extremism and terrorism within the United States, especially. You all will have seen a public statement about intelligence reports and a threat assessment. Part of that has been a released.

In addition, there will be a very intensive assessment of all of our efforts and what we need to do better, that is ongoing as well as other broader counterterrorism assessments and other kinds of assessments. This administration is taking this very seriously and trying to start with a stock-taking, a step back, to assess where we are and what we need to improve. I think the point is we're looking at a data-driven

analysis approach and a strategic approach before we make any changes to policy or possible regulations. Thank you.

AMB. DAVID A. GROSS: Terrific! Very, very helpful, and thank you for that overview.

For many people when they think about terrorism, they really—at least here in the United States, we often think about international terrorism. But the events of January 6, 2021 and other events obviously have refocused people on domestic terrorism. Do you see the administration refocusing and thinking differently about these issues because of concern about domestic terrorism as compared to international terrorism? Does that affect the thinking and the interagency process for coming up with positions?

SHARRI CLARK: Obviously, January 6th was a real wakeup call, not only for us in the United States, but it was a bit of a shock and certainly highlighted the importance of this issue.

We have, of course, been looking at the issue, "domestic terrorism," or violent extremism and terrorism within the United States for years. However, the changing landscape with the use of online platforms by groups and individuals who are loosely affiliated and influenced by things they're seeing online, this is a different kind of challenge. We have things like racially or ethically motivated, violent extremists or terrorists. We have differences in designations of international terrorist groups. We do not have that within the United States domestically, although, of course, we have statutes that apply to terrorism here. So there are a lot of things that we're looking at.

I think it is fair to say that over the last few years, but especially highlighted by January 6th, we are taking a hard look at domestic terrorism. The administration came in with that as a priority, though, of course, not forgetting international terrorism. We're seeing different uses of platforms by these groups, and we're working very hard to collaborate with tech companies, with other partners, civil society, in a whole-of-government effort, whole-of-society effort to try to address such terrorist activity together because, obviously, this can't be done by governments alone. This is one reason for this very strong focus and priority of these assessments.

AMB. DAVID A. GROSS: And speaking about broadening the conversation and governments not being able to do it alone, Dina, from Facebook's perspective, how do you see this project proceeding? I know businesses recently, I think in April, suggested that the OECD's TVEC project be paused. Can you tell us a little bit about what the current thinking is? I realize, of course, that this is a constantly changing set of dynamics, but from your perspective, where are we, and where should we be going on this?

DINA HUSSEIN: Absolutely. Thank you so much, David, and I really would like to, first off, thank David and Barbara for all their work around this panel. We appreciate all the support and being able to come to the table. But, also, I would like to thank all of our partners from the OECD because this process has been a very robust one. We've been involved in multiple calls, their ability to bring all of us together, and the ability for us to have a platform to take collective action when it comes to the transparency work has really been invaluable.

I think from the tech platform perspective, as I mentioned, there's been a lot of resourcing that's gone into this, and it's included a lot of resourcing that even for a big tech company such as Facebook has been quite a considerable investment, and I think we need to see how things pan out to ensure that

once we have seen the response to the first phase, allocating more resourcing and considering how we're going to address this more systematically in the long term is one of the things we're looking to do.

The other portion of this is really demystifying how other tech companies can get involved more robustly. I know that we've gone through multiple different processes of ensuring that as many other tech companies can come to the table as possible, especially in conjunction with Tech Against Terrorism and the GIFCT.

We want to make sure that we take a pause to enable new companies to potentially participate, uptake the baseline-level reporting that's already been created, and make sure that we're seeing how this process really manifests, whether it will encourage more tech companies to do this more often, which was one of the main goals. We're also hoping to see the response from smaller tech companies as well as ourselves around the level of details that they're able to share and the level of resourcing that is required for a legal perspective, from the tooling perspective, from the engineering perspective. We need to take stock of how this affects everybody in the ecosystem.

Another thing that I think we're interested in looking at is how the data that we're providing is going to be taken up by stakeholders that are outside of our industry. One of the things that we know has been highlighted as being extremely useful for us is to get clear context and background on either the goals or the aims or the policy rationale behind specifically the metrics that are going to be put out into the world. We want to know what's useful, specifically for that baseline. We can double-down on more resourcing around what's useful or maybe highlight what might not be as useful to the stakeholders and partners externally.

Then, finally, I really do want to emphasize that this is one of the processes that we're hearing a lot about from different stakeholders. As many of you know, the OECD has been a long-term partner of ours. We're also partnering around transparency with GIFCT. We're partnering around transparency with the Christchurch call to action. We're partnering around transparency in multiple different avenues.

To echo Sharri's point, we're hoping that at a certain point, we're able to also ensure that all of these efforts are not duplicated. When it comes to assessing who is going to do what, that's going to be interesting for us moving forward. I'm excited to hear from Sharri, Richard, and Erin about how we can partner with them, especially making sure that this is very counterterrorism-focused and ensuring that, where we can, we can rely on bodies like the GIFCT to take on a little bit more of the work and the partnership there as well.

AMB. DAVID A. GROSS: That's a great segue into Erin, of course. You talked a little bit, Dina, about what works, doesn't work, and so forth. Erin, are transparency reports the sort of thing that seems to work or not? Not all companies do it. Some do; some don't. How do you see it, and how do you see that fitting into the bigger picture?

ERIN SALTMAN: First, many thanks to USCIB, BIAC, and OECD for even hosting this conversation.

To your point, many companies don't have a transparency report. In fact, the OECD did some field work exercises and found that the vast majority of companies don't have transparency reports. This is a very daunting thing. There's a reason why a lot of companies don't have transparency reports.

First of all, the second you put one out, you know that you are going to be held to account to do that annually. For smaller and medium-size companies, this takes not just their data and engineering teams. This also takes policy teams, a lot of legal teams. Any time you're at a tech company, there's always a handful of lawyers in the room to just decide what you can and can't say and to decide transparency at what cost.

However, a lot of smaller companies, when we talk to them about joining the GIFCT, they mention that they're worried that certain levels of transparency might be great for governments and civil society but might come at a cost to them. They are worried about saying too much to the point that a bad guy can outwit the system or even sometimes be at the cost of user privacy, depending on how their platform is set up. We need to allay those concerns.

One thing about a first transparency report is the fact that you can't just speak to terrorism and violent extremism. A tech company knows that in its first report, there has to be parity across harms issues, such as all types of illegal content like child sexual abuse imagery or harms like bullying and harassment or spam, which is going to be much more prevalent than terrorism.

When GIFCT has companies join, we do have a membership process, and one of the membership criteria is to have at least an annual transparency report. However, you can't just demand that of a company because often they really don't know where to put their first step. Most companies we talk to say they'd love to have a transparency report like that of the 17 member companies that are a part of GIFCT. Four of the current members didn't have a transparency report before undergoing the GIFCT membership process.

So just having that as criteria actually brought companies to the table around transparency reporting, and that was in strong partnership with Tech Against Terrorism, who are our partners in doing a mentorship program with tech companies. As long as there is infrastructure for some hand-holding, I have yet to come across a company that says we just don't like the concept of transparency. It's more just that word. Without parameters and guidance, transparency could mean a million different things and have a lot of different risks.

One of the goals is something like the OECD baseline metrics, and baseline is important for most companies because usually a first transparency report might just say we removed X amount of "illegal content," and terrorism might be within that number. However, they don't have the data to stratify that point out.

We also need to support it with better multisector discussions. One thing that tech companies say all the time is that they can produce metrics that can speak to something as long as they know what the goal is. What does a government need to know? What does civil society want to know, and why? And when they know that why, then they can work backwards to see, "Oh. Well, this metric might help you," but when we say data and metrics and you work at a tech company, data can mean almost anything. Metrics could mean almost anything.

Having something like the GIFCT Working Group on Transparency, which is a multisector geographically diverse group that includes tech companies, human rights advocates, and the OECD. The OECD is, thankfully, one of the co-leads of that working group. It means that people can tease out the why, and then you see some of the smaller tech companies say, "Oh. Well, if that's what you're looking, we could

probably provide a little bit more on this if that's what's really helpful." Multisector discussion is extremely important. It's usually not the fact that a company doesn't want to be transparent. I have yet to come across that.

AMB. DAVID A. GROSS: Rich, so far, our conversation really has focused on what companies can do and should be doing and how they can do it. But, of course, in the conversation, writ large, there's a lot of conversations about regulators and the role of government. How do you see it? Should there be, for example, any sort of specialized platform regulator? How would they communicate with each other and deal with each other? How do you see it from a regulatory perspective?

RICHARD CLARKE: Well, first, let me preface my remarks by saying they're going to be mine alone and not necessarily those of AT&T, and just as Joe [Alhadeff] really acted as a free agent, I'm going to try to act that way too.

As to the issue of a platform regulator, I don't think we're intellectually there yet. Rather, I would prefer to see economy-wide regulators for things like privacy, consumer protection, antitrust, with each having authority over all industries to which that particular issue applies. This helps to ensure that there's equal treatment about a particular issue, no matter what industry is dealing with it.

That said, it may be possible that platforms' general market failures have no analogs outside of the platform industry. If that's the case, there may be a need for a regulator that happens to be platform-specific just because these issues don't arise in other industries. But as I said, I don't think we're intellectually there yet to define the platform-specific market failures that may exist. There's some commonality across platforms, but there's also a lot of differences that make it hard right now to envision a specific platform regulator.

AMB. DAVID A. GROSS: Well, along those lines—and this is open to all of the panelists—obviously, no one is really happy with the status quo, and everyone is trying to feel their way through. How do you see it? Should this be driven by an attempt to have self-regulation, despite the fact that obviously governments have a very strong interest on behalf of their people?

And most particularly, since this is a global set of issues, how do you envision that companies, governments, civil society, others ought to be communicating with each other not only at the OECD but elsewhere? Where do you see the action going forward? Dina, maybe I could start with you.

DINA HUSSEIN: Sure. Thanks, David. Very happy to jump in. I can only really speak to the Facebook perspective because, as Erin and I have always said, GIFCT and Facebook independently or Twitter or YouTube independently cannot speak on behalf of the entirety of the internet.

I am putting on my Facebook hat alone here. As many of you may have noticed, we've made calls for smart regulations – that is, regulations that are backed by informed understanding of how these tools work and of how these policies are built.

Recently, Nick Clegg, Facebook's head of Global Policy, wrote an impressive op-ed that outlines the four areas where we think there can be movement around regulation. That would include things like a reform of Section 230, which would take into account the movement forward that we've had when it comes to the tech industry. Second, the op-ed highlights how we could highlight more protection

against things like influence operations. Third, we really do hope that regulation can move us towards an area where there isn't as much of a gridlock when it comes to privacy regulation as well because these two things go hand-in-hand. Fourth, there is potential for a conversation around data portability so that we enable all of our different users to move their content and, to a certain extent, vote with their feet if they would like to move from one platform and don't disagree with their data policies.

And then, finally, Facebook would be interested in the possible creation of a digital regulator, of sorts, that's based in the United States. These are conversations that are not coming to an end anytime soon, and it would be useful to have an expert body that can parse these issues out.

Now, all of that to say, that is within the context of the United States, as somebody who is not an American despite the accent and works mostly outside of the Americas. I would also be wary that there is a little bit of a fracturing when it comes to all of the regulation, which has meant that there is a possible new area of isolationism when it comes to the protections being afforded to certain users and not others. There also might be a need for a conversation around the global protections afforded to users and not leave it up to companies to decide that these users get these protections, but these other users do not.

AMB. DAVID A. GROSS: Sharri, one of the core values of every U.S. administration is the free flow of information, access to information, and therefore, the importance of the Internet. Taking the issues that Dina was just talking about, where do you see the U.S. government taking this conversation? Obviously, the OECD is one place, but where else is the action going to be?

SHARRI CLARK: We continue to have global conversations with other governments and companies in so many multilateral forums and the UN about a lot of these issues, not necessarily always specifically on regulations. There is such a complex ecosystem here. There are so many issues that are intertwined with human rights, with regulations, with security. Trying to sort all this out has been really a priority for the last few years, and a lot of that being around roles and responsibilities of governments, of industry, of the public, civil society.

That is ongoing. For this administration, President Biden has expressed interest, as you all know, in reevaluating Section 230 of the Communications Decency Act, and so that certainly will be considered. As I mentioned, everything that you'll see from the Biden Administration going forward will be in the context of assessments currently underway.

It is too soon to say how and in what direction this is going to go for this Administration. For the current situation, our guiding principles, our policies remain the same, and I think that we will be taking a step forward on policy regulation in a little while. It's going to take some time to complete all of these assessments and really think about strategic approaches to any changes that may be coming. Thanks.

AMB. DAVID A. GROSS: My next question really is for both Rich and Erin. One of the concerns I think everyone has is that one of the core aspects of the Internet is that the technology, whether it's usage or otherwise, is constantly changing. I mean, the Internet that we know today doesn't look very much like the Internet we knew just a couple of years ago. So how do you anticipate that both industry, government, civil society, and others try to stay a step ahead or at least current compared with the usual fighting the last war all over again? How do you think we should go about thinking about these things? Rich, let me start with you.

RICHARD CLARKE: I don't know that the technology of the Internet is changing that much. The capabilities of various applications on the Internet are changing an awful lot. Tasks that we did not think would have been feasible back, as Facebook would say, in 1990 and 1996 to moderate content and to filter for various things are just multiple orders of magnitude. They are more advanced today with Artificial Intelligence and machine learning, and certainly, there are things that are far more feasible to be done today to filter out content that we think is undesirable.

But there's also the question about, well, how do we decide what content is undesirable, that this is something that differs between different countries, and it's very hard to draw generalizations. There's always going to be a conflict between what's in Country A versus Country B or just in different eyes of the beholder. I don't know that it's something that's amenable to boards of experts to make transnational decisions about. These are things that pretty much often there is agreement to disagree on and are going to have to be muddled out on probably a national basis.

AMB. DAVID A. GROSS: Erin?

ERIN SALTMAN: When we think about legislation or government perspectives, given the unique challenges each platform faces and the differences between platforms—so, for example, when we say terrorist content online, I'm pretty sure most people on the call, your mind jumps to think of social media, and that is actually already part of it but somewhat naïve and outdated compared to the diversity of platforms and apps that everyone is using. If you just took stock of all the apps on your phone, some of those are going to be social media, but a lot of them increasingly have to do with financial transactions or booking or storage, block chain.

All of those tools are used by humans, and when humans use them at large, they are also used by bad actors at large. We need to understand the diversity of what we mean when we say online regulation to not just think of a couple very big social media companies.

Within that framework, even those companies all have very different policies, tools, and user interfaces. There's increasingly this difference between, on the one hand, we could divide companies by big and small. On the other hand, we could divide companies by who has subject-matter expertise and who does not because you could be very big, but if you do not have counterterrorism expert inside, other than maybe the ISIS flag, you do not know what a bunch of these logos and symbols and references look like. You might be big and not have the subject-matter expertise.

Then thirdly, increasingly, what we are going to start seeing is that there are companies willing to come to the table and solve and troubleshoot together -- and then there are companies and platforms that do not want to come to the table. That's the point where maybe legislation is more relevant, particularly when we start seeing the companies, the same faces of companies keep coming to forums, keep trying to join entities like be at the table for the EU Internet Forum, communications with the UN Counterterrorism Executive Directorate, participate in the Christ Church call to action, and/or become a GIFCT member.

Then there are those that, even if you approach them, they actually do not want to be part of the dialogue or the solution, and so there are those voluntary mechanisms. When governments are overly prescriptive with the online environment or Internet of Things, that's when maybe we get bad

legislation. When a policy doesn't understand the nuance of how the online space operates, that's when we can get into hot water.

Lastly, we are starting to see legislation that starts contradicting itself in different parts of the world, and really, there is a constant battle between three pillars: those solving for privacy, those solving for security, and those solving for free speech. If you solve for just one pillar, it will always be at the cost of the other two.

Just as governments are having to navigate between those three pillars, every tech company is also having to draw policy lines between those three pillars. When we start seeing governments solving for one over the other and companies making different policies, we are starting to see clashes. This can become extremely difficult for a small platform to know how to stay just legally compliant in different parts of the world without pretty much breaking its internal systems or catering to one type of society more than another. These are big questions we need to ask ourselves.

RICHARD CLARKE: David, if I could just add that this is also linked to the business models of the different companies. Some have different business models that are based on, well, we're just trying to provide general information. Others have business models based on user engagement, and they think it doesn't really matter so much what the content is if it's engaging. And there's probably going to have to be a look at those as well if you are going to come to the root of the problem and perhaps a solution.

AMB. DAVID A. GROSS: Terrific! With the permission of the panelists and Barbara, let me try to do something which was not scheduled to do. Is it possible to get the extraordinary Audrey Plonk to weigh in here from OECD Secretariat perspective and see if we can technically—there she is.

BARBARA WANNER: Yes. I would like to invite Audrey to comment in the interest of inclusiveness.

AUDREY PLONK: Thanks, David, and it's good to see you. It's good to see everyone, and thanks for the rich discussion.

I just wanted to maybe provide a little context for the TVEC project to put into perspective some of the comments we heard. First, what we're trying to do with the project is to provide a harmonized way to collect information from companies about their moderation of TVEC on their platforms when they decide to report or when they're forced to report.

One of the issues that governments are very concerned about, particularly in the context of the OECD, is the amount of impending regulation around transparency reporting for TVEC specifically and a concern that those regulations will take diverging approaches to transparency reporting. This is exactly what the OECD does. It's our core mission is to harmonize at the international level the gathering and collection of data in order to turn that data into information that's useful and to create that evidence base that policymakers could build on.

So, while it has been a lengthy process, it's not as lengthy as many of our processes that many of you have participated in for many, many years. It has always had that as the motivating factor behind it. We are entering the third phase, and are very close to having a final set of baseline metrics that can be put out in that wild, as they say, to kind of test how platforms use it and respond so that we can iterate on it going forward over time.

The other thing I would say is to stress the voluntary nature of it. That also is an important thing about the OECD and the multistakeholder nature of it, that this is intended to be voluntary. Nothing the OECD does is mandatory, but it's intended to be voluntary.

It's intended to be a tool for governments and for the private sector going forward. Once we're able to share more publicly the baseline metrics, it will become more obvious how basic the information is that we're thinking about offering in the framework for companies to report on. There's lots of flexibility, and there's a decision tree, whether they say yes or no. There's lots of yes or no questions. There's lots of ability to provide text responses to some of the questions, and we've narrowed down a long list of questions that all the experts put together to a very small number going forward for that baseline.

I just thought I'd provide that little bit of context as we wrap up the panel, But thanks for giving me the floor. I really appreciate it.

BARBARA WANNER: Thank you, David and speakers, and thank you, Audrey, for stepping in at the last minute, unplanned, to make this an inclusive conversation.

Looking Ahead at the OECD Digital Economy Agenda

BARBARA WANNER: We're going to wrap things up with our "Going Forward panel," which will look at what we can expect in the future. In particular, one thing that I hope Audrey can shed some light on is how 2022 will be a special year for the OECD because it plans to host a Digital Ministerial in December 2022. Many of us remember the wonderful OECD Digital Ministerial in 2016 in Mexico. So our panelists will offer their thoughts about how the OECD as a global convener might continue to break new ground in tackling the challenges and opportunities presented by digital transformation of the economy.

Moderating this discussion will be Ellen Blackler, vice president, Global Public Policy of The Walt Disney Company. Ellen also serves as vice chair of the Business at OECD Committee on Digital Economy Policy Bureau as well as chair of USCIB's ICT Policy Committee. She will engage with Nuala O'Connor, senior vice president and chief counsel of Digital Citizenship at Walmart; Audrey, who you just heard from, of the CDEP Directorate; and then Makota Yokozawa with the Nomura Research Institute. Mac serves as co-chair of the BIAC's CDEP Bureau.

Ellen, the floor is yours. Thank you.

ELLEN BLACKLER: Hi, everybody. I think we will start with Audrey. For those of you who don't know, Audrey manages the OECD's work on the digital economy. Why don't you talk us through the four modules of the Going Digital III project that are going to form the foundation of the work going forward to ground us in what we can expect and how AI, the government access to data, and the TVEC issues that we've talked about today fit in going forward.

AUDREY PLONK: Thanks, Ellen. At the beginning of this biennium, which started in January 2021, we launched the third and likely final phase of our wildly successful Going Digital project. The third phase is, I think, extremely interesting and important, particularly for this audience, because it is broadly focused on data governance for growth and well-being. It has a focus on economic growth, particularly coming out of the pandemic, but also digital future around well-being, including things like privacy and data security.

There are four modules to the project. The first is access and sharing of data, which is probably really evident, again, to this audience, but that's where we're looking more deeply at governance, data governance models and frameworks for sharing data, getting access to data. I think we have some case studies looking at crisis situations -- like COVID but not exclusively COVID – and as Julie Brill mentioned at the very beginning, what could we have done if we had had more access to and better data, and how do we make that happen for the future? So that's the first module.

The second module is cross-border data flows with trust, in which we are partnering with the OECD Trade Directorate. That's where you'll find the work on government access, government access also on mapping, cross-border data flow models that trade has worked on, a follow-up on data localization work that we've done in the past, and generally this big discussion we had earlier around the importance of data flowing across border.

The third module is focused on firm's use of data for innovation, for competition and other things. For example, there, we look at data portability. We also look at competition issues, partnering with the Competition Directorate, and broadly speaking, how the private sector uses data to innovate and to grow. Data-driven innovation was mentioned earlier, the OECD's work on data for almost a decade now.

Last but certainly not least, we have a module focused on measuring data and data flows, and that's where we're really partnered with our Statistics Directorate to try to understand the value of data better. There's lots of different ways to measure data. It's difficult to value. It's also difficult to measure, but the absence of an interoperable way to look and value data, look at data and value it makes it difficult to understand its economic imperative. We're trying to break apart that problem a little bit in a new way with a few new approaches.

So we expect to wrap all that work up along with several other important workstreams like TVEC that we just talked about but also our work on Artificial Intelligence, which was featured in the conference today, into a Ministerial that should take place at the end of next year to really highlight all the rich work that the CDEP has done in the past—well, the past 2 to 4 years but even since 2016, the Cancun ministerial -- and then really chart the direction for the future.

As Andy said at the very beginning, the digital economy is the economy, and we said that back in 1996. But now we need to really live it going forward. Thank you.

ELLEN BLACKLER: It's good to get the overview of the way all these issues are going to be structured, the workstreams going forward. To round that out, before we dig in a little deeper, Mac, why don't you talk about the Ministerial from your perspective and what you see the goals being. What we can hope to achieve out of that Ministerial from your perspective.

MAKOTO YOKOZAWA: Well, thank you, Ellen. Yes. At past OECD Digital Ministerial meetings, we have issued big paradigms of these sessions. Joe Alhadeff was always leading the way for the new paradigm.

We need a new paradigm to realize the transformation of the next 6 years, and over the next year, we will be thinking about the key message. A key element will be the implication of trust. Trust, we have spent a lot of time discussing here today. Whether the word is used directionally or logically, explicitly

or implicitly, I think it is one of those key elements of the next new paradigm; for example, trust in government access to data held by the private sector, trust with the AI, and the list goes on.

At the same time, it is important to anticipate the meaning of the trust, and in particular for us, what it means for our business, this is very important. A new digital trust will reduce costs and risks in our business and help us focus more on our business resources on what they are meant to do.

As you also make your relations with customers and business partners more present and less stressful, the Internet is open, and it's first mission is to be connected from now on. A new paradigm should also be applied to the Internet structure itself that will ensure trusted access, trusted connection, a trusted structure for the next 30 years.

The challenge now for the next generation of the Internet will be how to create a digital infrastructure that will build the trust in the openness. In any case, I believe there is an economic debate in the OECD that will be exciting and it is a great to be a part of this circle and with our BIAC and USCIB colleagues, especially Julie Brigg, my colleague. Thank you.

ELLEN BLACKLER: Thank you. So the new paradigm is a good way for us to think about the work going forward. Nuala, it's a good segue to you because I imagine it's probably the case that Walmart wasn't really so engaged in these issues when the IPPs were first developed, but here we are now. Walmart is certainly part of the digital transformation from their vantage point, a global retailer online and offline. But how does this look to you? Because I think part of the new paradigm is all these new stakeholders who now understand or perhaps always understood, but now are really living this digital transformation. When you think about this agenda, what we're all looking at the OECD and those issues covered by the IPPS, do they seem relevant to what Walmart needs today? Are we looking at the right things for someone who's part of the new paradigm?

NUALA O'CONNOR: Well, thank you, Ellen, and a great thank-you to everybody at USCIB and BIAC and OECD and for all the great thinking that has gone into the IPPs and the work that's been done for the last many decades, in fact.

I don't know what Walmart's engagement was 10 years ago since I've only been at the company a year, and what a transformative year it has been! I came to this great American and now international and global brand at an incredibly challenging time for the communities and countries we serve and to lead a group called Digital Citizenship.

I should first start by saying yes, all of this matters because we do think of ourselves as a retailer. We are absolutely a retailer at heart and do a lot of other things as well and hopefully in the service of the public. But we are absolutely an omnichannel company, meaning we do things online and off, and we need our customers and our associates, what we call our employees, and our partners and vendors, wherever they want to meet us.

To me, that is a unique thing, and that's probably the number one message – that is, continue to think about the real experience of real human beings' lives and that they don't all happen online, although for many of us, it did happen a lot online this past year. That is not true of the majority of our associates who went to work in physical buildings, in stores and warehouses and in trucks and in all sorts of places.

It is a privilege to be able to sit in your house and talk about these great issues, but real people had to go to work in person, even under really challenging circumstances.

We want to meet and serve those people who come to us with all levels of different comfort with technology, with all levels of different suspicions or skepticism about technology and data collection. Hopefully, again, this new group that I'm so privileged to lead that is called "Digital Citizenship" is thinking about the company's role as a digital citizen in the Internet ecosystem in the digital world and also meeting our customers and associates as digital citizens with respect for their rights and respect for their dignity.

I love that people have been talking about trust so much today because that to me is the core of what we do and how we serve.

ELLEN BLACKLER: Thanks. I've been working in this field for what seems like forever, and a constant refrain that we've had is that these issues are really best addressed through the active collaboration with all stakeholders, including the private sector. We talked about that a bit earlier, as that was one of the hallmarks of this work at the OECD, that the OECD recognized that early on and brought folks in and developed ways to have that collaboration.

But another refrain has been how the work would really benefit from additional private-sector voices beyond what we think of as the tech sector. Nuala, you're kind of representing that here today. I think it would be really interesting to hear from you how do we get other companies to think about how these issues that we talk about here, AI and these principles, the trust paradigm Mac talked about—how do we get other companies to engage in this policy dialogue so we can make sure we're coming to outcomes that take everybody's needs into consideration and we don't have any unexpected outcomes because we haven't really thought of all the angles?

NUALA O'CONNOR: Well, thank you so much for that, Ellen, and I am also concerned about unexpected outcomes in lots of different places.

First of all, it's about thinking of every company as a tech company. I've said that for years. Every company is a tech company whether they realize it or not, whether you're manufacturing things, whether you are selling things, whether you are providing services, financial services and health care, human-centered services. I think it's also making our principles practical.

I always joke that I'm doing applied policy now that I'm in the corporate world again. It's really about making these principles live and breathe and practical for real human beings. We meet hundreds of millions of customers every single week, and so we have got to make sure that our use of technology and data are transparent, are ethical, are respectful, and are easily understood by people of all languages and all comfort levels.

It's really about being inclusive and making the principles and the policy work that for practical applied uses. We talk about this new digital transformation at Walmart. The reality is Walmart has been doing big data and big science and big tech for a long, long time. It's a big company, right? And it's been doing tech in supply chain and block chain and food safety and food supply chain and in really amazing transformative ways that keep people safe and get food on the table and do things that people really

needed not only in the last year but always. Where we need to think about these issues and these values are where it touches human beings, obviously, not just things.

But like I said, back to my main point, everybody is a tech company now. Everybody is using tech and maybe not always realizing that they are.

ELLEN BLACKLER: Mac, we work together a lot in multistakeholder forums, such as ICANN, the IGF, the G7 and G20 processes, where we, as business stakeholders, try to make sure that our input is considered, and other stakeholders are doing the same. What do you think lessons are for the OECD in the process of continuous improvement so that we can address the fact that everyone now is a tech company and everyone is a tech consumer? How can we broaden that conversation?

MAKOTO YOKOZAWA: Actually, this form of the discussion is the essence of the multistakeholder-ism, and we are business constituents, and we have guests from the government and also from civil society.

I recall that in some Internet public policy discussions, there was a debate that the multistakeholder forum and the OECD should be incorporated as one. What makes different is that the OECD explicitly states that all stakeholder groups, including the Business at OECD, participate according to a set process and with their own internal coordination.

Of course, most stakeholder groups participate responsibly in discussions outside the OECD, and there are structures that they are better suited to creating synergies based on the more free-flowing exchange of ideas rather than a statement of prior arrangement. Multistakeholder discussions are already a respected element, but to maximize the benefit, I think we need to maintain a situation where all participants are well aware of who represents what. I think OECD is doing quite well in this point. Thanks.

ELLEN BLACKLER: Yes. I'll make an observation. I worked with the OECD on the Child Online Protection Principles redo, and one of the things that I thought was interesting in that process that was helpful and improved the outcome and improved the broader understanding of the principles was that the staff took the outcome of the experts group and shopped it around. The OECD went to other trade organizations that hadn't been part of the OECD normal process. They said, "Here's what we're doing. Here's why we're doing. You guys look at it. Tell us what you think." I think the OECD did receive some input from private-sector organizations that wouldn't normally have been in the OECD orbit.

Audrey, maybe you can talk about how from your experience, both working for so long in the private sector in these forums and now being on the inside, what do you see? Tell us about the thinking you guys are doing about how to realize broader participation. I think it's an area where more is better.

AUDREY PLONK: Yeah. It's a bit of a balance always. It's not always just more, but the right participation for the topic.

I think within the OECD context, the CDEP committee is unique in that it has four stakeholder bodies represented. You may not appreciate that if you went to other parts of the OECD, you probably wouldn't have the same experience as you do with the CDEP. So that's sort of like pillar one, which is sort of the core. We value these stakeholder groups. We want them at the table. We work really hard to engage with them in between meetings to solicit their input, to prepare and work with them, and

BIAC is a wonderful example. We have CSISAC [civil society stakeholder group]. We have ITAC [technical community stakeholder group]. We have the labor unions represented. That's extremely helpful, but it's not where we stop.

We have other ways of engaging experts, whether they're in the private sector or any of the other communities, particularly academia or civil society, namely through the creation of these experts groups. I'll just go back to the AI work where our AI network of experts has now grown to 200 experts. They're not all from outside government, but the vast majority of them are. The AI Experts Group has now turned into four working groups across a huge stakeholder community, across many countries, not only OECD. It's a lot of work on the OECD's part, as you've seen, Ellen, from your experience with the children. But it's the core tenet. It's our core ethical and moral tenet behind the way that we approach our work because it is so important.

I do think, as we've learned from the trust in government access project discussed earlier, that it isn't always about more, but it is about the right people at the table and the right experts at the table. In that example, we have a really specific group of people that are experienced and able to talk about this very technical topic. Then we want to take that to a bigger audience that can then respond and react and help us take these principles forward to implement, and how do we take the philosophy that we share and the value that we share across OECD countries and actually turn them into actionable practice, actionable standards, actional policies. And that's where we do need that huge, broad community, not just to making the principles but then in implementing them.

For example, the AI observatory is an example of an implementation mechanism that I don't think we've ever done before at the OECD in this exact way where we're trying to study what do people actually do with this. Without that group of 200 people from all walks of academia, private sector, civil society, we wouldn't have the richness that is there.

I will also say that we're still a small team, and we do the best we can. So be patient with us. We have a huge mandate and a small staff, and we try to run at the speed of light.

ELLEN BLACKLER: Yes – this is a continuous improvement discussion, not a "you're doing something wrong discussion." I think that circles back to what Nuala was just saying about broadening the circle. We need to be taking that step of considering what do these principles mean in a way that's actionable to different kinds of businesses.

The emphasis that we've had in the AI workstream is serving as a model. We used it as a model in the children's work, that the principles are one thing, but there's really a lot of implementation focus. It doesn't end with the principles. We've all seen that over the last couple years this notion of implementation guidance or all of the work we do around implementation is probably just as important.

AUDREY PLONK: If I could jump back in, Ellen, just to say that it's one of the reasons I came back to the OECD. I wanted to get all of that rich work that is done off the shelf, including things like the IPPs, where you saw lots of people were like, "Wow! I hadn't really looked at those, but when I went back and looked at them, they're actually pretty good. You guys saw the future, and you wrote something down." I don't want to repeat that process. I want to build the evidence base and write shorter, more actionable things that can then get taken by a community of stakeholders, governments, of course, but beyond governments as well.

I think it's one of our strategic goals to make things more implementable. For that, we absolutely need your support and the support of the broad community because at the end of the day, you're the ones with the boots on the ground, as they say, with the experience in taking action.

ELLEN BLACKLER: Thank you, that's great! We're coming up on the end of our time, so we'll move to our lightning round. When I prepared for the panel, I went back and considered "What do those internet principles say anyway?" And then I went back and reviewed them. I want to hear from panelists what your first response was when you re-read them. What did you think? Mac, what did you think when you reread them after all this time? Unless you had them on your bulletin board and were reading them daily, anyway.

MAKOTO YOKOZAWA: Well, that's a very difficult question but a very important one. What would be the next new paradigm and next focus of the OECD? All of those items in the 2021-2022 Program or Work and Budget are very, very important. But one thing I just wanted to note is that much of our work as very much centered on the domestic policy discussions the OECD helps to harmonized this across many governments. That is the number one priority of the OECD's work.

But at the same time, and specifically after COVID-19, every country is isolated and fragmented. We need to talk about the focus on the domestic policy model or guidelines or any other principles, but also the importance of talking about the cross-border situation, how the regulation and the situation will affect our business, our cross-border business. That is very, very important. That means just looking at each tree one by one in the forest is very, very different from looking at the forest itself as a whole. Harmonizing with each other is important and having unified, collaborative action. So I would like to see a more specific focus on the cross-border environment for business.

ELLEN BLACKLER: I think that was one of the things that came through to me was that the Principles had been focused on that notion of interoperable policymaking, and the idea was not to have a mandate about who was going to do specifically what, but to set those principles for domestic policymaking so they are interoperable.

Nuala, what about you when you read them? What did you think?

NUALA O'CONNOR: So, to answer your direct question, I think they aged really pretty well. I think there are lots of durable principles, and I see threads of transparency and fairness, which to me are so important, giving the opaque technology that we are increasingly encountering in our daily lives, and fairness to all humans, regardless of their personal characteristics or comfort level with technology or familiarity or status.

The one area I really want to drill deep on in our future work is inclusion, really truly questioning whether we are including not only in our process in this conversation—and that's very hard. Multistakeholder-ism is hard, and it's hard to do because there are many people that don't even know the conversation is happening, but how do we create frameworks?

I always say to the folks at work, Walmart used to build a lot of buildings and stores in the real world. What is the architecture we are building for our digital world to serve customers and associates, and what are the values we are embedding in those systems, in the systems architecture, in the physical and digital infrastructure that will power the company and serve the customer in the next generation?

Because I think we have a real chance to be thoughtful and mindful and taking some of the great learnings from these Principles and the great work that Audrey and others do at the OECD and embed them, because some of these systems will be opaque and hard to interrogate.

ELLEN BLACKLER: That's a good note, I think, for us to wind up on -- this inclusion notion -- because I think while it was included, certainly, in the IPPs at the time, I think the stakes have changed for us. We have all learned a lot over the last year in different ways about the way that inclusion is presenting risk to us because we haven't done it great as a society and the opportunities, and of course, that technology provides an opportunity to do it better. In addition, we are all understanding more about the threats that it presents as well.

AUDREY PLONK: Thank you for organizing the sessions and for your partnership with the CDEP for all of our work. We couldn't do it without you.

BARBARA WANNER: Thank you very much, everybody, all of the speakers for providing such rich, substantive comments and very thoughtful analysis we'll draw upon, I'm sure, in taking this work in the OECD.

Before we turn off our laptops, I just want to recognize the outstanding USCIB team who made this event possible. First and foremost, kudos and sincerest thanks to Erin Breitenbucher who played an invaluable role in planning and executing what was our first virtual conference on Zoom, fraught with all sorts of technical challenges. Also key to the success of this event are Ed Ho, who is our in-house IT wizard; Kira Yevtukhova, our communications guru; Chris Olsen; Ashley Harrington; and Diana Mendez.

Thanks and my gratitude for everyone's generous support. Have a good day, everyone. Bye-bye.

[End of recorded session.]