THE BROOKINGS INSTITUTION

FALK AUDITORIUM

TECHNOLOGY, ACCOUNTABILITY AND INTERNATIONAL LAW

THE FOURTH ANNUAL JUSTICE STEPHEN BREYER LECTURE ON INTERNATIONAL LAW

Washington, D.C.

Thursday, April 13, 2017

PARTICIPANTS:

Introductions:

TED PICCONE
Senior Fellow, The Brookings Institution

SASKIA BRUINES
Deputy Mayor, The Hague

Keynote Speaker:

JOHN CARLIN
Chair, Global Risk and Crisis Management
Morrison & Foerster, LLP

Moderator:

JEROEN van den HOVEN, Moderator
Professor of Ethics and Technology
Delft University

Panelists:

JOHN CARLIN
Chair, Global Risk and Crisis Management
Morrison & Foerster, LLP

ALEXA KOENIG
Director, Human Rights Center
University of California Berkeley School of Law

MALIKA SAADA SAAR
Senior Counsel for Civil and Human Rights
Google

* * * * *

P R O C E E D I N G S

MR. PICCONE: Good morning, everyone. Welcome to Brookings. I'm Ted Piccone, a senior fellow with the Foreign Policy Program in the International Order and Strategy Initiative, and welcome to the fourth edition of the Justice Stephen Breyer Lecture on International Law.

I also want to welcome our viewers who are watching us via webcasting. We are very happy to co-sponsor this series on international law with The Hague Institute for Global Justice and with the support of the municipality of the Hague and the Embassy of The Netherlands in Washington.

Before introducing our speakers, let me explain why we chose the topic of technology, accountability, and international Law. Few of us doubt that the spread of digital technology and the Internet has vastly improved our knowledge of the world, our productivity, our ability to communicate instantly with each other, with millions of people around the world. But we now live in a world in which the intersection of these three concepts is fast becoming a chaotic traffic jam rather than an orderly movement of important principles, like access to information, justice, and human rights that are matched up to good practices that lead to positive outcomes for society.

And as in any bad traffic situation, accidents are bound to happen. Law enforcement's ability to protect the public is thwarted, individual privacy is violated, elections are manipulated, and victims wait for justice with no reply. What we need, in my view, is a set of rules, protocols, and standards that will help guide the many actors in this drama: governments, technologists, businesses, civil society, lawyers and ethicists towards better outcomes for the general public.

These rules are needed at both the national and international levels and they need to be harmonized in ways that protect our fundamental norms of human rights, rule of law, and justice. Not surprisingly, it was difficult to find just one expert who could integrate all of the complexities of this subject into one comprehensive answer. But we did find some of the very best minds who could, in true multi-stakeholder fashion, bring their expertise to the table and help us diagnose the problem and engineer some potential solutions.

Just briefly, since you have their bios in your programs, let me introduce them. Our keynote speaker John Carlin has unique experience managing these issues as the Justice Department's highest ranking national security lawyer, handling cases involving cross-border terrorism, espionage, and cyber threats. He now chairs the global risk and crisis management practice at Morrison & Foerster law

firm in New York.

After hearing from John with his keynote remarks, we will then ask Jeroen van den Hoven, a leading global thinker on ethics and technology at Delft University of Technology at The Hague, to lead a discussion with John and our two other panelists. We have Alexa Koenig, executive director of the Human Rights Center at the University of California Berkeley School of Law, who will give us a perspective on how technology can be used to advance accountability for grave human violations; and Malika Saada Saar, senior counsel on civil and human rights at Google and an outspoken advocate for women's and girl's rights throughout her career in law and advocacy.

After their discussion we will have time to take your questions before we break shortly before noon. Let me now ask Saskia Bruines, the newly appointed deputy mayor of The Hague, to make some introductory remarks from her perspective as a representative of the City of International Peace and Justice. Thank you. (Applause)

MS. BRUINES: Thank you, Ted.

Honored guests, ladies and gentlemen, it is a great honor for me to be here at The Brookings Institution, the most influential think tank of the world. And this is also a great honor for all of us that Justice Breyer gave his name to this lecture series. And I must say that over the last 12 months the Dutch were even more interested in the United States than usual.

First, the presidential campaign was the main focus and now everybody is watching your new president closely. And, yes, also in The Netherlands there is a lot of talk about the U.S. Supreme Court and the trias politica in your Constitution. And we admire your system with all its checks and balances. The judicial branch is the backbone of our democratic societies and thank you, Justice Breyer, for your commitments to our lecture series. We are very grateful for that. And thank you, Brookings, for your great hospitality.

Today at this Fourth Annual Justice Stephen Breyer Lecture hosted by the Foreign Policy program at Brookings we will focus on the intersection of technological innovation and international law.

Well, The Hague is at the crossroads of international law and warfare, including cyber threats. As you all know, The Hague is the legal capital of the world with all of its courts and tribunals. In The Hague, the world tries to prevent war with courts like the International Court of Justice in the Peace Palace, the only main organ of the United Nations based outside of New York. And if, sadly enough, war

breaks out, if conflicts erupt and escalate with all the violations of human rights that come with it, we now have tools to prosecute violators.

The Global Tribunal, the International Criminal Court to punish the war criminals, has a seat in The Hague. And The Hague is also rapidly evolving into a security hub. In The Hague, we have the largest security cluster in Europe, the so-called The Hague Security Delta. More than 200 companies, knowledge institutes, and NGOs are working together to create a better and safer world, a wonderful example of public-private partnership. Several other security hubs in the world are now studying this attractive public-private model.

Ladies and gentlemen, we live in extraordinary times. Terrorism is on the rise in the physical world and in the cyber world. Of course, these two are nowadays intertwined. The Hague Security Delta already has a wealth of knowledge in the field of cybersecurity. And, of course, we also need international regulations and laws in the digital world. The digital world offers us an overload of data. The smart use of this data -- for instance, the so-called Big Data for Humanity -- can be used to avert conflicts and to ease humanitarian and natural disasters.

But how do we protect digital privacy in a world without borders? And I'm very much interested in what our keynote speaker, John Carlin, will tell us. Under his leadership the National Security Division launched a nationwide outreach effort across industries to raise awareness of national security, cyber and espionage threats against American companies. In a transnational cyber world there definitely is an international responsibility concerning cybersecurity matters.

I'm also looking forward to an interesting panel discussion moderated by Jeroen van den Hoven from the Technical Delft University.

I want to mention one other person who is with us today, Dan Shefet, a French lawyer born in Denmark and based in Paris. Dan, where are you?

MR. SHEFET: Over here.

MS. BRUINES: I'm here, there. Raise your hand, please. Yeah.

Dan has specialized in IT laws, data privacy, and human rights on the internet and is an individual specialist for UNESCO on internet law. In 2014, he founded the Association for Accountability and Internet Democracy, and the main objective of which is to introduce a general principle of accountability on the Internet in order to secure the protection of human integrity.

Confusion over boundaries between good and bad users on the World Wide Web is growing. The necessary standards and protocols to applying technology to facilitate effective accountability are lacking. And during the working lunch after this event Dan will tell us a little bit more about his ideas concerning the setup of the seat of an international internet ombudsman in The Hague.

Ladies and gentlemen, I wish you all an inspiring session here at Brookings. Thank you very much, and I'm very honored to invite John Carlin to give his keynote speech. (Applause)

MR. CARLIN: Good morning. I am so pleased and honored to receive the invitation to give the keynote at this address. I was a little surprised because I'm not an expert on international law. And then I looked at the humble words of Justice Breyer when he delivered the lecture bearing his own name on international law the first time, which he began by saying he is neither an expert on international law or the law of other nations. And if Justice Breyer does not believe he qualifies, I assuredly do not. So for those of you expecting a discourse on the abstract nuances of Bavarian law, you will not get it today. Turn your webcast off.

What I did do was, as you've heard from background, confront a new type of threat in my job overseeing the National Security Division. The National Security Division of the Department of Justice was the first new litigating division in about 50 years. And it reflected a transformation in the Justice Department in our approach to threats that was driven by our nation's response to the devastating attacks of September 11th.

And the idea was simple: That prior to September 11th, we had failed to adequately share information across the law enforcement and intelligence divide. And that failure to adequately share information, be driven by what that intelligence showed the threat to be, had lead to the unnecessary death of thousands of people. And it was a mistake that couldn't be repeated again.

At the National Security Division that meant, in addition to certain legal changes that allowed the sharing of that information, culturally there was a change, and that the lawyers who prosecute cases through our criminal justice system would sit side-by-side with the lawyers who worked with the intelligence community to gain information about what the threats were. And that success would no longer be measured by the successful prosecution of a terrorist after the fact, when families are grieving and have lost loved ones.

That may be important to hold people accountable, but that's not success. Success

would be working through your legal framework, using all of the available legal tools to figure out how to prevent that attack from occurring in the first place, so that no one was harmed.

When you think about what the threat looked like then, and we became very effective at applying this approach, it really had to do with the movement of people and things. So old al Qaeda, in their strategic approach, relied on a model that involved getting people into a difficult to reach area in Afghanistan and Pakistan, training them, infusing them with further ideological fervor, and then deploying them back to commit complex terrorist attacks.

And, strategically, al Qaeda believed that success required them to do an attack of equal or greater scale than the attack of September 11th. That was complex and it required taking these people, moving them overseas, training them, redeploying them; multiple people getting things or objects into their hands so they could do attacks of devastating consequences. And when you think about what al Qaeda did in the attack of September 11th, like many of the issues we're going to talk about today, they took advantage of a change in technology that's caused so much good -- airplanes, that have allowed people to connect throughout the world -- and they took that technological innovation and turned it into a literal weapon of mass destruction to kill.

As we became better at that approach of working side-by-side across our legal departments and agencies and across countries to make it difficult for al Qaeda to do what it wanted to do, the threat changed. The new iteration of the threat, the growth of the Islamic State of the Levant, who is particularly good at taking advantage of this change, took advantage of a change in technology that we're all familiar with, which was the revolution in the way that we're digitally communicating, the boom in social media.

And what they did, just like al Qaeda had done with aviation, is they took something that has many, many positive and beneficial uses and learned how to weaponize it. And there, what they did was they took the low barrier to create very sophisticated propaganda. And when I say "sophisticated," we ran a program at the Department of Justice consistent with the all tools approach -- different than anything I'd ever done there in my years before -- where we met, me as the lead national security lawyer and then the head of our National Counterterrorism Center, we met with folks from Silicon Valley, with Hollywood directors, with advertisers, and we just said, this is the new threat. Look at what they're producing on social media as they try to turn human beings into weapons.

Essentially, they're trying to crowd-source terrorism. And what we showed them was, these are thousands of micro-targeted messages being sent out at the same quality as commercial advertising and targeting specific demographics, and they're sent out day-in and day-out. And it's having a real impact. It's changed -- just as our terrorism cases have been going down, they started to spike again and what we saw was different. In the United States, at least, there was no, thankfully, whole community that felt geographically isolated that they could target.

What we saw instead was a growth of terrorism cases across all 50 states. So the FBI director said there are investigations open in all 50 states. And during my last two years in the division we saw an explosion in the number of criminal prosecutions that we were bringing. We brought more cases than we'd ever brought before. And what did the cases look like? They weren't in any one particular region. We brought cases in over 30 different states and counting.

What they did have in common is the age of the defendant. In over half of the cases, the defendants were 25 or younger. And most troubling, in one-third, approximately, in one third of the cases the defendants were 21 or younger. In international terrorism cases that's simply never been the face of the threat that we've seen before.

And it's directly linked, I think, to the other phenomenon, which was that in almost every single one of those cases, social media was involved. And what it was is it's showing the success of this crowd-sourcing of terrorism where a terrorist group located overseas, outside of our laws, is deliberately targeting young and troubled people to try to convince them to kill where they live.

At first their message was come join us as a foreign terrorist fighter. And as the world through the United Nations, in an unprecedented resolution, unanimously said, we're going to work together to prevent foreign terrorists from coming from our countries into that region to do what they do. And what the Islamic State of the Levant does, make no mistake about it, is they murder Muslims and non-Muslims alike with impunity. They use rape as a political tool and a recruitment tool. This is the face of evil, and every country, no matter what our other differences, came together in the United Nations resolution several years ago to commit to combat that plague.

However, as we got better at preventing the movement of people into that region, they switched their strategy and said, kill where you live. And they used social media to do it and that's when we started seeing the spike. Message after message every day. It has a very small success rate. And

when I convened that group and was hearing from advertisers, what we did essentially was describe the threat consistent with our all tools approach and say, hey, the government's not in the best position to stop this message from reaching these people and working. What can you do about it?

And it was interesting to hear them analyze it. They're the ones who told me how sophisticated the advertising was. They looked at details, like how the Islamic State and the Levant put their brand -- so I had a little ISIL brand on each one of these micro-targeted demographic ads. And when I say slickly produced ads that look commercial quality, what I'm talking about -- and this is a literal ad -- it's not the devastating images of someone being slowly beheaded alive or burned alive, although they put that out. That's for people, to scare people who are their enemies and for those who have already joined the group. When they're recruiting they do something else very similar to what I used to see when I was prosecuting sexual offense cases, which is they groom.

So it doesn't start with that type of violent image. Instead, it starts with images of a handsome young terrorist overseas in the Levant handing out cotton candy to children. And that is what the picture of life is going to be like in the Levant. And these advertising experts were saying they did it in soft lens to make it look even more bucolic. That was the U.S. ad, when I went over to Europe and was talking to an audience there, and this goes to the micro-targeting. They had a very similar ad, also done in soft lens, also done with the brand, but there the terrorist was handing out, instead of cotton candy, Nutella, because that was the popular treat of choice for kids.

It shows who they're targeting, how sophisticated it is. And it couldn't happen except for our change in digital technology. That's why a terrorist overseas located in ungoverned space is able to reach in and cause a threat in the basements where children are playing online inside the United States, in Europe, and in other parts around the world. That's what the threat looks like when it comes to terrorism.

Let me expand that out a little bit to a different type of terrorist case that's linked to this new approach of crowd-sourcing terrorism. So, imagine you're at a private company inside the United States, in Europe, elsewhere throughout the world, and your information technology professional, your IT folks inside the company, the ones who are in charge of making sure you system is safe, say, hey, boss, I know we're in this mainstream retail company, we've got a trusted brand. Someone intruded inside our system and they don't look like they're the world's most sophisticated hackers. They weren't very good.

And what they stole was a relatively small amount of personally identifiable information: names and addresses. Way smaller than what we normally see, but don't worry, we got it.

The vast majority of companies around the world handle that on their own. They don't report it at that point, nor is it even a high risk event that gets reported up to their own executive management. And let's say a couple of weeks later the same guy comes knocking back on the door and says, Boss, we just received through Gmail, let's say, an email that says, give me 500 bucks through Bitcoin or I'm going to embarrass the company by releasing the fact that we were able to get into your system.

This also happens every day across the world and the vast majority of companies don't report. Sometimes it's referred to as "ransomware." And there are different ways that it can occur, but it's the same idea of extorting money for fear of cyber threat. And most companies either decide on their own not to pay, because they don't think there's that really great a risk, that somebody's bluffing, or they make the payments. As far as ransomware goes, $500 payment through Bitcoin, unsophisticated hack, this is about as low-end a ransomware threat as you're going to see. And most companies wouldn't report it.

In this case, and those are real facts, the company did work with government and with law enforcement, and lucky they did because it wasn't what it looked like. It was a low-level criminal trying to get $500, but it was also an extremist from Kosovo who had moved from Kosovo to Malaysia. His name was Ferizi and from Malaysia had hacked into this U.S.-based multinational, trusted retail brand company, and stolen these names and addresses. And then through Twitter had become friends with someone who was one of the more notorious cyber terrorists in the world at the time, a British citizen named Junaid Hussain, who had moved from London to Raqqa, Syria, where he was located at the heart of the Islamic State and the Levant.

He never met Ferizi in the real world, but through Twitter and other means they communicated. He radicalizes Ferizi and Ferizi provides those stolen names and addresses to Junaid Hussain in Raqqa, Syria. And what does he do with that information? He does what the Islamic State and the Levant had been doing, which is tries to weaponize it to crowd-source terrorism and culls through the list of stolen names and addresses for those who look like they're government employees because it's a dot-mil or a dot-gov, whether it's a state employee or a federal.

He then culls that into a kill list and, using Twitter, pushes that kill list back to the United States and calls on the adherence of the Islamic State and the Levant to kill these people by name, by address, using the stolen information that was entrusted with a retail company. A real case.

Because we're able to work together, we were able to take effective action. But what did it require? It required the United States working cooperatively with Malaysia to execute a criminal arrest warrant and Ferizi was arrested by the Malaysians, brought to the United States, found a lawyer, faced trial, pled guilty, and was sentenced to 20 years this past July.

Junaid Hussain was in ungoverned space in Raqqa, Syria, at the heart of the Islamic State and the Levant. He was killed in a publicly acknowledged military strike by Central Command.

Think about what that threat is and the speed at which it's moving. It requires us to do something we haven't done before. If you think of all the billions of dollars and energy that went into transforming how we approach cross-border terrorism threats after September 11th, almost all of that framework, time, and energy went into sharing within government and across governments.

This threat requires something we simply haven't done before and is an order of magnitude harder, which is how do you figure out -- how do you share that information with the private sector where most of this information and infrastructure resides? How do you share what you're seeing on threats effectively so they can defend themselves and take necessary actions? And how do you incentivize and properly encourage information-sharing back so that you can combat the threat? And how do you do that with a speed of threat that moves so fast, at the speed of digital?

I mean, think about this case alone. It's five different countries that you have to work across and the citizens involved are of five or six different nationalities. That is going to be -- is and will continue to be the new face of national security threats.

Let me switch there then to cyber properly. When it came to cyber-related threats I used to prosecute these cases. And when I did, I worked only on the criminal side of the house. And when I was prosecuting those cases, I worked with an FBI squad. There was another squad that did the intelligence. They were behind a literal locked, secured door, and I never knew what the heck they were doing back there and I never went on the other side of the door.

And as those of you know who are looking at the criminal threats, there was plenty to do even 10, 15 years ago on the criminal side of the house, so I wasn't banging on that door looking for more

work. Occasionally an agent would switch squads and they'd just disappear, never to be seen again, doing whatever they did on the intelligence side.

When I went over to the FBI to be chief of staff to then Director Mueller, the door opened. And one thing we were working on was how can we at the FBI share information across the different government agencies to get a better picture of the threat? And we did a pretty good job at the time. And, in fact, we had a giant jumbotron screen, much larger than the one behind me, and on that jumbotron screen we could watch in real time as nation-state adversaries hacked day-in and day-out into the United States, all across, and they'd hack something like a Brookings or a university, sometimes to steal information there, but sometimes just to hop from that university into a corporation. Then we would literally watch, because they had a visual graphic, we would watch the data exfiltrate out of the United States. Incredible intelligence feat.

Not a win, though. It didn't feel good watching it because it became clear what we're seeing isn't traditional espionage. It isn't the collection of intelligence for national security defense that's been legal under and recognized under international law for hundreds of years. Instead, it's causing real damage to real victims now, billions of dollars' worth of loss of intellectual property and trade secrets. And so we had to change our approach.

When I went back to the Justice Department to head the National Security Division, it became clear that, number one, we hadn't made the changes in this arena that we had made when it came to combating terrorism, so we weren't opening that door and sharing information. We changed that and created new national security cyber specialists in every U.S. Attorney's Office. The FBI issued an edict then that said thou shalt share this information with this new specially trained cadre, who know both the bits and the bytes and Computer Fraud and Abuse Act, and Electronic Communication Privacy Act, but also are trained to handle sensitive sources and methods, and now are read-in on what the actual threat looks like when it comes to national security actors.

And then we made a determination. We were going to change approach, take what had only been in the shadows of the intelligence world, just like Cold War espionage, and try to bring it out. Because if our challenge includes getting the private sector on board, we have to figure out ways to talk publicly about what the threats are so they can protect themselves and so that there's a will to take action.

That change in approach led to the first case of its kind: the indictment of five members of the People's Liberation Army, Unit 61398. This unit of the second-largest military of the world in China was targeting private companies for the benefit of their economic competitors. And when we charged this case it caused a fair amount of controversy at the time. Why are you bringing criminal charges against state actors? So let me talk a little bit about why.

Number one, you've got to look at what was actually happening. So if you read the facts that are put forth in that charging document, we go into detail about what this crime looked like, and what it looks like is theft. So you'd see, even though they were literally wearing the uniform of another army, they were going in and stealing things like right before a company here, a multinational company here, was doing a joint venture with the Chinese company where they were going to lease a lead pipe. You watch these members of the military go in literally the night before and steal the technical design specifications for the pipe so they wouldn't have to pay for it.

Or to use another example, this was a U.S. subsidiary of a German multinational solar company. They went in and there what they stole was the pricing information. So it's not always the intellectual property. They stole the pricing information. They used that stolen information to price dump and force that company into bankruptcy by price dumping. Then to add insult to injury, when that company sued for an unfair trade practice, they stole all the litigation strategy. A true insult to lawyers.

So what we were seeing is essentially anything that wasn't locked down, they were stealing. So that is partly why we brought it. This wasn't traditional intelligence collection, this was theft.

Secondly, and importantly, I think, for today's discussion, we never really made a choice that said it was okay to steal information. We just hadn't come up with effective way to deter it. But the fact is if we were allowing this to noisily occur day-in and day-out, I think Director Comey compared it to the actions of a drunken burglar in terms of how much damage they were causing in systems.

If we allowed them to noisily do it, it's like in U.S. law we have an example from our common law, which is if you let someone walk across your lawn long enough without telling them to stop, they have what's called an easement. They gain the right to walk across your lawn. International law, a large portion of it is international customary law. It's the same concept.

And so if you think about, it with that analogy, this case was like a giant No Trespass sign, get off our lawn. But it was vitally important to do this, to take actual action so that we don't set the

customary low bar as saying this type of activity is okay, but instead encourage other nations to be disciplined and stick to this norm that says this is not okay, this is not the way we want to live. You should be instead of investing all of that money into stealing this information, incentivize to invest this money into research and development.

That case was more successful, I think, than we thought it would be. We thought it was the beginning of a new approach. But it turned out to be, I think, quite impactful on changing Chinese behavior. Let me fast forward a little bit to the next major cyber intrusion.

So we had war gamed out for years what it would look like if a rogue nuclear-armed nation-state decided to attack the United States through cyber-enabled means. And we all got it wrong because we never pictured that the first big attack was going to be over a movie about a bunch of pot smokers. (Laughter) That is what happened with the Sony-North Korean intrusion. It's the only time in my career that I've gone to the Situation Room and had to brief the President, the National Security Council on the serious national security threat and start the briefing by trying to describe the plot of that movie, which if you've seen it, it's not easy to do. (Laughter)

But the reason why we treated it like a national -- not an act of war, but like a serious national security threat is what else was it? It was an attack on a fundamental right of free expression And it was also an attack inside the boundaries of another nation-state.

And so we wanted to send a message back not just to North Korea, but to all of the other countries and even non-state actors, who are figuring out what can we do in cyberspace? Is it different? Is it as many have described -- and it currently looks like, in some respects, the Wild West -- or is it going to be something governed by the rule of law?

In order to take that response, though, we couldn't have done it without Sony's cooperation. Right away they did the right thing and within hours were cooperating. That is the only reason why we were able to do what's vital in these types of cases, which is the investigation and attribution to figure out who did it. That's why we could, in less than 28 days, have the confidence that it was North Korea of such a high degree that the Bureau, in an unprecedented move, put it out in a public statement and the President echoed it from the podium in the White House.

The other thing we realized going around that Situation Room table, though, is that we were lucky in some respects that it was North Korea because unlike the well-honed system we had when

it came to putting in sanctions about the movement of people and things, so we had an effective regime for terrorists that we've used to great effect to deny funding and other means. And we had a sanctions regime set up for those who would proliferate weapons of mass destruction, but we did not have an Executive Order that allowed sanctioning for cyber-enabled activity. Even if it was activity that harmed the fundamental national security or economic interests of the United States.

Luckily, in that case, North Korea had done so many other things we had an available tool because it was North Korea. And if it had been somebody else, we wouldn't it. That's what led to, in April of that year, a new Executive Order that allows for the sanctioning not just of those who steal information or cause destruction, but significantly those who benefit, including companies or individuals, from stolen information. So even if the People's Liberation Army stole it, if the company that was the beneficiary, the rival company in China benefited from it, they could be sanctioned.

I think it was the combination of the criminal case, that new Executive Order, and a belief that we were going to continue to raise the costs because this was not an acceptable way, this rampant theft of information, that caused the highest levels of Chinese leadership to take a look at what they were doing and led to a breakthrough, a diplomatic breakthrough. President Xi sent a delegation, we negotiated with them on a so-called Four Points Agreement. And President Xi, along with President Obama, announced together as one of those four points that it is wrong to use one's military or intelligence services to target a private company of the competitive benefit of its rival essentially. That was the norm.

That breakthrough led to the G-20 adopting those same four points. I think that's the beginning in this Wild West of coming up with laws that we can all agree on.

Now, I wouldn't have had much of a career as a prosecutor and in law enforcement if agreeing on laws meant that everybody followed them. So the next step then is ensuring that we enforce those laws that we agree on. And you've seen us attempt to apply this new approach not just with North Korea or China. We had named four major actors that causes problems in this space: Iran, North Korea, China, and Russia.

So we've talked about North Korea and China. You also announce charges against Iranian-affiliated actors for their denial of service attacks that hit 46 different financial institutions, affecting hundreds of thousands of customers, and costing tens of millions of dollars.

That same group did what would violate another one of these four-point norms, which is they went in and accessed the sluice control systems of the dam in Rye, New York, the Bowman Dam. If that dam had been working properly they would have been able to remotely open the dam and flood the area that was down beneath the dam.

Now, as it so happens that dam wasn't working. It was down for maintenance. But we decided that our crumbling infrastructure should not be our first deterrence against cyber threats, so we continued -- so we did bring charges.

The last, and the one that's gotten a little bit of attention since then, is the Russian interference with U.S. elections, with the intent to undermine confidence. And make no mistake, this wasn't just an attack on the United States. This is part of a concerted effort against democracy and the principle that people should be able to freely elect their government, and they view it as a success. So in that instance, I think we were not fast enough, when you look back, attacking this new approach of figuring out who did it.

It was made public on October 7th, before the election, as to who did it. That was not adequate deterrence. After the election, on December, I believe, 29th or around there, you saw a deterrent action taken. If that had been taken pre-election, I think it would have had a far greater impact because it was actually one of the most severe series of actions that have been taken to deter. It combined sanctions against 11 different individuals or entities, throwing out PNG'ing, a variety of intelligence operatives inside the United States, closing two facilities, and releasing malware that Russians were using to compromise systems across the world.

But timing matters. And this is important, I think, to examine and try to learn whatever lessons we can with a clear-eyed examination because they're targeting European elections now. And we just heard the director of the FBI and the head of our national security agencies say to Congress several weeks ago in testimony that did not get enough attention -- there was attention paid to all sorts of other parts of the testimony, but not to the most chilling statement in it, which is they said Russia's going to do it again in 2020. That was their assessment. They may do it as early as 2018 and it looks like they're going to do it in Europe, as well.

This, I think, requires collective action around the world. And part of that model needs to be a concerted approach that says we can and will figure out who did it. That, two, we're not afraid to

make it public, as we've seen in other instances now, whether it's China or North Korea. And third, that there will be severe consequences and that we will continue to up the level of the consequences until the behavior stops because it's not acceptable to use concerted campaigns to try to undermine confidence in democratic elections throughout the world. That challenge awaits.

Let me end with one or two other thoughts. One, as we are trying to figure out how to combat these threats that are data-driven, be it Islamic State exploitation of terrorism or cyber-enabled attacks, including blended threats that combine criminal activity and nation-state activity, we have to do and figure out a better way to combat conflicts of los that make it incredibly difficult to issue lawful process in order to be able to take effective action. And this cuts across a couple different ways.

One is figuring out how to incentivize, and this is one of the four points, countries to, if some criminal activity is coming from within their borders, to cooperate, to take effective action to prevent another state's citizens from being attacked criminally or through nation-state means. A good example of how not to do this would be what was just revealed in the Justice Department indictment of Russian actors linked to the Yahoo case where, in that case, the FBI had sought to cooperate with its Russian counterparts, shared information about who the crook was what was committing criminal activity, and then they recruited that individual and started using him as an intelligence asset to use the stolen information from companies. So that would be an example of how not to do that norm. So that's one.

Secondly, when it comes to the movement of data across borders it is in the interest of human rights and the protection of civil liberties, it's in the interest of national security, criminal justice, and economic growth, I think, to encourage a regime where data can move freely. But in order to do that, we also need a regime where individual sovereign states feel that they have the necessary legal tools to protect their citizens. That is a hard problem to solve.

The failure right now of solving it effectively is driving towards data localization, which I don't think anyone, regardless of your perspective, thinks is a good result, whether it's for human rights, law enforcement, or economic reasons.

The frustration that I've heard all the time, and the U.S. is often the recipient of it because right now the largest companies are located within the U.S., is let's say I was meeting with a colleague in Europe or the United Kingdom and they said, well, look, when I'm investigating a murder inside by own state's boundary of one U.K. citizen on another, I need to serve process and often the email, other data is

essential to bringing the case. When I go to serve it on your company, the U.S.-based Internet service provider they say it's forbidden under U.S. law for me to provide you that information.

Instead you need to use what's called a multilateral assistance treaty, or MLAT. I'm only exaggerating slightly, but MLATs are essentially older than the dawn of time and require you to do something in quill, in quintuplicate, and with a thousand pages on yellowed pamphlet. And so they are not efficient. They take at least 10 months. So to tell a local police officer your investigation's on hold while you make this international legal request of another country has not been a satisfactory answer.

Because of that, there's increasing pressure then. They're taking action anyway and the pressure now, in a lot of cases, is forced to either, in some cases, arrest company officials for failure to comply with the process; or, in other cases, demanding that data on citizens be held within the country's boundaries, which maximizes the ability to access it for other reasons, as well.

So one approach, I don't have that much confidence now that we're going to be able to solve this problem for the whole world at once with some massive treaty. So instead, one approach that we were trying with the United Kingdom was if it's a country that fundamentally shares our values and we provide equivalent, not necessarily the same but equivalent legal protections -- a judicial-based process, a certain standard of proof that you have to hit under the law -- that if it's an investigation that involves your own citizens, essentially takes place on your territory, that instead of using the MLAT, you can serve the same type of process you would serve inside your country.

That model, and, you know, there are complexities in the details, but a version of that got introduced by the Justice Department in the Obama administration in July of last year, and one reason I'm curious to hear your people's thoughts. But I think that a good potential model would be if you can one-by-one get countries to join on, show that it works, that it's respectful both of privacy and civil liberties, and allows law enforcement to do their job. Then I think it creates a bar that other countries will be encouraged to increase their legal protections, civil liberties protections, and others, because they want to take advantage of this type of treaty arrangement. And it will reduce the pressure for law enforcement or national security means for people to come up with their own solutions and it places companies in the unenviable situation of being right at the center of a conflict of laws.

So I will close there and just say as we approach these, I'm so glad we're holding this topic today, but it's never been more urgent in terms of what the threats are that we're facing and our

respective national security communities are facing. And we're right at the cusp of another technological transformation. So as much damages can be done by the free movement of data that comes from exploiting a move where we took everything that we value that was in analog -- papers, books -- moved it into digital space, then connected it through a protocol to the Internet that was never designed with security in mind. We did so at an incredibly rapid pace without accounting properly for risk and we're playing catch-up. That's where we are.

We're on the cusp of another change, though, and this is the so-called Internet of Things. This is billions and billions of new devices that are already starting to be rolled out that connect everything from pacemakers in our hearts -- the first versions that were rolled out didn't have encryption and were hackable; to drones in the skies -- same thing happened there; to cars on the road.

By 2020, even if they're not self-driving, essentially, according to most studies, about 70 percent of cars on the road are essentially going to be computers on wheels. And as was shown by a proof of concept hack where someone came in through an entertainment system, took over the steering and braking system, that led to the recall of 1.4 million vehicles inside the United States. Those, too, were rolled out without taking security into account in the design process. And it's not through bad intent. It's that the incentives were does the product work as designed? And the answer for the pacemaker, for the drone, for the cars was yes.

What they weren't adequately taking into account was what would happen if a bad guy, a crook, a terrorist, a rogue nation-state chose to take advantage of vulnerabilities? Have we built in security by design?

As we're on the cusp of this transformation there might be, you know, just in one area alone, might be as significant as when you move from a horse and buggy to a car with a driver is going to be the move and the impacts on society from a car with a driver to a driverless car. We have to get that right on the front end and the time for that is now.

Thank you. (Applause)

MR. VAN DEN HOVEN: While we are being wired up, John, thank you very much. It was a very inspiring and insightful story you told us there, very good illustrations also of what we have as a general topic here, accountability and international law, and technology.

We are very privileged to have panelists here, Alexa Koenig and Malika Saada Saar. They both have an impressive CV and record in this field of dealing with human rights and international law and new technologies.

So, as a starter, I would like to ask them to respond to your story, and then we have some more remaining general questions to the extent that we haven't addressed them yet, and then later on, we will open up to the floor.

First, as a matter of order, a practical thing, I've been told this is about accountability and technology, this is being Webcasted live, so if you don't mind, and if you do mind, you will have to adjust to the situation slightly.

Alexa, can I start with you and ask you to comment or raise some questions?

MS. KOENIG: Thank you, first of all, for your comments, and also for having me here. It's a big honor, of course, to be here. A lot of these issues are so salient and so timely, and I feel like we're really racing to play catch-up at this point from a law and a policy perspective.

You gave us certainly plenty to respond to in the comments that you pulled together. One of the big things that really stood out to me was the concept of silos, and how critical it was, particularly after the events of 9/11 to break down silos between law enforcement and other sectors of society.

I think that's a trend that we need to push even further. A big piece of this, I think, is really going to be figuring out we finance the different bodies of knowledge that are out there in society more generally.

Just to give an example, one of the things that we're experimenting with on the UC Berkeley campus is we have a human rights investigations lab that we're trying to use to break down the silos among disciplines on campus, and pull together teams of students who work in computer sciences with people that are working on law and policy issues, with investigative journalists, with people who really understand the cultural complexities of a lot of the areas in which we are seeing conflict today.

We right now have 60 students working together that represent 25 different disciplines. Among them, they have 18 different languages. The idea is can we pull together sort of rapid response teams as conflicts erupt or as information is shared from the field, so they can be learning from each

other about the methods at their disposal, and creating more systematic and creative solutions to some of the challenges that we're facing.

So, I do think another piece of the breaking down of silos is not only between government and private corporations, but thinking how we can better tap into and harness the institutions we have at our disposal, leverage the incredible wealth of talent and creativity on college campuses, and then also think back from a temporal perspective even earlier.

Another thing that you mentioned that I think was so important was thinking through the temporal chain of relationships and responsibility. You mentioned that accountability comes too late, we can't just rely on the legal accountability piece to solve a lot of our law and policy challenges, so we need to think how to prevent these issues from the outset.

You also spoke about the weaponizing of people. I think if we turn that on its head and we think through how we can reach earlier down our own chain of responsibility and how we can build a citizenry who is much more digitally literate than the one we have today, who really thinks critically and creatively about how decision making happens.

Amnesty has been piloting this really exciting project called Our Digital Verification Core, where they are basically trying to link students on different college campuses to look at photos and social media posts that are erupting from conflict areas, and teach students how to analyze them, how to debunk them, how to think through critically, how to address them.

I think if we have a population that is trained in those skills from the outset, and I mean starting back in pre-school, we're going to have a very different way of approaching this new world that we have found ourselves in about how we communicate.

The piece around emotions, I think, was really critical that you raised as well. You talked about how there were social media tools that were put together that showed people handing out Nutella or cotton candy. I think better understanding and thinking through how people engage in decision making about what to do, whether it is to engage in terrorist activity, who it is that you are going to support from a political or policy perspective, has also been somewhat neglected.

Those are insights I think we can really gleam from the sociological sector and other potential partners. One big example that I always try to grapple with is on decision making, there are sort of two strains of populations that have been identified. One is people make decisions based on what they

see as the moral rationale of the underlying substance of a phenomenon. Another is that people make moral decisions based on sort of being law abiding citizens, and probably people in positions of authority.

I think when we can basically harness those two different ways of thinking, we're going to come up with policy messaging that becomes much more powerful than it would otherwise.

One quick example from that, I like to use the example of whether you put your child in a car seat, and why you would actually go about doing that. Well, some people do it because they think morally that's the best way to keep their child safe, so it's a much more substantive perspective. Others do it because it's the law, and they know they will be penalized if they don't do that.

So, really creating kinds of tools and technologies that think through how people make decisions around those two different frames, I think, could be quite helpful.

The data sharing piece. I think the need for thinking through data flows is so incredibly important. One of the hats that I've been wearing is to help administer the Peck Advisory Board for the International Criminal Court, and talking with major tech companies about how can we facilitate access to information that will ultimately link the highest level of human rights abusers, war crimes perpetrators, to these bottom level people on the ground who are committing the rapes and murders.

Well, a big part of that is tapping into social media and the ways people are communicating today. The challenge, of course, is when we meet with the major tech companies, they say we will go through a legal process.

The problem is there are several barriers to going through that legal process, one of which is the International Criminal Court, a new kind of institution, and the kind of institution that we might see increasingly on the global stage, where you're looking at an organization that's not tied to a particular state, but to a particular function.

So, they can't necessarily use the same treaty process, for example, that would be used by a state government. What are the different ways we can figure out how to create new systems of information sharing that ultimately facilitate that process.

Two final points. Transparency is such a big part of all of this. I think the more we can be designing policies and technologies that are transparent, the better off we will be.

I said this, and to some extent, I'm joking, but to some extent, I'm not, I almost feel like we need a Google translate at this point for basic algorithms, or at least better training for people in

society, around how to think through, how to design algorithms for access to information, but also to better understand what they're doing.

It's going to be such a big piece of how we move forward and how we can actually make smart calls about next steps. Transparency is such a big part of what government relies on in order to have trust from people, much like those of us who are working in the human rights space. I think the only way we ultimately engender trust is by actually pushing forward with transparency.

Last, I think that listening to you speak, one of the things that really jumped out to me is also more creative thinking needed about how we not only combat tech challenges today with more technology, but how we think through low tech solutions to these high-tech challenges, and even no tech solutions to these high tech challenges.

I think so much of our focus right now is on the shiny object of how we deal with stronger encryption and new tools, but it's a race to the bottom in some ways, and sometimes, it's a race to the top.

Just using very basic examples of the experimentation that's happened with how do we knock a drone out of the sky, do we do it by jamming a GPS signal or do we train hawks to knock them out? Do we de-mine a particular war zone by creating new technologies to locate these mines, or do we train rats to actually sniff them out and help us locate them. Do we ultimately figure out better encryption practices, or do we actually figure out how we take things offline and actually not use technological tools, and when is that most appropriate.

I think there's a lot of experimentation and thinking we can do. Thank you.

MR. VAN DEN HOVEN: Thank you very much. That is quite a list, and rightly so, because the lecture raised a lot of points. Are there some points that you would like to off the cuff immediately reply to?

MR. CARLIN: I think there were many good points made. One is I fully agree on the cost disciplinary approach, and talking about the National Security Division and its creation.

Prior to that, it had been four different sets of lawyers reporting to four different chains, so those who did prosecutions reported through one chain. Those who did the intelligence authorities and oversaw compliance with the intelligence collection laws were through a second chain. A third chain was

the lawyers who did the regulatory work, to review national security threats, like investments, through the Committee on Foreign Investment inside the United States. Another chain who did the cyber.

So, putting them together and allowing that expertise, and that's just in one field of the legal perspective, I can't imagine how it was done before, having inherited it after we had done that cross disciplinary approach.

As I was saying, in terms of meeting that was new for us, but when it came to changing the way people -- potentially hardening your populous, so critical skills to not be prey to this type of propaganda technique, that's exactly why we were meeting with these experts.

If you had predicted when I joined the Department of Justice in the late 1990s that I'd ever wear my prosecutor hat be meeting with Madison Avenue advertisers, Hollywood directors, Internet service providers, and human rights groups, I would never have predicted it, but that is why and partly why we are saying this is not a problem we can solve.

We need to continue to bring criminal cases against terrorists at this rate until we have a better solution, but success is not locking up 21 and under. Success would be figuring out a way -- it used to be our long-held assumption that you couldn't get someone to go from an idea to a violent act without meeting them in the real world. That's clearly changed, and in so many other ways as well, really trusted friendships entirely online and through social media.

How do you change that dynamic? Is there any message coming from the government -- I'm still wearing suits even though I'm out -- but it is not going to be effective with the disaffected 21 year old set and under set.

How can you incentivize and educate people in the private sector, whether it is the human rights community, advertising, et cetera, to see the challenges and then apply the same creativity they are doing day in and day out in other fields, to whole new approaches that we would never think of.

I can assure you I had never used the term "micro targeting" of a demographic for advertising purposes until we did this type of meeting.

I think it raised some very vital points.

MR. VAN DEN HOVEN: Alexa mentioned the experiment that's going on with Berkeley, of bringing those people from different disciplinary perspectives together to tackle those hard problems.

Have you seen or come across other examples of this? You described your discovery, finding out the hard way, more or less piecemeal engineering, all your cases were this works, this doesn't work. Have you seen examples where people are doing this systematically, pursuing this building of a research agenda to educate the next generation of academics and entrepreneurs that have that under their belt?

MR. CARLIN: I don't know that I've seen it in particular projects. I'm going to use a government phrase and then correct it, so we called it "countering violent extremists," but the first thing we heard when we actually met with people who were experts was that's a terrible name because you will never win something that has to do with countering, you need to instead have something they are for. Nevertheless, the name has stuck.

I think in that arena, I've seen it. I think the Belfer Center at Harvard is trying a similar approach. I look forward to hearing from others as to what they think.

MR. VAN DEN HOVEN: There are a couple of points, and then we will go to Malika. Another point that was raised was the issue of transparency and algorithms, and the new European data protection regulation will require this explanation or explainability of what is happening under the hood, let's say, literally under the hood in the case of the Volkswagen.

It's not obvious from the outside what's going on, and if it's starting to affect people in a serious way, we should be able to explain, and the relationship with trust, of course, if we cannot do that.

You haven't mentioned trust. Can you say a little bit about that?

MR. CARLIN: Yes, let's start with the second first and then come back. Your last point was about how we shouldn't think necessarily of a tech solution to tech problems. I mentioned one version of that, which was the critical thinking.

I said in the remarks about how the Bowman Dam attack wouldn't have been successful if they had chosen to execute that authority because the dam was down for maintenance.

It is also true that the Russian affiliated actor attacks on the Ukrainian power grid were not as effective as they could have been in part because that power grid was 30 some years out of date. The operators knew how to operate it manually, because they hadn't completely switched to a digitally operated system. That actually caused it to be resilient in a way that you then see with our electoral system.

I think you have heard people talk about the fact that one of the reasons why, even though they may have attempted it, people had great confidence that on scale, the actual votes, although there was other mischief, weren't affected. Well, the U.S. system is a complicated hodge-podge of thousands of state and local systems, some of which are digitally connected and some aren't, which makes it incredibly hard to impact on scale.

In none of those cases was it designed with security in mind, but I do think now that we're thinking about -- which we didn't do as we put a lot of these systems online, if you start thinking and measuring risk on the front end, making choices, which are here are the benefits, but here are the realistic appraisal of the risks, that a new way of thinking will be there are certain things that just shouldn't be connected to the Internet.

Similarly, there may be certain information that you don't want to have online, or if you do, you want to have segmented it, encrypted it, or used other easily available tools, that are inefficient, but if you have done an adequate tradeoff on risk, you may decide it's worth the inefficiency, which would be a different way of thinking.

On transparency and trust, I think I was talking about transparency in a way that doesn't get as discussed as much but vital, which is we weren't doing a very good job of talking about what the threats are, what the intelligence was that we were seeing.

That inability to talk about it publicly then helped feed the continual discounting of risk, I think, in some of these areas, that then leads to new systems that continue to be vulnerable. That was one of the cycles we were trying to break by having a new approach of bringing things into the light using some existing tools, like the criminal justice system, where you have the means to make public charges, you have a system where you can adjudicate it rather than treating it as an intelligence problem.

I think transparency in different ways is important with each of the authorities, and certainly in any Democratic country, you cannot do the job you're expecting to do to protect your citizenry without their trust.

It's particularly true when you're dealing with challenges that are in the case of terrorism, where you need -- the way we were able to resolve most cases and the message we are getting out is somebody spotted it, like here's a troubled individual, looks like they're moving toward violence.

If we intervene early, it may never hit the criminal justice system, because they never go from idea to violence. You can't do that if people don't trust what happens, if you make a referral or if you seek help outside your community.

MR. VAN DEN HOVEN: Would you say that is one of the major challenges, designing those new institutions and intelligence agencies and their protocols and procedures in such a way that we can strike a balance between let's say protecting privacy and fundamental rights, and on the other hand, efficaciousness or effectiveness in crime fighting and fighting terrorism?

MR. CARLIN: I think sometimes it is objected to, to treating it like two different things or a balance. Often the privacy that you're protecting, maybe because someone -- right now, the greatest threat to our privacy online, I don't think here or in Europe, is from the government. It's from the variety of criminal groups that are taking and selling your information on a very effective black market, and nation states that don't share values that target you because of what you think or say for human rights violations.

So, in many respects, having a rule of law, the way to do that effectively, I think, can accomplish both, and they marry up.

The other thing I'm finding when I'm outside, and curious of others' thoughts, if we had a system of carrots and sticks designed to encourage people to share information, we don't have that rightly calibrated right now, so even when there's trust say of law enforcement to share information, there is great uncertainty in one state, there is great uncertainty as to whether or not they are violating the laws, regs, or rules of another state in which they're operating.

And then there are uncertainties within that state of what's going to happen to me on the regulatory side, am I now going to get hammered for having failed to keep the information safe, for privacy or other reasons.

You want to incentivize both. I don't think we have it right now, and it's great when you're a lawyer on the outside because it's an area of massive confusion and conflicts of law, so if you want full employment for lawyers, this is a good regime.

I don't think for policy purposes it's great, and the answers we give are often I don't know or it depends or you have to make a choice. If you cooperate in this regime, you're violating the laws of the other regime. That's not ideal.

MR. VAN DEN HOVEN: It was interesting to see how you talked about the FBI and the door, so these are kind of designs of how you structure your particular situation to let information pass through, or the relationship between government and companies, in the case of protecting people.

There are some other questions I would like to come back to later, but first, I would like to ask Malika to react.

MS. SAADA SAAR: I'm going to take this in a very different direction.

MR. VAN DEN HOVEN: Sure.

MS. SAAR: I think what you shared was a narrative of causing the challenge to borders, you know, the 20th century in many ways was a century of the creation and entrenchment of walls and borders, certainly the 21st century is a narrative around surmounting and collapsing and dismantling walls and borders.

The world in which we are in, this new digital reality of borders being collapsed and the implications of that around national security, around shared data, all of that is there, that is a narrative that is powerful, that challenges us in terms of law and policy.

From a human rights perspective, I want to tell another story that stands alongside what you have shared, and that's the story of what human rights looks like in a new digital context, and the intersection of human rights and the advancement of tech.

I think about this in a very different and real way. I think about this in terms of the story of Mamie Till. Mamie Till was the mother of Emmett Till. In 1955, Emmett Till was a 14-year-old African American boy who was visiting family down South, and ostensibly whistled at a white woman, and that night, he was pulled out of the bed he shared with his family, he was beaten, lynched, and thrown into the water. His body was retrieved.

Mamie Till said I want the world to know what happened to my boy, so she insisted that he have an open casket, and that the pictures of his mutilated body would be photographed and then shared with the world.

That was the beginning of the civil rights movement, that there were conversations that civil rights marchers had years later, talking about it was the image of Emmett Till in the casket that led me to fight for equality.

I think about Mamie Till when I think about the power of tech around human rights abuses, because every human rights abuse, every war crime, every act of abuse, so often is in the context of the walls, and the isolation, and the silence, and the ways in which tech allows us to surmount the isolation and the silence that always protects and perpetuates human rights violations.

The most powerful example of this is one within this country that we see has happened in the last couple of years, and that's police brutality. The conversation that we are having around police brutality now is a very different conversation than a decade ago.

A decade ago, the conversation around police brutality mostly happened in black and brown communities. As a result of the Smartphones that we have and the ways we can capture video of the police beatings, of a man being choked in Staten Island by police, the ways that video has been captured, and then shared on global platforms like YouTube, has completely changed our conversation around human rights abuses that happened within law enforcement.

It has become a popular square conversation. That is because of the ways in which what has isolated us within our own country around race and culture, those walls were surmounted by the power of these technologies, of the Smartphones and global platforms.

I think about that time and again, whether it's the story of an individual activist in Uganda fighting for LGBT rights, who is beaten, and that video is then shared on global platforms, so we as a global community bear witness to that human rights violation, and the space between the U.S. and Uganda is collapsed, and its human rights violation is witnessed and rallied against.

I really have come to believe as a human rights lawyer more and more that the more digitally connected we are, the less opportunity there is for wide scale human rights abuses and genocide. It is because of how we can collapse the walls and the spaces to be able to bear witness, to be able to disrupt the silence and isolation that allows abuse and genocide to play out time and time again.

I also have remarkable hope and hope that some of the conversation we have here in talking about this intersection between human rights and tech can also go to the opportunities to create technologies to be able to better hold accountable war crimes.

As you spoke about, the app of eyeWitness to Atrocities, right, that allows anyone with a Smartphone to be able to capture a human rights abuse, and then what plays out because of this app is it

is giving time, the GPS locator verifies where it has played out, it is encrypted, it is shared at a data center that is part of the app, and there is a panic button that can be pressed to dissolve all of the connection to the individual who has videoed that moment of abuse.

I'm fascinated by the opportunities that we have to create a space between engineers and human rights defenders to create more of these kinds of technologies that can be used to go after war crimes.

I mean imagine if we had that during Bosnia. Imagine if we are able to hold Assad accountable for the war crimes in Syria, what we will have to be able to charge him with is so much more powerful because of tech than we ever had available to us in Bosnia.

That is part of where I hope this conversation goes as well, because it is the other part of the conversation around the promise and the potential of how we actually can move human rights forward because of what's available to us as digital tools.

MR. VAN DEN HOVEN: Thank you. John, would you like to respond?

MR. CARLIN: I think there is great --

MR. VAN DEN HOVEN: Potential there.

MR. CARLIN: Potential. I think it's a mistake to assume that because we've had a change, and I think you would agree, that the change in technology does not equal walls down, borders down, and a new world in which we are going to live in freer, safer regimes that are more protective of human rights.

I think there is great excitement that was kind of occurring on its own as regimes fell, repressive regimes fell for a period of time in the Middle East, and people talked about a social media revolution in the way people were going to govern in the future.

That's not where the trend line went, unfortunately. If you look now, and this is part of what I was addressing, I think there's a move now towards the localization of data that makes it more difficult to share information, and makes it easier for a repressive regime to abuse its own infrastructure in a way that's inconsistent with internationally held norms and principles.

In order to prevent that from being the world, we can't take for granted it's going to head in the other direction as technology improves. It's going to take a concerted effort to really articulate what our commonly held values are, and then the hard process of figuring out how to implement them in a way

that if people don't feel safe and trust their government, you lose, I think -- it's not always right, they may be relatively safe but fear, if people are driven by fear, then that does not attend towards regimes that are protective of human rights and civil liberties.

We are simultaneously in a world where you can project abuses in a way you never could before and get people together, and where groups can exploit that. That is why I called it "crowdsourcing terrorism" that's used for good.

I met with -- it was one of the most painful experiences in a career where I started prosecuting in homicides and rapes, but one of the most painful experiences being meeting with some of the families whose loved ones were taken hostage by the Islamic State, talking to them and recognizing certain failures we have had in communicating with them and helping them, but listening to a description of what it is like to see your son slowly beheaded, and knowing that the world is watching it.

Both opportunities are there with a powerful new set of technologies, and we need to figure out how to make sure that it attends more to the good than the bad.

MR. VAN DEN HOVEN: You talked about the weaponization, a very striking example of how digital technology can be used, the panic button, as we wanted to perform but without all the drawbacks.

My question to all of you is how do we bring this about? Who is our audience? Who are we addressing with this question, if we are all on the same page and we say let's shape digital technology in such a way that it does demonstrably so what we want it to do without the drawbacks, without the violations of human rights, without all of the risks and threats that we introduce in addition.

MS. KOENIG: I think as you so rightly pointed out, the way that we are using technology today is bringing forward voices and stories that we needed to hear.

What I'm concerned about is that in addition to getting access to these stories in really critical ways, there's an inequality piece that we also have to grapple with internationally.

I think thinking through the proliferation of Smartphones is an example of how that shift to the voices we are hearing is a really important one, both from a gender perspective and also a class perspective.

I think there is kind of a classic example where one tech company created an app for recording sexual violence and conflict violence, but it was targeted and rolled out in a part of the world

where really only the men had access, and if the woman was to actually get hold of her husband, brother, or father's Smartphone and download this app and actually use it, she was potentially revealing that she had in some way been violated, and that could have really bad consequences.

I think thinking through the ways technologies can have no impact, even when beautifully designed, or can have very negative impacts, is something we have yet fully delved into and explored.

Using the great example of eyeWitness to Atrocities, which I think has been so brilliantly designed and really thought through the chain of custody piece of it, so we can think through how the survivors, the activists, who are risking their lives every day to get information, whether it is domestic or internationally out of war zones, so that whatever they're gathering has as much potential evidentiary weight as possible has been a huge part of the education process over the last five years.

I think what we need to think through next are the distribution components of that, how do we get this into the hands of the people who can use it most, what does that look like. A lot of times, that is adapting existing technologies and really understanding what technologies are already used on the ground, to make them more secure and user friendly.

The other piece is on the opposite end. I know one of the challenges is once you have gathered all this information and incredibly rich data, who do you allow to have access to it?

I think that's a sticking point where we are at in terms of the human rights field right now, do we need to create some kind of blind trust or an escrow system whereby the activists who are sharing the information have some degree of control, and some degree of ability to decide who can have access to that information, and protect their identities, because so often they are putting their lives at risk to share it in the first place.

What are the policy considerations about who we give this information to, and what do we expect in terms of how they will use it and the transparency around that. Those are conversations, I think, we are just beginning to have, and really need to delve into more deeply.

MR. VAN DEN HOVEN: What do all of you think are the responsibilities -- we haven't touched upon it yet -- of the IT industry? We are using all these gadgets that are produced, not for these kinds of human rights or the common good, but preferably for revenues, which is okay, of course, but it is something that we have to bear in mind, and adding all these little gadgets and services and products

doesn't necessarily lead to kind of the decent society that we want, what do you see as the responsibility of the IT industry in this?

MS. SAADA SAAR: If I can begin, I mean I am at Google. How I have seen it in my role is really playing off what you have said, the importance of bringing human rights defenders into the room with engineers, so that these products are developed in a way that it doesn't just sound nice, it's not just a nice gadget and tricks, but the context in which the activists need to use the app is fully understood, and all the implications and challenges are fully unearthed between the activists and the engineers.

I think that is a very powerful area that we need to be able to grow more, and it is something our companies are at a powerful place to do.

I think the other piece for me is also in light of what you have discussed, emerging markets, right? We have to be digitally connected, right? Folks who are in areas of the isolative rural parts of the Sudan, where there are human rights violations every day, have to be digitally connected in order to be able to hold accountable their abusers. That is not a reality right now.

There is a reason why we see more evidence of human rights abuses in Syria than what's happening in parts of Sudan and Somalia, right?

For me, there's a commitment in speaking to emerging markets, not simply for revenue and capital, but in order to be able to recognize that there's a human rights reason to do emerging markets, and as we do emerging markets and stay committed to that, we have engendered consideration of how it's done as well.

I think the other piece for me has been -- this is also around transparency, this is the new concentration of wealth and power, right? That's what we are. The importance of being able to make sure that human rights defenders, women's rights defenders, understand that, and understand the landscape of it, and have access to it.

So, that has been very critical for me in this role, to make sure that the women's rights organizations have contact and connection and dialogue with Google, and that the same is done in other areas of human rights defenders, that there is a way in which the same opportunities that we hold accountable civil society, the private sector, government, that kind of approach also has to happen in the context of tech.

MR. VAN DEN HOVEN: Shifting companies to Facebook, you talked about this micro targeting and self-radicalization, that is basically a result or in part a result of the fact that that environment is designed or constructed in such a way that you have these feedback loops, and people kind of get locked up in filter bubbles and echo chambers, so their self-radicalization or the dynamic properties of that behavior are a result or a function of the structure of that environment.

No amount of bringing people together and having them sit around the table and dialogue about these things will change those very basic architectural principles that then will give rise to the problems that you will have to deal with. Is that correct?

MS. SAADA SAAR: At Google, for instance, we have this whole counter speech effort going on, so when you see radical YouTube videos come up, also what comes up are other videos that point in the direction of the work around tolerance and inclusiveness that is happening in Muslim countries, in areas where there is extremism, and that came out of conversation and dialogue with human rights defenders.

MR. VAN DEN HOVEN: So, you would say there is a shift from this is all the market but now they seem to realize what incredible influence these kind of top five IT industries have on the shaping of our society or our future society, and they will take responsibility in proportion to their contribution? Do you see that kind of --

MS. SAADA SAAR: I'm hopeful. I certainly see it playing out at Google. I think both Facebook and Google around the fake news are recognizing the ways that we had to address this.

MR. VAN DEN HOVEN: Editorial responsibilities.

MS. SAADA SAAR: Exactly right, and how do we use an algorithmic response but also how do we think through what our responsibility is here because none of this is neutral.

MR. VAN DEN HOVEN: Right. Absolutely right, yes, we are not talking about shoelaces, we are talking about the fundamental structure of a digital society.

Is there the same level of optimism with the other members of the panel?

MS. KOENIG: I think one of my biggest growing concerns is exactly as you mentioned, this growing concentration of power in the way that we are using these different digital technologies. If we look at there really being three super companies that are emerging as having a tremendous amount of

control over our ability to engage in artificial intelligence and machine learning, to think through how we share information and what those information flows look like.

That was power that was traditionally held in the hands mostly of government actors, and we created an entire society that's built on thinking through what transparency tools we need for government, but we really haven't thought through this shift in the way power is happening globally, and what kind of transparencies, and getting to your carrots and sticks piece of this, what kinds of incentives need to be baked into this emerging global environment so that we do have a lot more transparency than we would have otherwise, how is that good for business and for corporate actors, and how is that then good for society as a whole.

MR. VAN DEN HOVEN: John, would you like to respond to that?

MR. CARLIN: You've touched on some of the most challenging issues. I think it is definitely true that we were seeing the fragmenting of certain groups online whereas instead of a way to be exposed to new ideas and new people -- I never liked the term "self-radicalizing," because when we looked at it in most instances, it wasn't self-radicalizing.

Instead, you would end up in this echo chamber of hate, and that was true for the motivation of domestic terrorists, which is usually defined by those inspired by hatred of a particular ethnic group here or homegrown reasons, and it was true of international terrorists, those who were being deliberately targeted as part of a strategy by a terrorist group.

You would have often very young and influenceable and sometimes those with other mental challenges that would end up in this echo chamber of hate where everything they saw would affirm -- which is why I think people call it "self-radicalizing" the view they started to have.

How you get into that sphere or echo chamber in a way that's consistent with the idea that you should have the right to choose who you are able to communicate with, and secondly, and a very difficult issue is fake news.

That's not so new. One case that I didn't talk about, a Syrian electronic Army case. This is a case where one version of fake news is they spoofed a terrorist attack on the White House, and because they caused fear and panic through that terrorist attack, the stock market lost billions and billions of dollars. Fake news, before we were all using this term "fake news."

The terrorists' use of just utterly false propaganda about what life was like in the Levant, along with made up abuses carefully tailored, about what those who opposed Islamic State were doing. We didn't use the phrase "fake news" for that either, but that was an incredibly effective recruiting tool. Now, you have this nation state interference with an election where we started to use the term "fake news."

It is very challenging, who is the arbiter of what's real and what's fake. The regimes have long said, for instance, human rights activists' films in areas of abuse, and it just didn't happen, you are hearing it right now with the chemical weapons, it's fake.

Is there a way to both call it for what it is, that we are seeing some regimes exploit and deliberately push fake news and take advantage of technical algorithms to push them, without having a drive to the bottom where people throw up their hands and say I don't know what's real, so I'm not -- I'm just going to believe essentially what confirms my already strongly held belief.

MR. VAN DEN HOVEN: All those things you said apply equally to outside of the domain of terrorism and radicalization, but also kind of more broadly to society and citizens at large, for all the victims in any kind of presidential elections or in the Brexit, we know the people working on AI and big data have played a very important role in all of that. That seems to be a really important issue.

I think we need to open up to the audience. There are a number of microphones available. I saw someone in the back.

MS. MacKINNON: Hi, there. My name is Rebecca MacKinnon. I direct a project at New America called Ranking Digital Rights. I'm also on the Board of the Committee to Protect Journalists, and co-founder of a citizen media network called Global Voices.

I want to raise an issue that hasn't been brought up directly yet, which has to do with an increasing tendency in Europe in particular, but I think also a desire by other legislatures elsewhere, to hold Internet companies liable both for extremist speech, efforts of recruitment, and so on.

There is proposed legislation in Germany right now that would require Internet companies to basically pre-censor anything that's deemed illegal, thereby, basically holding the company responsible for making the legal judgment rather than a court or a government official, which raises a lot of accountability and transparency questions.

There has also been a tendency in many places, this country as well as in Europe, to call for a weakening of encryption, to call for requirements for backdoors, for law enforcement and other government officials, which has caused great concern among human rights communities and investigative journalists and others about the potential real negative consequences for human rights over the long term globally, if democracies lead the way in weakening encryption.

I would love if the panelists could comment. Thank you.

MR. VAN DEN HOVEN: Thank you very much. Who would like to respond to that?

MS. SAADA SAAR: I can begin. You are right to raise all those issues, especially the latter, which is a real challenge and affront to human rights protections to weaken encryption, and I know we are very unsettled by what's playing out.

I think also within the U.S., we have Section 230 of the Communications Decency Act, which allows for intermediary liability protections, and it is really the backbone of the Internet.

I have very real concerns around what happens when you begin to hold tech companies accountable for third party content. At the same time, I feel that we are, within Google, and I think Google is not alone in this, really struggling with this tension and dance between freedom of expression rights and the normalization of hatred.

There are no clear answers around how to pivot, but it is a tension that we have to deal with every single day, to be able to not be engaged in censorship, and at the same time, not allow for a digital landscape in which extremism and hatred are normalized.

Just to add, I just want to make sure that we recognize this is not just about terrorists and international extremists, it's also about within this country as well, and white supremacy organizations and the same type of tension that we are in the middle of with white supremacy organizations, too. It is not simply about terrorists and foreign nationals.

MR. VAN DEN HOVEN: There is a question here in the front.

MR. SHEFET: Hi, Dan Shefet. Before asking my question, I'd just like to comment on what you said. I happen to be working with the German Ministry of Justice on the fake news bill you referred to. There is no such obligation in that bill of pre-screening or monitoring. It all works on notice take down, pre-screening and monitoring would be a violation of the Cybond Net law case, European Court of Justice. So, there is no such thing, and please, for everybody to know it's not the case.

The question I would like to ask you is in terms of accountability of the private sector, and it's been mentioned already that maybe encryption is a problem or not, you mentioned the evidence problems, you mentioned the mutual assistance system that doesn't work, how do you see -- there are very specific fact cases like San Bernardino and so on, what was the position on the cooperation with the private sector on breaking encryption when needed for law enforcement purposes?

MR. CARLIN: There are a couple of different thoughts. One is we need to recognize there's a real problem, that not just law enforcement in one particular country, like the United States is facing, but law enforcement in national security agencies in every country around the world.

It's a problem that's driven by exploitation of a new form of instantaneous communication that does much good, so it doesn't mean the technology is bad, it has great potential, but it is an issue that is going to require a legal policy solution.

I worry if we take the approach of either it's not a real problem, it's something that's being made up, or that it's one where the value of free and instantaneous communication trumps all other values that won't actually lead to a world of freer communication and less regulation, but it will continue the speed with which we are moving towards a trend where data localization is required by law, if you're going to provide your service in a country, because at the end of the day, whether it is my German counterpart, French, United Kingdom, Belgium, as each faces this same issue, not only are they incredibly frustrated, they are primarily to date -- this will change -- U.S. companies are having the debate.

In Germany, it is a U.S. company causing the problems for local law enforcement, there is even less tolerance for the answer of we have no solution.

To define the problem crisply in San Bernardino, for years we have worked a constitutional system out where if you're able to meet a certain predicate under the law, so probable cause, you go to a neutral detached magistrate, a judge, to swear out a search warrant, then when you go to effectuate the search warrant, you have the technical means to do it because it's something like -- it's a very invasive technique, which is why it is subject to so many privacy protections that are enshrined in our Constitution, the idea that you can do it, but that it also requires these protections.

That is a problem as old as the Fourth Amendment. It includes searching through someone's privacy and possessions. As we have the new technology, and not, I think by original design, you have the prospect where your phone is outside the boundaries of law enforcement, process for local

enforcement, or your communications, unlike how they are with the telephone, are outside the bounds of law enforcement, no matter how great the need and how high the predicate.

That is the issue I think people are struggling with, and I don't think it has an easy answer. That said, if we recognize that as the problem we're trying to solve, I tend to think you can innovate your way both technically towards it, so the way you maximize the security of the information, continue to make the private sector party the protector of that information, and only allow it through targeted approved law enforcement means.

If we agree that was the world we wanted to live in, then we could design our way towards it. I think that is what you heard President Obama articulate at South by Southwest.

There is another world that says in both directions, either we think we should always have more access to the information in that world, or we think there should be a completely outside of state reach, no matter how great the need or what, the law enforcement processes, it should just never be reachable.

I think even if you have that view, that will actually result in something less like that world than you desire as states react.

MR. VAN DEN HOVEN: Some more questions over there.

QUESTIONER: Hello. My name is Camilla. My question is going back to the idea that now with technology, we are able to see human rights abuses that were previously just known within the communities.

However, what we see now is that still a lot of the narrative is shaped by media, so it is like the man who came to New York City, the tourist that came to New York City to stab any black man that he saw because he was upset about black men having relationships with white women, and yet, we saw the media talk about it as this well-dressed man came and stabbed someone instead of labeling him as a terrorist.

We see some countries get flags on Facebook and others don't. We have all this information accessible to us. However, the narrative, like within the U.S., is very like white centric.

Do you think the narrative is going to change on its own regarding this, or is there anything that could be done to change it from any perspective?

MS. SAADA SAAR: What I find interesting and hopeful is that the narrative is not owned by one space any more, right? So, the narrative is also produced and reproduced on Twitter. The narrative is also owned and shaped by YouTube creators. Our top YouTube creators get more hits and have more subscribers than the main news media stations, right? CNN can't rival what our top YouTube creators get in terms of the number of eyes on them.

That to me is what's fascinating, whereas before, there was one concentration of power and authority that owned the narrative, and often that authority was not representative of the country or globally. That has powerfully shifted, and I think it is only going to be recreated and reframed even more moving forward.

MR. VAN DEN HOVEN: I have two questions over here.

MR. HERSHEY: Loren Hershey. I was in the Anti-Trust Division back in the 1980s. I was involved in the breakup of AT&T. I was invited to come over here as a guest scholar, so I have a request of you -- that was in 1986/1987

-- this is too rich. I prefer to be an optimist, but you're chilling me and charming me at the same time.

Will you come back as a foursome and re-present to us periodically, and that would go all the way through 2020. (Laughter) Thank you very much.

MR. VAN DEN HOVEN: We'll have a discussion about that over lunch. It is a very interesting suggestion.

With this, I'm very sorry, I'm being nudged here. Can we do one more question? One more question. You're lucky.

MR. RIDOUT: Tim Ridout, Non-Resident Fellow at GMF and part-time curmudgeon. I'm concerned that the tech companies are sort of claiming this sort of self-righteous, you know, the defenders, and many of them are doing good work, and I agree with Malika that bringing attention to these previously unheard voices and drawing attention is a very good thing.

For example, there was just this deregulation of privacy rights that the Trump Administration signed, and this is going to be a boom for ISPs, advertisers, tech companies, and they are selling people's information. I have already read something in the Brazilian press that is questioning whether this is going to run afoul of their 2014 Internet governance legislation, which is very protective of Brazilian citizens and their rights.

So, what about when tech companies are infringing upon the rights of citizens? Thanks.

MR. VAN DEN HOVEN: Good question.

MS. SAADA SAAR: From Google's perspective, we were not supportive of that, and do not see that as a boon in any way.

MR. VAN DEN HOVEN: It will also be a serious problem for the privacy shields and the carefully negotiated kind of level playing field in data protection regimes between Europe and the U.S., of course, and that will have a huge impact. So, thank you very much for that.

I think from the discussion, it is clear that we are up against huge challenges. We will have to draw upon different disciplines and different bodies of knowledge, and bring those people effectively together to work on designs that are comprehensive, that our systems designs involve people, software and hardware, institutions and governance, regulations and protocols and all of that, the whole kit and caboodle needs to be designed. That is something that we refer to as "value sensitive design."

So, I thank you very much for your contribution to the panel, the wonderful discussion, the generous sharing of your ideas, and John, of course, for a wonderful, beautiful lecture.

Thank you very much. With that, we're done. Thank you very much. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

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

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020