TECHONOMY 2017

The Internet Under Attack

Speakers:

Mark Anderson, Strategic News Service

Peder Jungck, BAE Systems

Rebecca MacKinnon, Ranking Digital Rights at New America

Moderator:

David Kirkpatrick, Chief Techonomist

(Transcription by RA Fisher Ink)

Kirkpatrick: We did not intend this conference to be a relentless assault on Facebook, Amazon, and Google. If you read the article that I wrote in our magazine, you'll see that I try to be nuanced myself, but it is interesting the degree to which the concerns have risen close to the surface in the last couple days. I did tell the panelists backstage, one of the things I'd like them to talk about, since they've all been here, is what they think about the dialogue we've had over the last couple days at any level or really on any topic since this is the penultimate session. In terms of what we're approximately up here to discuss, even though the title is "The Internet Under Attack," I think of it probably more to be about how we now have an interstitial tissue for global society which we call the internet, which has fundamentally changed the landscape of society, politics, and the economy. What does that mean and where does it go next, given the panoply of challenges and threats that exist—and there are many, as you will hear us discuss.

Maybe we should start by addressing either one of those two things; it's your prerogative. let's start with Rebecca MacKinnon. Most people have heard Rebecca MacKinnon talk at some of our sessions, she runs the Ranking Digital Rights project at New America, which really aims to assess what technology companies are doing and how well they're doing it, particularly in the area of privacy, but in other areas as well.

Peder Jungck is the Chief Technology Officer of BAE Systems Intelligence and Security. BAE is a giant British aerospace company that has a very big government contracting business in the U.S., which is the part that he works for and is the Chief Technology Officer for. He has a long

background in the advertising industry, which gives him an interesting perspective, as you'll hear.

Mark Anderson is the CEO of Strategic News Service, a longtime journalist, consultant, pundit on technology, and the operator and host of probably the only other conference I know of where the things we've talked about so freely here would routinely come up, called Future in Review, that's been happening for 13 years now. So he and I are somewhat blood brothers in this business. Now, Rebecca.

MacKinnon: Thank you, David.

Kirkpatrick: Also, she used to be CNN's Beijing Bureau Chief—

MacKinnon: Yes, long ago.

Kirkpatrick: —And has done a bunch of other interesting things. She wrote a book called *Consent of the Networked: The Worldwide Struggle for Internet Freedom*,.

MacKinnon: Thank you, David. As it happens in *Consent of the Networked*, which was published more than five years ago now, I had several warnings in that book, and one of them I illustrated with a slide that I often gave in talks that I think would be useful to reprise here. The slide has a circle with democratic countries here, and authoritarian countries here and the assumption, the narrative not just in Silicon Valley but in policy circles, in media for a very long time—which I contributed to back in the '90s when the internet showed up in China, and it was like "there's no way the Chinese Communist Party can survive this." Boy, were we wrong—but there's been this assumption that you've got democracy here and you've got authoritarian societies here, and that because the internet and because capitalism, the authoritarian societies are inevitably and inexorably going to end up over here in the democratic side.

What I've been worrying about for some time is that if we're not careful, actually, we're going to meet in the middle. That you're going to have authoritarianism adapt to the internet, not only survive and thrive, but adapt the internet to its purposes, and we see China as exhibit A for how that works. Meanwhile, democracy kind of moves towards, you know—driven by populist leaders, all kinds of different forces, surveillance capitalism, etcetera—ends up becoming less democratic and is in this kind of manipulated, maybe you call it authoritarianism, maybe you call it populist quasi-democratic, whatever you call it. But basically, the differences between authoritarian society and democratic society are going to break down unless we very consciously and actively work to prevent that from happening, and I think events of the past year have shown where that's going.

There's a couple other trends that are going on that we need to think about, and you suggested that we think beyond just bashing the tech companies, and I think we need to be careful about some of the regulatory reactions and responses. And I think there have been some very important proposals put forward at this conference and elsewhere about the need for more

transparency around algorithms, around data collection, around advertising and so on, but there's also been a lot of regulatory proposals by well-meaning politicians in democratic societies placing greater liability on internet platforms, calling for censorship, essentially. Censorship systems that are going to be very welcome around the world by many non-democratic nations as making it easier for them then to impose laws on Facebook and Twitter and Google's properties to crack down on society.

Kirkpatrick: Yeah.

MacKinnon: And this is part of the problem. "Internet Under Attack" is really civil society under attack because civil society in the past decade has been very successful in using the internet in challenging authority, and now authority is fighting back. They've figured out how to use the technology to fight back, and at the same time you've got a clash of kind of nation states clashing with global sovereignties of internet companies and nation states figuring out how to use these globally internet platforms to carry out information wars against one another. And we don't we have either legal and regulatory systems, or political systems, or ways of holding power accountable that's actually going to serve the further human rights, democratic and open societies, and we need to figure this out, fast, or we're going to meet in that middle and get stuck there.

Kirkpatrick: One quick point to underscore—this idea that the societies are fighting back—it's been reported but it's not as widely discussed as perhaps it should be, that Facebook was about to launch in China in partnership with Baidu in the spring of 2011. There was a lot of movement; they were very far along that path. The Chinese leadership saw what happened in the Arab Spring that winter, and they put the kibosh on it. And that's exactly the kind of movement you're describing. They were very wise; they knew what was coming; they understood—they acted in their own interest.

MacKinnon: And they don't need Facebook, because they've got Chinese alternatives.

Kirkpatrick: Well, that's something else.

Jungck: The one thing I would react to is, I would say that I don't know how governments will all merge and how the population will get to the middle, but the internet is definitely in the middle of both of these worlds: the authoritarian governments and the West. What I would say, though, is we need to be aware—and I think you can see that for $200 dollars' worth of rubles you can influence something—that the open ecosystem of social media we have created, and the copies like VK and Alibaba and all the rest that exist around the globe, were built to produce brands, whether to defend them or to be able to go and socialize those things. And governments care about producing brands and feelings within people and we've made it so it's the lowest cost to be able to go sell something, which might be a vision, a message, a riot, whatever it may be, from that piece. What we need to step back, is to take a look at not even

just "here's the technology," because we can regulate Facebook, but are you going to regulate every one of the other thousand social media companies that aren't even based in the West.

You're just going to see the influence of something going around. But realize, what you have is, while in China they might want to go and control what the social media company does, in many ways they'd like to figure out much more what their dissidents are doing outside of that country and what we've done is serve them up on a platter as an ad. Let me find everybody who's got this type of interest, where they go and do. And I think this is where we need to get to, as this conference has talked about, the openness of the data and who is producing what types of questions, who is producing what types of things within these systems, so that people can truly have transparency. Because the thing that we at least have on our side is the willingness to be transparent. And I think that is really where you get it, so that then everybody can get into the dialogue, and the notion that we can just—you know "we're going to control it, we're going to do it"—realize we are serving up these tools for a global stage to be able to interoperate with. And I think that's where we need to step back and understand, what are those ideals and what are those goals of everybody around the globe with all these types of technologies and these data repositories? And then, are they sticking bad data into it to make it have bad decisions, or are they going in and asking it questions about people that maybe isn't the right type of thing that we care about.

Kirkpatrick: I think these are the kinds of insights that your ad background allows you to see, maybe sooner than some of us. But you made some interesting comments to me as we were preparing about the fact that these are advertising systems and that the quality of information that they are capable of producing and their sophistication vis-a-vis what governments themselves have from a regulatory and from a fighting-back point of view. Do you want to just go there a little?

Jungck: I helped IPO the first permission email marketing company in '99. And we could see when you open the email, when you clicked on it, when you went to the shopping cart and you decided that the shipping fee was too high, and that Tuesday at 9:10 a.m. was the best time to go say "free shipping." And you'd go and you'd get it, and we could predict the response rate, and you could see that. That was almost 20 years ago. The amount of money that's been put into the ability to understand the mindset of a person and how they will respond is bigger than many of these other governments around the world could ever invest into their tools and technologies, and it is the western commercial tool set that we're providing to all of our consumers that is the apparatus of all of our adversaries.

And I think we forget this often. These social media tools that ISIS uses, that all the rest of these things go and communicate, it is not a separate set. And these tools are amazingly effective. That is how you have brands that have survived for decades, because we're able to go and see when somebody else is trying to sell a product counter to our brand; we're able to protect that brand, we're able to go get people inspired about it, we're able to see when they're

leaving the brand and going to something else and coming back. We talk about that as selling a product, but you've got to remember: an idea is a product. And I think that is where we often forget that somebody else may be trying to sell something different.

Kirkpatrick: Just to take what you just said and something you said to me before—you're sort of saying that advertising systems are the best intelligence systems, and they have been weaponized.

Jungck: Darn right. And it's too late, Pandora's box is already open. You can't go back.

Kirkpatrick: Wow. That was very interesting. Mark.

Anderson: I'd like to take this back a little further and maybe a little bit broader.

If we got back to the invention of the net, we had ARPANET, Science-Net, these basically very benign science groups talking to each other about how to conduct pure science. And if you did that whole run over time and you did a chart of some kind saying, "Good Guys versus Bad Guys" on the system, there were zero bad guys on day one, basically. It's many years now later, and I think we have many, many more bad guys on the system. It makes sense, it's true for any kind of human system you build, as time goes by the bad guys figure out how to break into the bank, whatever it's going to be. No matter what you look at today, whether it's bank robberies—a lot of bank robberies happening every day, in the cyber world—if you look at the dark net and all the things being sold on the dark net and how many people are down there doing business; no one even knows. So, I would make the argument, which I have no way of defending whatsoever, that this has been a pretty much straight-line story, and that we have increased the amount of negative behavior on the net every day and it's not going to stop. And it's a dark view of the net, it's not just a dark net.

I have some perspective on this, as I think you know, because we've been looking at the economic side of cybertheft. We might be the best in the world at the meta scale of this. We watch nations vying with each other, and we've briefed all the three-letter agencies in the world about this, so we're pretty good at this. And we understand, for instance, what China wants to do with the internet, and what they have done for 30 years. They've been stealing intellectual property from corporations, BAE Systems is fully briefed on this, I'm sure. So, if you care about trade and money and power, and you look at the internet from that perspective, and you're Xi Jinping your job is to take IP from other nations and commercialize it, sell it half-price and wipe out BAE—that's your job. And they're doing a great job at this, if you're Eriksson, if you're Cisco, if you're Nortel Networks, Motorola, Alcatel; make a list of companies that are dead or dying because of this project. So when I look at that kind of use of the net, and if we look at it from a global economic perspective, the answer is, that's a very effective model that China has, and it's been an extremely negative influence on both global trade and innovation.

So I'm deeply concerned that there's kind of an easy talk way to talk about the internet, and very few solutions—which we talked about this morning at the breakfast meeting—true solutions. We saw NSA create botnets and they published the papers about it.

Kirkpatrick: Who did that?

Anderson: Our guys, the NSA guys. They knew how to make botnets a long time ago. We are participating as well, so everyone does this. But that's not good, necessarily. Will we get to the point where no one in this audience trusts the net for anything? I think we might be there now, in a way. I mean, who feels safe about their ID? No one. And they shouldn't, because everyone in here has probably been pawned. At what stage does the boiling frog get angry? This is really a bad situation and I don't see it getting better. So, I'm deeply worried that there's this ongoing slow growth of negative behavior, and a bunch of us good guys are tolerating it for some reason, but it's not getting better. And I worry about it on an international scale and I worry about it on a personal scale.

Kirkpatrick: You've been an advocate for—and seen the emergence of—treaties on things like intellectual property,

and China, and they have signed.

And I understand you to think that they have moderated their behavior to some degree, as a result of their international agreements.

Anderson: Yes.

Kirkpatrick: Isn't that the case?

Anderson: Yes. I do believe—

Kirkpatrick: So that's a good thing. That's progress, that's something that we could have done that we did, right?

Anderson: Yes.

Kirkpatrick: Okay. Is that possible to take further?

Anderson: I don't think so. In other words, yesterday morning there was a report published that China's back at it again, and that we've just been missing some of this stuff—

Kirkpatrick: Back at what exactly?

Anderson: They're re-tasking their teams to do APT attacks against commercial enterprises in America, despite the treaty. We think that there are a lot of countries that don't have those treaties that are getting hit by China now.

Kirkpatrick: Okay.

Anderson: And that China's in a wave of using stolen IP and doesn't need to steal it by cyber means, since they've got 80 percent of the theft happens through human intelligence.

Kirkpatrick: Let me ask you one thing that's related, that I don't think people in this audience have given enough thought to, and I don't know if either of the other panelists have thoughts on this, but I think it should be on the table. If China was smart enough to prevent Facebook from coming into China in 2011, they probably figured it out in many ways a lot earlier, and Facebook and Google and a lot of other companies—we could list a list this long that are operating globally in some fashion—that basically have had relatively permeable employment situations, so how likely do you think it is that moles are inside our great tech companies now?

Anderson: 100 percent.

Kirkpatrick: 100 percent?

Anderson: Yeah. I'd go further and say, we could talk for length about the Human INT program from China; it's a gigantic program. But it's equally interesting, since you've brought up Facebook twice; Facebook was not the only company in e-commerce prevented from joining the Chinese market—all of them were. And there was a distinct decision at the top that they would copy our business models of our companies—being the West, us—and then reproduce them inside China and not allow us to come into the Chinese market even though they could come into our market. They can buy our companies, but we can't buy their companies. And the fact of this unevenness to me is striking. I just don't understand why, whether you're from Britain or America or Germany, when this happens—Germany is kind of waking up now—you'd go, "wait a minute, this isn't a fair trade. If you can buy my companies, I should be able to buy yours." If you're going to let Alibaba into America, then we should allow Amazon more traction in China. But that's not the case.

MacKinnon: And, of course, these Chinese companies are as successful as they are thanks to American capital.

Jungck: Yeah. Take a look at Xiaomi from a phone system company, it's like, my wife just bought an iPhone X and it finally now has a camera that catches up to what we were able to get in Singapore a year ago but you can't even buy in the United States.

Kirkpatrick: Really?

Jungck: Now, if you'll get every one of the founders who was at Motorola, Google, all the rest of these things—

Kirkpatrick: Apple, yeah.

Jungck: You'd probably realize why they can't be here, because it's probably got a lot of our IP in that. But, yet, that's the types of things that you're seeing. I think, while this may be "The Internet Under Attack," I think the one thing that has been freeing, and at least we saw this within cyber, was when you finally got to the point of saying, "You know what, I cannot trust the systems." Like when I knew that somebody was going to swipe my credit card and I'm going, "Fine, how do I go make it so it doesn't matter anymore?"

There's a freeing level of when you start with this foundation of saying "Don't trust it." Presume that they're here. Presume that you have that, then all the sudden you can go and start to say that "well, if there is no trust in any of this, how could I build that?" And if you look at people trying to go and say, "Don't try and defend my social security number, that's not a valid number, give me a blockchain equivalent." Give me something different. Let me start to build something and say, "Please don't defend upon my privacy based upon my social security number because it's probably out there." I can tell you with the OPM attack, there's lots of people who have it now. But from the rest of those things if you start there, now all the sudden we can build upon that, and that's where we need to get this transparency out there. Saying, "It's happening." Let's quit debating whether it's occurring or not, whether somebody's trying to do this; let's rapidly get the world to have the view—

Anderson: You see private networks being built now. There are whole networks that are dark fiber that are completely aside from the internet. And that's the real answer that the big kids had in science and the military for dealing with this problem.

Kirkpatrick: Okay, quick question. This is sort of a side question, but the Equifax attack—we all were distressed that it occurred, I think we can accept that. Were any of the three of you concerned about your personal data after that attack.

MacKinnon: Sure.

Kirkpatrick: You were. Because my question is, based on some of the things you've said, wouldn't you pretty much assume that all of it was more or less available already in some form to somebody if they really had ill intent?

MacKinnon: Yes, to both questions. I mean, that doesn't mean you're not concerned—

Kirkpatrick: It just means more people have, more people had it—

MacKinnon: So it's like, okay, there's yet another layer of—

Anderson: Well, and who had it?

MacKinnon: Yeah, sure.

Anderson: Because none of that stuff showed up.

Kirkpatrick: Many people think that that was a governmental attack.

Anderson: Right.

Kirkpatrick: Yes, we know that. I don't want to go too far down that, because there's too many other good questions. Rebecca, I wanted to ask you to talk about what you're doing now, The Ranking [Digital Rights] Project, because you've come to some interesting conclusions. Not any of them particularly reassuring, but there are some nuances that are worth mentioning in terms of how you see these various companies in the firmament.

MacKinnon: Right. What we do is evaluate 22 of the world's biggest, most powerful internet, telecommunications, and mobile companies. We have a global cross section on 35 different questions that are looking at these companies' policies and commitments and disclosures that affect users' freedom of expression and privacy, including security as well as an aspect of privacy.

And two companies get Ds, everybody else fails, basically; the transparency is bad. One of the points of this project is not that transparency is everything, it's not sufficient, but it's the necessary first step. We need greater clarity about what companies are doing with your data, with whom they're sharing it. We want people to be able to see what the differences are in the companies' policies and push companies to disclose this, push whether they're doing due diligence, push whether they're doing impact assessments, security assessments, what their governance mechanisms are for assessing risk both around privacy and security, but also around expression and content. And I would argue that companies' lack of transparency around how content is policed, how a person's information environment is manipulated and shaped. The total lack of transparency around this has contributed to the problems we have today and has contributed to the mess that these companies have found themselves in because they haven't been clear with other stakeholders, they haven't been clear with regulators, they haven't been clear with the public; and so now there's this big backlash. And that if we get more transparency we will be able to at least work through some solutions.

But what this is really about is the exercise of power. Because you cannot have accountable governance, you cannot have an open society, unless you know who is exercising power against who to what end, and if they're abusing power, if they're exercising power without consent of the governed—

Anderson: You mean facts?

MacKinnon: Right, well, yeah, there's that.

Anderson: Yeah, that fact thing.

MacKinnon: That fact thing. If nobody has any idea who's exercising power upon whom, against whom, to what end, you can't hold anybody accountable. And then you can't have

accountable governance, whether it's private or public governance or anything. So that's where I'm looking at the corporate transparency piece, but governments are not transparent about the demands they're making on companies, both to censor content or to hand over user data, and there's a big movement to get governments to be more transparent. Not to warn the adversary about what they're doing, but at least to have basic level of transparency that there's accountability that can prevent abuse. And we're very, very far away from that as well. And there are a lot of government policies and laws around the world, including the democratic world, that are preventing companies from being transparent as well.

Anderson: I worry deeply about this.

MacKinnon: Not that that is the total solution, but it's one step towards figuring out where we go.

Anderson: I love transparency and I agree with you, but I worry deeply that that's not really the solution, it's just a good thing. And that if you're Russia or anybody and you want to control an election, you don't have to pay for ads, you don't have to be identified as the guy who paid for that, you just go in with 100,000 botnet members and start reinforcing your beliefs about whatever. And that creates the division in this country that leads to the next election. And no one will ever be able to break that down. I don't think they're ever going to figure out how to fight that. We'll have our botnets fighting their botnets.

Kirkpatrick: Allow me to say one thing on Facebook's behalf and in their defense: You can't really have a botnet inside Facebook. If they were to enforce their identity rules, there would be no bots. The problem is that—I think they themselves said the other day that 10 percent of their identities are fake, which means technically they could be botnets—it's enforceable. I would strongly predict that this will be one of Facebook's biggest responsive efforts in coming months and years, to drastically reduce that number of fake accounts that are in there, which can be done by various means.

Anderson: So since we don't trust their numbers, David, what if it's not 10 percent? What if it's 40 percent?

Kirkpatrick: 20 percent?

Anderson: What if it's between 20 percent and 40 percent?

Kirkpatrick: Okay. Well, then that would be—

MacKinnon: The way they're enforcing identity rules, however, is so ham-handed. So—

Kirkpatrick: Well, they have to get better at that.—

MacKinnon: A bunch of women named Isis had their accounts deactivated a couple years ago.

Human rights activists around the world, whether or not they're using their real name, are the most vulnerable to having their account deactivated because Facebook says we're going to deactivate you unless you provide your passport or something, and they don't, because of the way the flagging mechanism works. We have some real problems here in terms of

how you're going to balance rights and security.

Anderson: —Look at the Equifax hack you just brought up. How hard would it be for some nation to take that information—you just said it was a nation that stole it, probably—and turn that into 145 million accounts?

Kirkpatrick: I think it could be made hard, it's just a matter of new systems that don't yet exist. The issue that you raise about human rights activists in countries that are repressive not feeling safe on Facebook because they have to use their real names, that is legitimate and is a very tough one to solve. I think they have more clever and subtle ways of dealing with that now than we might necessarily know because Facebook does want to be a positive force, but anyway. Your theme is very consistent, though, that the efforts that we may make in a democratic country, supposed like ours, to solve this could really make it worse in other countries.

MacKinnon: We need to be thinking globally about this.

Kirkpatrick: Yeah. And I think—

MacKinnon: We need to be really assessing what is the global impact of an action you take in one country—

Kirkpatrick: Which is another way of saying that, for all the negatives about these companies, you still see having a very positive impact globally in many respects.

MacKinnon: Sure, they can. Yeah. Absolutely. And there are still a lot of places around the world where independent investigative journalists can't reach audiences any other way than through Facebook and Twitter, and are really dependent on them. And I would argue that if we, in our desire to figure out solutions to this existential crisis we're facing, make it so that civil society in the most embattled places cannot use these networks, then civil society—the weaker that civil society is in transitional places, the worse our security is going to be, actually. Even from just a security perspective, you want to have an approach that strengths civil society, that strengthens independent voices in Russia, that they have a space to exist.

Kirkpatrick: Right.

Anderson: But we had this conversation this morning about *The New York Times*, yesterday, and the fact that Facebook, until very recently, doesn't pay them anything and takes all of their hard work and makes all of the ad money off of that. And we're seeing the destruction of what

I would call fact-based society because of that kind of behavior by the social networks. So in these countries—not the ones you're talking about, which need to have that access—but the ones where free speech is a really big deal, and democracy is a really big deal, we're degrading our ability to have a democracy.

Kirkpatrick: But this is why the headline of the piece in the magazine that I wrote has the word dilemma in it, this is not easy.

Jungck: One interesting place is, a lot of these go into the negative use. In Syria, it was very hard to figure out what was going on with the refugees. Instagram was actually the best social media network because people do not have Androids and iPhones and high-dollar phones. They had ones that could take a picture, also ones that you didn't have to type a lot for. And they were able to rapidly start posting: Here are pictures of what's happening. We were able to go and really able to see what was going on over there. What was happening in that refugee crisis in real-time, as it was coming out, from those pieces, from these networks doing it. And it gave a voice to a population that had no voice, they were in a land that wasn't even their own and many of them were able to go do this. And so there's many valuable benefits to these things. What we need to understand, though, is that these systems are all being used in so many different types of way, and that is not what they were conceived to be.

We're arguing over whether there was 10 percent or 40 percent of the people within Facebook are fake accounts. But yet, we sat here for a day and a half and talked about people saying, "it's augmented humans." So fine, let's go find 20 people willing to give up their real identity, go have a computer or a bot or whatever be able to augment one person to act like fifty online, these things already exist out there, they're armies and they can have a huge voice.

Kirkpatrick: Just to throw in another thing, John Kelly on this stage this morning said, "the future security battle is going to be AI versus AI." And if you listen to Facebook and Google talk about how they think these problems will be solved, it's "AI this and AI that." But it's going to continue inside—it's challenging. I want to get some audience voices in here because I know there's some interesting people here, as there have been for these two days. Okay, please, identify yourself.

Janice Nickel: I am Janice Nickel. This is kind of a dreamer comment/question; we talked about blockchain and that brings trust and verification into transactions. Is there any way that there could be an analogous way of verifying and bringing trust into software?

Jungck: There's a bunch of things that are digital identity. If you think of, for example, AI is software, it has algorithms, and one can go in and say, "Hey, I've made my algorithm visible," and if you just take the simple notion that was talked about here, where "This is how it prioritizes decisions," whether it's for, as Roku was talking about it, it's going to be the lowest cost for those. Or whether it's for the most relevant type news, we can put integrity around it. And I think that's really where when you're getting blockchain or the rest saying, "That was the

algorithm we promoted for somebody to look at and review." The system can say whether or not that's still the one that's there, and did it work, and you can get these voting-type systems that are in there.

Presume today that you have no trust, how would you overlay a trust-based system, blockchain is one technology that could be used for that. If you start getting there now all of a sudden, we can start to have a debate.

Kirkpatrick: This is a subject that I've heard a lot of people talk about over the last couple years, Union Square Ventures notably has talked about blockchain-based alternatives to these social networks for a time and they're investing in it. And I have heard recently that some of the biggest players are putting some serious money behind systems of this type, so we may see some interesting developments.

Dan Elron: Maybe the traditional internet is dead, as we discussed the past couple days, but I wanted to connect two sessions—this one and the previous one. We're just beginning, kind of, with IoT. Should we trust the IoT to the current internet, should we wait, what kind of solutions do you panel members have, and will you connect your own home devices that can do things, maybe a pacemaker, etcetera, to the current internet?

Kirkpatrick: Dan always asks good questions. And throw 5G into that too, because it really does create a different technical set of capabilities.

Jungck: Be scared. I just published a thing on LinkedIn for cyber security awareness month, and I'm like, "Why should my garage door opener be talking to the house, sitting behind the firewall, talking to my car on all of these networks in which no device in that entire food chain is even able to upgrade the firmware?" And who knows who wrote it, and what—

Kirkpatrick: I just have to say—I just saw a headline yesterday: "Connected Door Locks Take Off."

Anderson: I unplugged all of our Alexa devices in the office, in the house, we don't have any of that stuff, we don't have any locks like that—

Kirkpatrick: You wouldn't have any of that?

Jungck: I'm not living scared—

Anderson: It's a complete nightmare.

MacKinnon: No.

Jungck: If you live scared, you give up.

[LAUGHTER]

Kirkpatrick: I'm going to go look at my living room on Nest right now.

[LAUGHTER]

Anderson: Easy to hack.

MacKinnon: We're collaborating with Consumer Reports, and while Ranking Digital Rights looks not at the Internet of Things companies so much we're working with Consumer Reports to start examining the policies and disclosures of the companies running everything from smart toys to smart TVs to fitness trackers. And their disclosures, and their governance, and security audits, is so much worse than the Ds and Fs that we're seeing in the more conventional internet space—

Kirkpatrick: It's like we have two types of brains going: one is the build it fast, IoT brain, and the other one is like, "Oh, the security thing? Later for that."

MacKinnon: Right.

Kirkpatrick: And we can't do that anymore.

Anderson: Security has to be at the beginning, and it's not.

MacKinnon: As I commented in the breakfast session, it's like putting drugs out there without testing them, or putting cars on the road without ever having crash-tested them, or anything. We're just sticking all this stuff out there, and figure it out later. The human cost is going to be existential, if not catastrophic.

Anderson: It's not secure.

Kirkpatrick: And again, to make another statement in the attempt to be to the internet giants, it's not only their responsibility. I mean, we essentially have a government that's been asleep at the wheel about this.

MacKinnon: Absolutely.

Kirkpatrick: I think they get more blame than Facebook, Google, and the other internet giants. If there wasn't for Senator Warner, there almost would be no one in the Senate who even knows what questions to ask.

Anderson: Let's say something nice about China, since I said something not so nice. Their guys are totally qualified. The people who run China have generally been to MIT, or Harvard, or some other place like that—

Kirkpatrick: Ph.D. engineers—

Anderson: They're engineer Ph.D.s, managed many levels of government, know how to build a bridge; they're brilliant at engineering, and they know all about tech. As you just said, in the entire 535 we have in DC, maybe Mark Warner's the only guy.

MacKinnon: Yeah, well that's the pitch that you hear in Beijing for why their system is better, and why Africa should adopt theirs and not ours, right?

Anderson: Yeah.

Kirkpatrick: It's interesting that you could actually go to down the road—how could we create a political system where technically and psychologically competent government officials could ever emerge in a system like ours? At the moment, it's not something to be too optimistic about.

Anderson: No.

Kirkpatrick: Okay, anyway. Who else?

Alessandro Vigilante: You'd need radical political—

One of the best panels of the conference this year. Great stuff, terrific, guys. I wanted to go back, David, to what you were mentioning about identity verification and so on.

Kirkpatrick: Identify yourself first.

Alessandro Vigilante: Alessandro Vigilante from Fidelity. Coming into the U.S., it was impossible for me to get a mobile phone, a credit card, a bank account, water services at home, internet, a lease agreement—anything. Anything—impossible. Nonetheless, I used to be a freelancer; I used to run my own AdWords campaign on Google, without providing absolutely anything. Luckily, I'm not a hit man, but I could have sold anything—absolutely anything on Google—without any of the regulation that I needed to go through for all of these things. Even with Airbnb, I don't let anyone in my house without a government-issued ID. So why is it such a utopia to think that Google, Facebook, Twitter, and so on, should go to a proper government-certifed ID before onboarding a new user?

Anderson: Google spends $10 million a year on lobbying.

MacKinnon: Again, with ID that might work within certain types of jurisdictions, but if you're a global platform, and you actually want to serve users in countries—if your internet is connected to your passport ID, you're in jail, even though you're doing things that are supposed to be protected under international human rights law, there are some issues there.

Anderson: Well the trend is, each country has its own internet, and this whole thing just changes radically.

MacKinnon: And that's the trend

Kirkpatrick: Just to clarify, your concern is that anything we do in the quasi-democratic countries to try to regulate this will be copied in its most controlling and authoritarian aspects in other countries and used as a justification—

MacKinnon: Either copied or will have impacts. You just need to consider that if you're regulating a global platform, what is the impact going to be not just on a teenager in Menlo Park, but on a range of users, or even on people in the United States who have good reasons to fear for their privacy, victims of domestic abuse, or people within certain orientations, or certain communities.

Anderson: Well that was the Google hack, it went after Stanford students who were standing up for human rights in China.

Kirkpatrick: What if there were an extra-national entity that issued the IDs?

Jungck: But why do we need an ID when the site knows what you're going to buy and who you are before you ever get there? In some of these types of things, we sit and talk about this, and the sites already know who you are, what you're going to buy, the ads kill me with like, "Guys, c'mon, I already bought it yesterday, turn them off." They're so dead-on accurate, but yet we're trying to do this. We still don't even have all of the states on to an ID that we're going to even accept at TSA and we're all confined to an Old World notion of "I'm going to get an ID and a passport" when the internet knows exactly who you are and has for quite a long time.

Kirkpatrick: But wait a minute, you're also a believer that the information will get out, you haven't really said it that way, but on the phone you said to me you're still confident that you can't really suppress bad stuff the way you used to, despite all the bad things we've been talking about on this panel.

Jungck: Oh yeah.

Kirkpatrick: Okay. But if you take your analysis of the internet's targeting capabilities based on the ad technology literally, then Rebecca's point about human rights activists is basically moot, because they no longer have any anonymity.

Jungck: Correct, there is no anonymity on the internet. It is long since gone. And that is this premise that's there. And in every case the only difference of what people find is time. How long is it until enough of the data was analyzed to go back and say who said it when.

Kirkpatrick: But okay, that is a disturbing indicator that for all of her human rights activism and legitimate concerns, as dictators around the world gain more technological competence—

MacKinnon: We're all screwed.

Kirkpatrick: We basically will have—

MacKinnon: We're going to be in the middle.

Kirkpatrick: —no ability to fight back. It's again the arms race of the empowered citizenry versus the empowered governments, and that's scary.

Jungck: But separate the notion of you as a person are able to fight only because you're anonymous. Separated from the freedoms that we protect in the West, is that, no, everybody should be able to have a voice. And the difference is, is that if we think that then something puts ourselves at risk because we say it, then we need to defend that. But don't go and think that the only way we can say something is because nobody knows who I am, because eventually somebody will get a hold of Watson, they'll get a hold of all these databases, they'll get a hold of them and you'll be able to go back in time, and that is the issue.

And so, sure, today you might not know who I am when I say something on some account. But eventually you will know that account is me.

Kirkpatrick: We do have to end, but it's interesting, just an observation: If we worry about dictators because of this kind of logic, at the same time, today's *New York Times*, they're hammering at this issue of money laundering by literally everybody—even Bono and Queen Elizabeth—is being accused of money laundering—

Anderson: Paradise Papers.

MacKinnon: Yeah.

Kirkpatrick: Again, it's a consequence of internet-based transparency, that we can have these revelations, so this arms race is so sophisticatedly complex, but it almost suggests that Central Asian dictators will probably have their money exposed at some point, too, and those are the worst people in the world. So maybe they're won't be able to—

MacKinnon: But will it bring them down or not? Or will they prevent—

Anderson: Well then, we going back to, they'll have their own internet—

Kirkpatrick: Well let me ask you to end by predicting: long-term human rights—optimism or pessimism?

MacKinnon: My father's a historian. Very long term, I'm optimistic—next hundred years, not so much.

Kirkpatrick: Oh God. Okay, well that's a sad way to end. Thank you so much.

[APPLAUSE]