From Cybercrimes to Deepfakes
Friday, July 18, 2025 - 12:30 PM ET/10:30 AM MT
https://www.youtube.com/watch?v=rJH1pmBOa_I&list=PL7fuyfNu8jfP8TWSJzPCsyScNGwbW6xbQ&index=32

Speakers

- Ginny Badanes, General Manager, Tech for Society, Microsoft
- Jeh Johnson, Co-Chair of the Board of Trustees, Columbia University; 4th U.S. Secretary of Homeland Security, U.S. Department of Homeland Security
- **Moderator:** Steve Clemons, The National Interest

Clemons
Thank you so much. Niamh. Let me say, to Chris Coons and Senator Warner, they're going to have their fan club right out in the back over there. Thank you very much. I don't know how many of you were here last year. Just put your hands up. How many of you were at 2 AM and came back to a hotel room here? It didn't work, the key. That was Crowd Strike day. If anybody remembers, Crowd Strike had a glitch. I could not get into my room at 2 AM many of you others had other things that may have happened, travel, etc. I had the pleasure of interviewing Anne Neuberger, the National Security Council, Kent Walker, Google and others. I'm kind of dealing with that, but it's very relevant to today as we discuss the topic from cyber crime to deep fakes, securing the public square while let me just start. We have Jeh Johnson and Ginny Badanes. We have an important task in front of us, but it just struck me that one year ago, we had this problem, and it was one that was an accident. It was an accident of an update. It was not nefarious, as best we know. So I want to ask you to start here with you, Jeh, and say that exposed the vulnerability. It could have been nefarious. Maybe it was a learning moment for villains in the world. I'm very interested in how villains reach and see these moments, but I'd like you to reflect for a moment on the broad question of our vulnerability as a society in a world where we're so dependent on technology, and particularly digital connection technology, that moment and today.

Johnson
So, um, can everybody hear me? Yes, I have learned in my public service career that things are rarely black and white, and several things can be true at the same time, our public square, our internet, is at the same time both perhaps our greatest strength as a free and open society And a huge vulnerability. I believe that the internet has enabled citizens to be more engaged in our democracy. For example, when you look at the levels of voter participation, with the exception of 24 over the last several election cycles, voter participation has gone up over and over again, and I'm sure a lot of that is simply because more Americans are more politically engaged, because it's so much easier to be politically engaged now, but at the same time, because it is a public space with few barriers to entry and standards for exit, we are more vulnerable to attacks. We're more vulnerable to mistakes, somebody failing to test drive and upgrade before they give it to their customers, and so it's a continual work in progress. Obviously, that's not to say that we

should, in some way, limit Americans' access to information, political opinion. I mean separate discussion about deep fakes, AI and so forth. But this continues to be a work in progress, and I've seen a lot of progress just since I was at defense and homeland security with, for example, our election infrastructure. I think we've come a long way just in the last 10 years on that project.

Clemons
Ginny, let me get your take on this moment and you deal with, you know, tech and democracy from Microsoft, I have gotten in and tried to do my best. I'm sort of a neophyte in this, but working hard to become a promulgator of deep fakes when I have spare time learning the tools that are easily available and viable, taking friends of mine and having them say and do things that I find humorous, and so it's part of expression and comedy. But I'm just interested at what point your work in tech and security gets overwhelmed by the rising tide of a new kind of competence that may not have a North Star, that you've got to be careful with these technologies or a North Star and guardrails, that you can't take these technologies and begin committing crimes with them.

Badanes
Sure. So I mean to the point about the fact that you can use these tools for fun, but you can also use them in the tools and weapons framing, right? And this is not new, and that's one thing that we've really tried to keep our eye on as we consider the emergence of AI and the way that it's it's being used across the world is the acknowledgement that it is a very powerful tool that can be used for fun, for productivity, for a lot of things, but of course, people are going to weaponize it. And I think that really came to clarity for us, because last year was, of course, the biggest global election year that the world has ever seen, with billions of people being eligible to vote all around the world. And we are at a moment, as Microsoft, where we want to talk about the good of AI and the tools and the ways people can be using this to improve things from productivity to democracy. And yet we were constantly confronted with the question of, yes, but aren't deep fakes going to destroy democracy? Oh, I thought you were gonna ask me a further question. And so what we were challenged with at that moment was a combination of, where are the obligations in this? There, of course, the bad actors and the way that they behave, and there are ways we can disincentivize that behavior. But ultimately, as tech companies, we had obligations as well. We joined together with a lot of other tech companies and made some voluntary commitments, because it was also with the awareness that the regulatory framework was just not going to come together in time. It wasn't saying we didn't want to be regulated, or we're looking to avoid regulation. Instead, it was saying we have a very short window. There is a lot of concern rising. The technology is improving, and we see bad actors starting to weaponize it, and with these critical democracy democratic elections happening around the world, including, of course, in the US, we felt like there was an important role for technology companies to step into that that was around that one particular issue we learned a ton from.

Clemons
So let me ask you a question both, are we frogs being cooked in a pot trying to convince ourselves that we have safety and security, or are we being cooked by circumstances we can't control? When I looked up to see how much cyber crime there was in the world. The number

this year is 10 and a half trillion dollars. That's a huge number. It's staggeringly big, third largest economy. Yeah, it's the world's third largest economy. And so it makes me wonder, as we talk about this somewhat, you know confidently, why are we so bad? Why are we screwing up? What is missing to bring that 10 and a half trillion down? Oh, I don't know, to a trillion.

Johnson
So every time I get a briefing on one of the boards I sit on from the in house, cyber security person, the information security person, done this, we're doing that. We're doing this. We're doing that. All these green boxes on the slide deck. I think to myself, you're safe until you're not. Those on offense are much more ingenious, aggressive, creative, than those of us who are on defense, and those have been this is as long as I've been looking at this issue, this is still the case. We struggle to keep pace with the ingenuity of the bad guys on the other side, third largest economy in the world. That's stunning to me.

Clemons
But, you know, Ginny, let me answer that. But as you're talking about that cyber crime, and I remember asking one of your competitors out there at Google, Eric Schmidt, when he was CEO, I think I may have done it in Aspen, what will make Americans fall in love with AI at some point? And he says it'll solve a couple of things. It'll solve identity theft, theft and fraud. And maybe it's doing it, I'm not sure, but maybe it's enhancing identity theft and fraud. He'd also say, in a different vein, medical diagnostics are going to be revolutionized and improved dramatically. And I think if you look at that, it is pretty significant. But I am interested in the sort of mixed results that we've seen, and how, when you get to what we, I think, Mark Warner was talking about earlier, trust. Are you worried about the collapse of trust that Americans and many citizens around the world in democracies having virtually everything. And I'm just wondering what you think? What's the magic wand to bring some of that trust back, given the technological threats to it?

Badanes
Sure. Well, trust is our key to doing business. If people do not trust the products that we're putting out there, they're not going to use them, they're not going to sign contracts, we will not exist as a company, and so as a company, particularly in the role that I sit, where I work with groups that are critical to society, such as elections and journalists and others, we recognize that if we don't have trust in the products that we're putting out there, if we're not building them in a way that we can demonstrate as trustworthy and that we ourselves are not trustworthy, then people aren't going to use this technology. And to the point about AI use it is, of course, going to be a benefit. In fact, most people you talk to in the cyber defense space predict that it will be a better tool for defending against than causing cyber because the nature of the way that you review attacks is just going to be simplified by the use of AI. So I'm very optimistic on that side. It doesn't mean that we take our eye off the ball of where it's going. And I worry a lot about the lack of trust in society having in their ability to understand what they're looking at online, right? And that's one of the like critical pieces that we're really trying to work towards, again, cross industry and with governments, is how do you get to a point where an individual a point where an individual is looking at a screen and they see a picture, and they have any context as to

whether that picture is AI generated, AI manipulated, authentic, and the creation of an image with AI is not necessarily bad, so you always want to be cautious not to apply that.

Clemons
So what's the answer, Jeh, to solving this technological gap between safety and, you know, you and I were talking before, and you said, you know, the source of America's strength, In some ways, is also the driver, as big as vulnerabilities. I'm very taken by that. But as you sort of look at this question and say, particularly, I hear it from a lot of companies, honestly, we need more digital literacy. Well, we got people, and I'm just wondering, how you meet people, where they are. How do I take, you know, my, you know, other look, we're getting older as a society. And not to say that older people aren't able to be technological, technologically literate, but it's changing so rapidly.

Johnson
This one really struggles with that, by the way.

Clemons
Yeah, so you're really smart at it.

Johson
No, I struggle with keeping up with the technology.

Clemons
Yes, so tell me how we solve that gap.

Johnson
So two years ago, former Judge Michael Luke and I were asked to co-chair a task force of the ABA on how to secure and sustain our democracy.

Clemons
Tell people what the ABA is.

Johnson
American Bar Association lawyers, because it could be bankers. And we put together a really, really impressive group, non-partisan of Americans that includes retired federal judges, the former Chief Justice of the state of Ohio, people like Bill Kristol, people from the business world like Ken Chenault, Ken Frazier, Richard Haass and others. And rather than say, "well, this is what's wrong with the Trump administration," or, "this is what's wrong with Democrats in Congress," we wanted to look at the underlying public sentiment that leads to some of the election results we see. Part of what we are putting forth as a recommendation is around the cybersecurity, in the cyberspace, in the public square, in our in our dialogue, there are a lot of positive uses to AI, as I think we all know, but there we ought to be able to flag for the consumer, something that is AI driven, something that is AI created. It ought to be prohibited to put deep fakes in political ads, for example, so that's flagged so the American public sees, you

know, “Warning” this is, this is AI manipulated, either in a positive way or some other way. What we should not do, what the government should not do, if we are to regulate in this space, is try to regulate speech, regulate content, it deem something as as fake news, because you always have to think about, if you give this government the authority to do that, what is that going to look like in four or eight years in the hands of another government?

Clemson
So we only got a few minutes, but I want to ask a very blunt question. There is, Ginny, there are a lot of people out there who have power in this political environment in the United States, who believe it is their First Amendment right to create deep fakes, to obfuscate, to create necessarily mistruths that are based on that. That's part of the free expression. And rather than investing in a lot of this architecture, you see kind of a disinvestment in it. What is the solution to that? Does, do the Microsoft, do the major super carriers of the digital space, need to become the accountable and responsible agents, as you see this fight going on over the vulnerability of cyber and some people embracing that vulnerability as an opportunity?

Badanes
So I'll keep this quick, but I think that an analogy to spam makes sense here, which is essentially there was a point in time where Spam was overwhelming the internet. It was coming into your inbox, and this is many years ago. At this point, lot of you folks on the front row probably don't remember this, but at this point, does spam still exist? Of course, do people still fall for scams? Yes, they do, but it's controllable. So if your question about cyber crime and a little bit about how we address this from a solutions perspective, that was not because the tech industry figured it out alone, and it was not because we worked on education campaigns and everyone learned just don't click on those links. It was because all the different sectors came together and had a role to play different intervention point, yes, there was a role for policy makers. They made laws like the can spam law. They made it so you couldn't be where it was illegal to send certain types of emails. You would be prosecuted if you did. Tech companies figured out spam filters. And this continues to be a commitment. We're making it better every, every day. And then, of course, yes, there was an education component that came to it, and that was a government, industry and private sector solution. So when we look at these really thorny issues, anyone who tries to sell you just one of those intervention points is missing the broader picture, because it will never be just one of those things. You have to have them on combination.

Clemons
Jeh, just real, finally, quickly here. Then I want to get at least one question from the audience. You see a lot of tech CEOs in Washington. These tech CEOs used to look at Washington as a place they wanted to spend the least possible time. They were innovators on the West Coast. You know, I remember being at one of the tech CEO’s homes years ago, and they were talking about, “Hey, could technology actually end death?” And there were a couple of DC types in the room who said, “Boy, that's going to be really bad for entitlements.” You know, Washington is looked at as a place that gets in the way of innovation, gets in the way of progress, but now they're all there. They're helping to support, you know, President Trump's inauguration, in the

box, meeting him, seeing him. What is your concern? Is it that you're seeing a hyper powerful government that's going to whack these companies around? Are you worried about the collusion? Or do you have no worries at all?

Johnson
Would you believe me if I said I had no worries at all?

Clemons
Sure.

Johnson
I think it depends on the administration we're talking about. I agree with what you said earlier, that high tech, big tech, you know, for the most part, has tried to stay away from Washington. I'll answer it this way. When when I hear from members of Congress like the last two who were just up here, that gives me a lot of faith in our democracy. People like Mark Warner and Chris Coons, I think, understand this technology, and that gives me a lot of confidence. You know, it's easy to bash Congress, but when you meet, you know, a number of extraordinary individuals who are in Washington. Now, I think there's every reason why corporate America, you know, big tech, should be engaging in the process… in the democratic process.

Clemons
You know, one of the things I think is important and complicated is that while you've got Chris Coons and Mark Warner who stand out in so many different ways, we have to somehow, in my view, this is my own editorial comment, figure out how you broaden that so you've got all these senators, no matter where they're coming from, reflected in our democracy, you know, warts and all, and they're somehow part of that conversation, and feel like they've got states in it. But we'll take one question in the two minutes we have. Did you have your hand up, sir? Let's take a quick mic right over here. And make it super short.

Audience Member One
Yes. **[Name unintelligible]**, Hoover Institution. Is there any danger of hijacking AI, nuclear warheads, nuclear weapons? Is there any consensus between those nine states which has nuclear weapons to avoid that?

Clemons
Different panel but we can go into that. Jeh, what do you think about AI algorithms nuclear safety?

Johnson
Yeah, so I haven't been privy to Intel briefings now in over eight years. I know what I don't know, so I am reluctant to wander into an answer to that question. I'll put it that way.

Clemons
Ginny, any thoughts on that?

Badanes
It’s hard to answer that question directly, but I will say we should be considering AI as the threat to national security. The way that we think about it is, and the way that we hear about it a lot, especially from leaders around the world, is similar to the case that we saw last week with Marco Rubio, where he was deepfaked and someone was calling world leaders and having conversations and extracting information. That's the area that I think is a real current threat, where we have evidence of it, and that's an area we need to focus.

Clemons
In the 30 seconds I have left, Ginny, and I know you probably have been following this pro public report about Microsoft contracts with us, government digital safety of the Pentagon and many Chinese workers that are overseen by those with clearances, but nonetheless, many Chinese workers working on that system. I just want to ask a broad question. You can answer that issue if you'd like to, but the broad question is, for security and safety, particularly in the national security space, do we have to security space. Do we have to hyper nationalize all of the players in that we used to have a kind of digital comments, a scientific comments, that went over boundaries, that work with allies. Is that in jeopardy? Is the science ecosystem? Is the digital awareness ecosystem in trouble because of what we know, in part, because of the issue we learned today about Microsoft?

Badanes
I mean, I think that’s such a broader question than you would necessarily want someone in the tech industry to answer. That's something that a lot of the folks in this audience, and probably Secretary Johnson should answer. The way that we think of these challenges right now is, first of all, if this is a live issue, it's even since we've gotten up on the stage, there probably been development. I know that my colleagues are working closely with our customer on it, and while I don't have a lot to add to it right now, I will say that we take our customer security and national security very seriously. So most likely, we'll have something more to say soon; it'll be rooted in that.

Clemons
I mean, Jeh, the big, the big, you know, big answer question, I think, is whether or not we continue to be a place that draws in the best and brightest engineers from around the world, where we have an ecosystem that is not just American, but it's American, plus many others. I think this is what this case is raising, is anxiety that you don't have, US citizens playing all roles and functions in that, but I don't know a system technologically that can advance, that can be innovative, unless we somehow continue to apply brilliant people from wherever they're coming. So tell me where I'm wrong.

Johnson
I agree with that, and the risk of insider threats is not by any means something you paint on the backs of a foreign national. And so, and I believe you're right, we do depend upon global talent, global economy, to make us as great as we are.

Clemons
Well, with that, we will end this. Please give a big round of applause to our fourth Homeland Security Secretary Jeh Johnson, co-chair of the Board of Trustees of Columbia University and Ginny Badanes, General Manager for Tech Society at Microsoft. Thank you both so much.