# THE ASPEN INSTITUTE

# ASPEN SECURITY FORUM

# DEFENDING DEMOCRATIC INSTITUTIONS: ELECTION 2018 AND BEYOND

Doerr-Hosier Center
Aspen, Colorado

Thursday, July 19, 2018

Suzanne S.: All right. Good morning, everyone. I'm Suzanne Spaulding. I have the honor of being a member of the Aspen Institute Homeland Security group. I am the former Under Secretary at the Department of Homeland Security, where, until noon on January 20th of 2017, I was responsible, with my team, for cyber-security and critical infrastructure protection. I am now leading a Defending Democratic Institutions project at the Center for Strategic and International Studies. I have the privilege of introducing today's ... Or, this morning's panel on elections in 2018 and beyond.

Even as we at DHS were working through 2016 with state and local election officials to secure our election infrastructure, we understood that what was of greatest concern was less that an adversary would be able to somehow take this decentralized system and alter votes that would alter the outcome of the election, but that they could do things that would undermine public confidence in the legitimacy of the outcome of that election. What we further understood, particularly as time went on throughout the summer and into the fall, is that this was part of a long-term campaign by Russia, not just to interfere in the 2016 elections, but a campaign that started long before 2016 and continues to this day, with a much broader goal of undermining democracy, undermining its appeal, making us weak, and undermining public confidence and respect and trust in democratic institutions well beyond elections.

That includes ... We've seen very clear indications of their attacks on the idea of a free press and free media, but also we need to broaden our lens and understand the attacks that are taking place on other institutions, including our justice system and the judiciary, which we see in comments from Putin, Lavrov, in constant attacks from RT and Sputnik, in social media attacks around judges and courts that are dealing with divisive cases involving immigrants, for example. So I was really pleased that the title of this panel was not just 2018 Elections, but 2018 Elections and Beyond, to encourage us to think more mindful of the scope of this, as clearly articulated by the Director of National Intelligence, Dan Coats, earlier this week, that the Russian activities are persistent, aggressive, pervasive, and that they are about attacking democracy and undermining the concept of democracy.

We have got a great panel here this morning to tackle these issues. I'm going to let our moderator introduce the panelists, but I'm going to introduce our moderator, Michael Isikoff, who is an award-winning journalist and a best-selling author. A long career in journalism, he's currently the chief investigative correspondent at Yahoo News, but he has also been a journalist with NBC and with Newsweek. He has written a number of books. Most recently, he is the co-author of a very relevant book, "Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump."

So I'll let Michael take it from here. Thank you, Michael.

Michael Isikoff: Okay. Thank you, Suzanne. We have a great panel to talk about the topic du jour, Russian interference in our elections and protecting our elections. To my left, Monika Bickert, former crackerjack federal prosecutor, now Chief of Product Policy and Counterterrorism for Facebook, the company right in the middle of this discussion. To her left, Michael Chertoff, former everything, including Secretary of Homeland Security and now head of the Chertoff Group. To his left, Jeanette Manfra, Assistant Secretary for Homeland Security for cybersecurity and communications, and actually is the point person for protecting our election this year. So there will be a few questions for you, Jeanette. Tom Burt, Corporate Vice President for customer security and trust for Microsoft, and Kim Wyman, Secretary of State of Washington state.

So Assistant Secretary, I want to start off with you, no surprise. How does it feel to follow the boss, by the way?

Jeanette Manfra: Oh, I'm used to it. It's good. She's good.

Michael Isikoff: Okay. You testified before the Senate Intelligence Committee last March and, in your testimony you said, "Russian efforts to influence the 2016 US presidential election demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations." So what went through your mind when you watched the President of the United States standing next to Vladimir Putin suggesting that which you had told the Senate had happened maybe had not have happened?

Jeanette Manfra: I would say that, first, I think it was important for us to be able to continue to engage with Russia. Overall, we have to be able to engage with all countries, and I think the president has made it very clear since then that he does support the intelligence community assessment, which is what I was referring to in the testimony, so I'm comfortable with how things are going.

Michael Isikoff: You're comfortable with how it turned out, but when you were watching it at the time, where you comfortable or uncomfortable?

Jeanette Manfra: I'll admit, I think I was sleeping while it was actually happening, but when I watched the sort of the out-brief of the event, and then talking about it, I think that the president's trying to balance a lot, and we haven't ... as the secretary mentioned, we have a need to find ways to work with Russia. I think he clarified his statements afterward and made it very clear that he does support the intelligence community assessment.

So I recognize ... I've been in government a long time. You have to balance a lot in these complex geopolitical relationships, and I believe that's what the president is trying to do.

Michael Isikoff: A former colleague of mine, Ruth Marcus at the Washington Post, wrote a column the next day saying the only honorable course for people in positions

such as yours was to resign. So I want to ask you the same question that Peter asked the secretary. Did you, or have you, considered resigning?

Jeanette Manfra: Never.

Michael Isikoff: Michael Chertoff, if you were in the same position that you were in the past, Secretary of Homeland Security, and you heard the president say the kind of comments that he made in Helsinki, would you resign?

Michael C.: Well, first of all, I mean, I can't imagine President Bush saying that. But, look, I would say this. It's really important to recognize that people like Assistant Security Manfra, and Security Nielsen, and others, are doing important jobs, and they're actually doing things that are good and important, and I think as long as you feel you can do that, you should stay. If there comes a point in time that you no longer can function effectively, or you're asked to do, or directed to do, something that violates your conscience or the law, that's a different story. But you don't necessarily have to agree with everything as long as you can contribute and do the mission that you are assigned to do.

Michael Isikoff: Assistant Secretary, I want to ... There's been a lack of clarity about just what the nature of the threat right now is for the 2018 election. Of course, DNI Director Coats, the other day, said the system was blinking red, referring to Russian attacks on our digital infrastructure. FBI Director Wray, yesterday, said we hadn't yet seen intrusions into state election systems this time around like we did before. So help us clear up. I mean, is the system blinking red? Are there particular threats you're seeing playing out right now? Or are you just speculating that the Russians will do the same thing they did last time?

Jeanette Manfra: Sure, and to sort of start with Director Coats' statement, which was much broader around our vulnerability of our digital infrastructure, generally, I think from our perspective, what we see is actors attempting to get into critical infrastructure broadly, and then that's an attempt to hold us at risk in the homeland. Now, whether they have the intent or what that escalation path looks like to use, sort of disruptive capabilities that they may have in place, is a longer discussion, but from my perspective, we do see a concerning increase in country's nation-state attempts to infiltrate our critical infrastructure.

We've issued a series of products specific to Russia attempting to intrude into our critical systems, energy systems, aviation, and others. On the positive side, in that case, private sector and government work very well together, and we were able to stop them from achieving any of their goals, but those sorts of things we see a lot. We also don't have perfect visibility into our critical infrastructure. Most of them are owned by the private sector, and what we see is intelligence. So we need to work with the private sector to understand what they see, so that we can correlate and better understand Russia, or any nation-state that's seeking to infiltrate our critical infrastructure.

With regards to the election, I think you're right. I think it has been a little confusing because it's nuanced. The way that we think about elections is you have a very broad, foreign influence, or malign influence problem, that Director Wray and I think Dave Rosenstein will talk about as well. You have this broad sort of Russian effort to really undermine our democracy, and this is not something new. This is a longstanding thing that they've been trying. Our digital platforms, perhaps, make it easier for them to scale and do it more quickly. So that's sort of a broad thing, elections being part of that, and the FBI really has the lead on working to counter that. We support them.

We distinguish between using digital platforms and others to spread false messages or all the things that are associated with malign influence, we distinguish between that and actual attempts to gain unauthorized access into a state or local system. So while we see Russians continuing to attempt to influence and undermine our democracy, we're not seeing the targeting of the actual state and local election systems that we saw in 2016 right now.

So that's how it's nuanced. I recognize it's complicated, but that's what we see.

Michael Isikoff: But on that point, Tom Burt, I want to ask you, because Microsoft has been doing a quite innovative thing, trying to use the legal system to flush out Russian malicious cyber actors. We were talking just before this panel started. In the course of doing so ... I want you to explain how you're doing that, but also you actually have found some evidence of Russian intrusion in this year's election.

Tom Burt: So starting at the beginning of that story, which was part of the 2016 election, Microsoft's security team supported both the Republican and Democratic National Conventions, and during the Democratic National Convention, our teams observed that there were domain names being registered that looked like Microsoft domain names, but really weren't, and so our security teams and intrusion teams started to do some deep dive, and discovered that these were being registered by an activity group that at Microsoft we call STRONTIUM.

One of the things all of you know is that there's no common naming for these activity groups. We use elements to track them, but it's the same group that's known as Fancy Bear or APT28, and that it's very much the subject of the newest indictment, where the indictment cites very convincing evidence that indeed that organization is directed by officials in the Russian GRU, and we don't know that. We know that their conduct is consistent with that, but the indictment cites a lot of evidence to support that.

So that organization was registering fake Microsoft domains and using them for a variety of purposes. As command and control computers at sites for phishing attacks to take and land those who are victims of phishing attacks, and by using fake Microsoft domains it made the whole scam that they use to infiltrate and control their targets look more legitimate. So we actually treated that like we do

with the botnets that were very active in taking down these criminal botnets, and we said, "This is very similar. We can use a similar judicial remedy."

So we went to court, Eastern District of Virginia, and we got an order taking all of those domains and transferring them to a Microsoft controlled sinkhole. We executed on that and as a result, we actually saw evidence of the breadth of the infected victims that that organization, that we called STRONTIUM, had-

Michael Isikoff: How many domains did you find?

Tom Burt: We ultimately have taken down 90 different domains in several different [inaudible 00:14:42]. So the goal here was to say to this organization, "Stop using Microsoft domain names. If you keep using them, we're going to make it more costly for you." We're not going to be able to stop them from doing their espionage activity, but we can say, "If you use our names, we can go to court and get a remedy that makes that whole thing more costly, and you're going to lose a bunch of the data that you are investing in in the first place, because it's no longer going to come to you. It's going to come to us."

We've had several of those over the two years now that that litigation's been ongoing. We've gotten a final judgment. We've put in place a very unique and innovative special master process so that now, within 24 to 48 hours of us discovering that that organization has registered or is using another fake Microsoft domain, we can get it taken down and transferred.

Michael Isikoff: But in the course of doing this, you discovered some activity that's relevant to this discussion of 2018. So please tell us what that was.

Tom Burt: That's right. So earlier this year we did discover that a fake Microsoft domain had been established as the landing page for phishing attacks, and we saw metadata that suggested those phishing attacks are being directed at three candidates who are all standing for election in the mid-term elections.

Michael Isikoff: In this year's election. 2018.

Tom Burt: In 2018.

Michael Isikoff: Phishing attacks against congressional candidates.

Tom Burt: Against the staff of ... Yeah, of three candidates for election. Now, whether-

Michael Isikoff: Can you tell us who they were?

Tom Burt: We can't disclose that information because we maintain our customer's privacy. So we won't go there, but I can tell you that they were all people who, because of their positions, might have been interesting targets from an espionage standpoint as well as an election disruption standpoint. We don't know the

answer. But we took down that domain and in working with the government, actually, we're enabled to avoid anybody being infected by that particular attack. Our team-

Michael Isikoff: So they did not get into the-

Tom Burt: They did not get in.

Michael Isikoff: Of those candidates.

Tom Burt: That's right. They did not get into those candidates.

Michael Isikoff: But they tried.

Tom Burt: They tried. They weren't successful, and the government's security teams deserve a lot of the credit for that, but ultimately, that one was forestalled. I can say, consistent with what you've heard already, I think it's true, because one of the things Microsoft's been doing over the last couple of years is working in closer partnership with the other security teams in other leading technology companies, including Facebook, to share threat intelligence information, to look for opportunities where we can do joint operations, at least one of which was in the press last December, and what we can do to help protect our community using the threat intelligence information that we have.

I would say that the consensus of the threat intelligence community right now is we're not seeing the same level of activity by the Russian activity groups leading into the mid-year elections that we could see when we look back at the 2016 elections. We don't see the activity of them trying to infiltrate think tanks, and academia, and in social networks to do the research that they do to build the phishing attacks that they then launch, and we're not seeing ongoing activity like the one we were able to disrupt much earlier this year.

That doesn't mean ... As Secretary said, it doesn't mean we're not going to see it. There's a lot of time left before the election. So we and the others in the private sector are trying to be vigilant about that, and we're trying to do more than just that.

Just a quick plug for one of the things we're doing at Microsoft is we've launched a Defending Democracy Program. We are working with Secretaries of State, we are working with ... We did two three-day seminars for both the Republicans and the Democrat community on how they can strengthen the security of the campaigns themselves, which are key attack vectors for the Russian actors. So we did those two three-day seminars.

We're going to continue to work both with campaigns and with the election process, to see what we at Microsoft can do to bring to bear things that we can contribute to strengthening the electoral process in general, and that's across

the election process, the campaign process, and even, ultimately, the whole, much more challenging and interesting issue of how do we deal with disinformation in some way, and other things the technology industry can do to contribute to that.

Michael Isikoff: Secretary Wyman, you oversee elections in Microsoft's home state. Tell us what you are seeing so far in this election, and also put it in perspective from what you saw in 2016. Were they scanning, probing Washington State's election system?

Kim Wyman: Yes, they were.

Michael Isikoff: They were?

Kim Wyman: They were.

Michael Isikoff: How did you learn that? And at what point?

Kim Wyman: Well, I know that for many people in the room, it seems like elections is new to cybersecurity, but those of you who know anything about our systems know that that is just patently not true. We've been in this field for 15 to 20 years. The moment we started putting Internet results out on election night, we knew we could be vulnerable. So we've worked very diligently behind the scenes. Like your world, we just kind of don't want you to think about us. If you don't know what Election Administrators do, then that means we're doing our job well, if we're not the focus of the media.

So in 2016, we started seeing activity on our servers that was unusual, and we were able to block a few IP addresses, and we had a suspicion that they might have been foreign actors, so we contacted the FBI and began working with them, and about the same time was when President Obama declared elections as critical infrastructure. I can confess up here that as an Election Administrator, it made me nervous because the strength of our election system is that there are 7,000 people who are either elected or appointed who oversee elections at the local level and at the state level, and that's a strength, because it's so decentralized you can't have one person who could have an impact and change the outcome of the election.

It's a state responsibility. My nerve wracking moment was kind of battling the resources that Homeland could provide to us, and how it could just really strengthen our security against ... I really don't want the federal government coming in and running our election system, and my role is to make sure that doesn't happen. So in 2016, we started working with Homeland Security, and it was a partnership that was a little bumpy at first, because I think our worlds ... I think they're different, but I'm now realizing that they're very much the same.

We're about transparency. My job is to instill confidence in the voters of my state and the voters across the country, that our elections were fair and they were accurate, and that people that were eligible had an opportunity to participate, and that's what the ... role and responsibility of every Election Administrator in this country. So we're about transparency with the media, with the public, and all of a sudden, I remember distinctly when Assistant Secretary Manfra was being interviewed by Congress, and she was asked directly if the Russians had hacked our system, and she said that 21 states were attempted ... There was an attempt to get into 21 states, to which all of us went, "Wow. That's the first time I've heard that on the news. That's a little alarming, but okay."

Our first question was, "Are we one of them?" To which, of course, the answer was, "Well, we can't tell you."

Michael Isikoff: All right. Assistant Secretary, can you explain?

Kim Wyman: But, no, no, no. But, wait. But, wait-

Michael Isikoff: All right.

Kim Wyman: There's more. There's more. So it was a little rough, and there were a few months where we couldn't know, and it was very frustrating from our end, but we understand now the why, and it makes a lot of sense. I think that-

Michael Isikoff: Wait, wait. What is the why?

Kim Wyman: The why is they were still working through the intelligence and they were making sure that they weren't releasing classified information. I-

Michael Isikoff: But you already knew you'd been targeted.

Kim Wyman: We did, but we hadn't had it confirmed externally until ... I mean, we were pretty certain we were one of the 21. It turned out we were. I think what it led to ... My bigger point here is we worked through that communication challenge, and I was a little critical of DHS initially because I was frustrated. But out of that, we've worked really hard to get those communication channels worked through. We have a coordinating council now that is working very well to address those communication issues and work through it.

Further, as we are working through this, simple things like, and it's governmental territory, and for those of you in the private sector, I apologize, but our OCIOs that oversees the state system is part of our system, the backbone, but our system is separate. So when, for example, the MS-ISAC was giving us information, they would have meetings, and we'd find out about it two weeks later. We would say, "Why weren't we in the meeting?" "Oh, well, you were." "No, we weren't. Who was in the meeting?" And then they would name

our chief information officer for the state, and that's awesome, but that doesn't help me because my chief information officer needs to know that information directly.

I don't report to the governor. I answer to the people. My responsibility is election administration. That sounds really territorial, but it's an important distinction, because if anything happens, it's not the governor who's going to be answering to the people. It's not the governor who's responsible. So we've worked through those, and I think that it's been a really good, healthy thing in the end, because the resources that we're getting from Homeland Security are invaluable, and they are making our system stronger, and are helping me be able to instill confidence in my voters that our system is strong and they can have confidence in it.

Michael Isikoff: Assistant Secretary, you were obviously making a point of how closely you're trying to work with the states. How many of them have taken you up on your offer of providing voluntary cybersecurity assistance based on the declaration that the election systems were critical infrastructure?

Jeanette Manfra: Can I also address the 21 state thing?

Michael Isikoff: By all means, yes.

Jeanette Manfra: Because there's been a lot of sort of different reporting on this. The entities that were targeted were notified at the time that we knew about it. There were certain things that we couldn't tell them at the time, partly because we didn't know. For those of you who deal in cybersecurity, you don't, and frankly for any sort of security, you don't know everything right away. You have to sort of continue to conduct an investigation. We knew that it was suspicious and we wanted to make sure that they knew about it via the MS-ISAC.

For those of you who aren't aware, the Multi-State Information Sharing Analysis Center, we partially grant fund this organization and they have sensors that states can voluntary participate in this program, but sensors deployed throughout the states. All states have at least some of their systems behind it. So we didn't have perfect visibility in 2016. We're working to improve that.

So our process is whenever we get ... There's two ways that we can get information that an entity or a person is being targeted. Usually we deal with nation-state activity. One is through some reporting by a private sector entity or even a victim. The other is through intelligence. When we get that information, our priority is to engage with the actual victim or potential victim. We have a policy that we don't talk to anybody else about that potential compromise. We engage just with that victim, and we don't disclose who they are.

Where we ran into some issues that we didn't fully appreciate at the time, is even though we notified the targets, or the potential victims, we didn't, at the

same time, have that sort of communications mechanisms with the Secretaries of State, and so after engaging with that community for a while, and talking about kind of the 21 states. "Is my state in? What actually happened with my state?" We recognized that it was important to go back and talk to all the actual heads of the election communities in those states, to walk them through what actually happened.

So we did notify. There's a lot of sort of reporting out there that we didn't notify until a year after it happened. That's not true. We did notify the actual targets. What we did a year later was actually engage with all the election senior administrator, and what Secretary Wyman is talking about is now we have in place a protocol so it's very clear who DHS is going to notify in the event that there's anything happening within their state, and we don't run into this issue again, recognizing that we're not going to know everything at the time of the notification.

So to your question, which I've now largely forgotten-

Michael Isikoff: It was how many states have taken you up on-

Jeanette Manfra: How many states have ... Yes.

Michael Isikoff: Cybersecurity assistance.

Jeanette Manfra: Right. So we have ... There's a variety of different programs.

Michael Isikoff: Yeah, I should just say the reason I ask is because when then-Secretary Johnson first proposed this in 2016, there was enormous pushback, especially from Republican Secretaries of State who saw it as a federal takeover of state elections.

Jeanette Manfra: Okay. So all 50 states are partnering with us in some form or fashion. We have a lot of different sort of capabilities and offerings that we provide, but all 50 states are taking advantage of some capability that we offer, and they're all participating, importantly, in the Election Infrastructure Information Sharing Analysis Center, which the MS-ISAC runs, and that's the place where, similar to our industry, has their own places where they can share information amongst themselves and have tailored products, that's the place where they can talk sort of amongst themselves, share best practices, but also communicate with us on any issues.

So some specific things: We have the cyber hygiene scans, which is ... We actually started with the federal government. We scan the entire federal government every single night, all external facing devices and sort of, "Hey, here's some critical vulnerabilities you've got. You should look to patching them." It's a relatively common service, but we've got 34 states and 52 counties or localities participating in that. We have five elections companies that are

participating in that. Just because they're not participating with us doesn't mean they don't have the service. Most of them have it.

We've also got 18 risk and vulnerability assessments, which is much more in-depth, actually us red teaming their systems, trying to hack into their systems and giving them a report of sort of mitigation actions that they can take. But we have a variety of other programs that they're participating in.

Michael Isikoff: I just want to ask you about one line in the indictment that the Justice Department released last Friday that popped out at me. You're talking about how you've been working with the states, but in the indictment, deep down, the indictment says that a guy named [inaudible 00:29:56] is one of the GRU officers, and his co-conspirators, on or about October 28th, 2016, so very late in the election, visited the websites of certain counties in Georgia, Iowa, and Florida, to identify vulnerabilities. That's the first time we heard about this, that they were actually getting into county websites that actually do the vote counting.

First of all, were you aware of that? And secondly, how will you know, or be alerted, if the same sort of intrusions happen this time?

Jeanette Manfra: So it said they visited the websites to look for vulnerabilities. That is not the same thing as actually-

Michael Isikoff: Intrusions.

Jeanette Manfra: Gaining unauthorized access into a system, and that's frankly ... We saw that a lot. The special council investigation is ... It is a separate activity, and they are continuing to conduct investigations. As they learn things relevant to our mission, we absolutely do work with them. So I guess I would just say those weren't intrusions into the system. They were scanning, and if you talk to anybody who runs a system, they are scanned by malicious actors probably hundreds if not thousands of times a week, and now that we're all talking about elections, I'm sure they've seen a massive uptick in that.

So I'm not particularly surprised they're scanning. I think the good news story is they didn't get in. The defenses are working. That doesn't get enough play, but the state and locals have some pretty strong defenses. They're blocking these attempted intrusions and I think that's important.

Michael Isikoff: Kim, do you got a quick one?

Kim Wyman: Yeah, I just want to make one distinction that I think is really relevant here. In the elections world, you sort of have two systems. You have the election administration side. That is voter registration. That's all of your records that have your data so we get you the right ballot on election day. The other side is the tabulation side, and that's the actual systems ... Those are the systems at

the county level and the local level that are actually tabulating the ballots that are counted. Those two systems are separate and, as I've said, for the last 15 or 20 years, the best practice and the standard across the country, is those tabulation systems are in no way, shape, or form ever connected to the Internet. They are all physically secured and have a lot of physical security as well as electronic security.

So when we're talking about the election system being hacked, or people trying to get in, realize that the elections administrators across the country are very aware of the attempts that could be made, and they keep those systems air-gapped and away, not WiFi connected, and all of those things, as a security measure. So we're talking about separate-

Michael Isikoff: But just following up on that, I want to read you a story that has just broken in the last few days, a disclosure that came about because of a series of letters that Senator Ron Wyden wrote to elections systems and software, which is the nation's top voting machine maker, and they admitted in correspondence with Senator Wyden that the company had installed remote access software on election management systems it sold over a period of six years. So that suggests there is a vulnerability there. Is there not, Assistant Secretary? If some of our voting systems have remote access?

Jeanette Manfra: I mean, yeah, absolutely. If they were configured in a way, or the Secretary set them up in a way to actually allow that to be connected to the Internet, which they don't. I think remote access on very critical systems is probably not a good idea, whether you're running an energy system, or a voting machine, but there are compensating controls, and I guess I would defer to Secretary Wyman, that they put in place to ensure that regardless of what vulnerabilities the machine has, there's other physical controls they have in place.

Michael Isikoff: Monika Bickert, I have a lot of Facebook questions.

Monika Bickert: All right.

Michael Isikoff: But before I start, I have one more question on the indictment for Michael Chertoff, about something that struck me. The indictment announced by Deputy Attorney General named 12 Russian GRU officers, and "others known and unknown to the grand jury". The US intelligence assessment from January 17, that everybody has now endorsed and said they agree with, said all this activity was ordered by Russian president Vladimir Putin. Based on what you know about the way indictments are drafted, you are the former head of the criminal division, is Vladimir Putin an unindicted co-conspirator in that?

Michael C.: I mean, that would be a really wild guess, to use a technical term. I mean, it's very standard-

Michael Isikoff: Why wouldn't he be, then?

Michael C.: Well, it's very standard to have a line in an indictment that talks about others known and unknown. Partly that's because there may be others who would be unindicted, co-conspirators, partly it leaves the door open to adding people as more evidence comes in. So, look, I mean, the intelligence community has made an assessment. I don't think it's surprising that an operation like this would be authorized at the highest levels. In fact, I should mention that the Homeland Security group issued a statement which I think is on the Aspen website, making it very clear that the members of that group believe that this was something that was definitely authorized by the Russian government.

But to guess as to what that line means is kind of-

Michael Isikoff: But to include a foreign leader as an either unindicted co-conspirator, or an indicted co-conspirator, which the Justice Department has done from time to time-

Michael C.: Yeah, that's right.

Michael Isikoff: I think of Manuel Noriega.

Michael C.: Exactly.

Michael Isikoff: Why wouldn't Putin be named in this indictment?

Michael C.: I mean, the answer is if there's enough admissible evidence to indict somebody, you would name them, provided you think, A, that there's no collateral or different reason to keep them out. That would be to keep evidence confidential for a while, or because it's pointless because you're never going to get the person. So, I mean, you have to ask the people who wrote the indictment about this. This would be a wild-ass guess on my part.

Michael Isikoff: Okay.

Michael C.: Just a technical term.

Michael Isikoff: Facebook has been sort of in the middle of this whole discussion on multiple fronts. So Monika, I want to ask you a just sort of basic threshold question here. During the 2016 campaign, the US government was very focused on the cyber intrusions and largely missed the huge social media component, thousands of Russian trolls from the Internet Research Agency creating phony accounts, placing phony ads on Facebook, paid for with rubles. How is it that Facebook also wasn't aware that this activity was going on?

Monika Bickert: I'll echo some of what's been said up here, which is that there was definitely more of a focus on the traditional types of cyber intrusion, and hacking, and phishing attempts, attacks on the Facebook infrastructure. That we were focused on, and in 2015 were seeing activity by APT28, and reporting that to the

relevant authorities. The information operations, that is a much tougher thing to define and detect, and it violated our policies because we require people to be authentic on Facebook, and these were accounts that were behaving inauthentically, but detecting this, detecting these accounts, was something that we were far too slow to do.

Some of the things that we're doing-

Michael Isikoff: Weren't the ruble payoffs kind of a clue from the get-go?

Monika Bickert: Well, the reality is we've got six million advertisers, and advertisers pay in a variety of different currencies. Some of these were in rubles. We have legitimate Russian advertisers. And as has been widely reported, the content in these ads, much of it would not, on its face, have violated our policies. This was content that was a little harder to find if you were looking at the face of the content. There's some sorts of policy violations where you look at the face of the content, and it obviously violates policies, you remove it. That's the easier stuff.

The harder stuff is looking at who the speaker is, and determining if that is really the right person, and that's actually quite hard to do. What we're doing now to try to get better, and we are in a much better place, a couple things. One is introduce some real barriers and some deterrents into the process. Some of that involves requiring a greater transparency around political or issue ads than is required even with television advertisements. So now, if you want to run a political or issue ad on Facebook, you have to go through an identity verification. You've got to be within the United States. We mail you something. You show us a government ID, and the last four of your social security number. I mean, it's a pretty onerous process.

So this is designed to ensure that the people who are advertising about political issues in the United States are American actors, and we know who they are, and now we're also showing on those ads who has paid for that ad. You can also click and go to an ad's library ... By the way, if this sounds like a big change, it is, and if it sounds easy, it's not. We've had all kinds of enforcement errors because trying to detect what is an issue ad, trying to define that, has proven to be incredibly thorny, and we've had-

Michael Isikoff: How do you define it?

Monika Bickert: We are looking at the Proposed Language in the Honest Ads Act as a guide. We're also talking to a lot of third parties. So if something is a legislative issue of national importance, or if it concerns an election, or a candidate for election, that's something that we would include, and you can go on our site and you can see exactly how we define this, but you get into these really thorny questions about whether or not something should be covered or not, and right now we're

taking a broad approach of saying even if this seems really over-broad, we want to make sure we're erring on the side of knowing who these advertisers are.

Another reason that this is notable is because when advertisers are running ads on social media, they expect it to be fast. That's the whole beauty of it. You want to have a sale tomorrow. You go on today, and you promote whatever you're doing, and it goes live right away. That can't happen now, and we've had a lot of advertisers say to us, "This is too onerous for us to have to get something in the mail, and respond, and get authorized." That's the sort of precaution we're putting in place now as a barrier.

Michael Isikoff: That's the purchased advertising component, but you also are dealing with the fake news, hate speech, and other areas where you're trying to police content, and I know you've set up a whole new systems for doing that with artificial intelligence, then reviewed by actual people who have-

Monika Bickert: Yes, generally.

Michael Isikoff: But when peoples look at Facebook, they look at things like Infowars. Alex Jones, who has published all sorts of stuff, Sandy Hook massacre didn't take place, Pizzagate. Yet they're still up on Facebook. Why is Infowars still up on Facebook?

Monika Bickert: So anytime that Infowars posts content that violates the policies, we remove it, which we have done, but there's a difference between removing the violating content and actually removing the speaker. There is a point at which we will do that, if people continue to violate our policies. Infowars is not there yet. But if they meet that certain threshold then we will remove them.

In terms of how we think about false news, because I know there's a lot of questions about it, there's a couple things we do. The majority of the false news content that you see on a social media site like Facebook is the financially motivated spam type of stuff. So you defeat that by, in our case, largely using technology and artificial intelligence to identify accounts that are spreading spam, accounts that are false. We've gotten a lot better at that in the past couple years, and now, before the German election, before the French election, we were removing tens of thousands of accounts. Before the Alabama special election, we were removing a lot of accounts using that sort of technology, that were Macedonian spam type accounts.

So that's one thing you do. But then you have these stories that are misinformation, people on different sides might say, "This is just sensational," or, "This is clearly false." What we're doing there is we're using ... We don't remove the content. What we're doing is trying to provide more information so that people can put the content in context. So if there is a story that might be false, and that might be because people have reported it to us as false, or because our technology is telling us that, for instance, in the comments under ...

You share that story and your friends all say, "This is a hoax, you idiot," or that sort of thing, if our technology is picking up on that, then we send that to third party fact checkers.

If they agree that this story is false, then what we do is we counter the virality of it. So we'll reduce the distribution, and then we include, for anybody who sees that on Facebook, related articles. So you see the article, and then underneath it, it's a series of here are the articles from mainstream publications around the Internet, so that you have the ability to put that in context.

That's a result of having tried a couple different things and looked at what tends to engage people. Initially what we were doing was saying, "This story is disputed. Click here to learn more." And we were finding that that didn't necessarily drive people to click and learn more. The related articles and providing more information is working better.

Michael Isikoff: But I have to say that there is still confusion about your thresholds for when you take stuff down and when you don't, and there is, seemingly, inevitably, a lot of arbitrariness to it. Now, Motherboard just published some of your internal guidelines for a chain-

Monika Bickert: Oh, we published those.

Michael Isikoff: Oh, you published them. Okay.

Monika Bickert: We published those back in late April.

Michael Isikoff: Well, they were claiming [crosstalk 00:44:32] for it. A training document for hate speech says that a organization or public figure, if there's a page that has ... The page has to receive five strikes within 90 days for the page itself to be deleted. Facebook moderators are told to remove a page if at least 30% of the content posted by other people within 90 days violates Facebook's community standards, and another hate speech document says a profile should be taken down if there are five or more pieces of content from the user which indicate hate propaganda, photos of the user present with another hate propaganda.

So that seems like, first, a bit complicated. And B-

Monika Bickert: It's far more complicated than that, even.

Michael Isikoff: But then who's making the call on whether this is a strike that goes against you or whether this is an example of hate speech?

Monika Bickert: This is one of the interesting parts of our job, is trying to figure out what the consequences should be for any one policy violation. So the policies are public. They have been for years. Back in April, we took a really unprecedented step in publishing the internal guidance that we give our reviewers. Every once in a

while these things would get published, they'd get leaked, they'd get published in the news, and our thought was sort of, "We might as well just put it out there. If people want to know it, let's just put it out there." So we published it in April, and now you can go on the site and you can see the guidance that we give our reviewers.

Now, when it comes to enforcement consequences for policy violations, there's obviously a lot of different shapes that violations could take. If you upload an image of child sexual abuse imagery, your account comes down immediately, it's reported to law enforcement. If you bully somebody in your high school class, you get a warning. So there's different sorts of levels of consequences for different types of policy violations. We also have different levels of reviewers, and reviewers are trained in different ways.

So some reviewers are dealing with certain types of content where the answers might be more simple, and in certain ... Like, for instance, we had a report recently that said something like, "When reviewers see this content, they are never to delete it, and they are never to leave it up on the site. They are to mark it as sensitive and escalate it." What that means is sometimes the reviewers have to send it up to a higher level. So what the enforcement consequences are, there is a rubric for that, but it's pretty complicated.

With pages, you might have a page that has 20 administrators, and it's publishing 300 pieces of content a day, and you've got one bad actor among the administrators. What we would rather do is take action against that one person, or let other people in that page have the opportunity to reform the page.

Michael Isikoff: But do your reviewers actually have debates among themselves? Does this qualify as hate speech or misinformation, or not? And, as a corollary, are you the ultimate arbiter? Are you the content cop?

Monika Bickert: There's about 7,500 reviewers ... Actually, there's more than that now, but that's the last public number that we've used. Sitting around the world who do the first level of review. They have really no leeway to have conversations about should we count this or not? If you go look on our site, the rules are very detailed and objective. Now, that's great in one way because it's good at things like reducing bias and getting things escalated. It's bad in another way, in which ... By that I mean, you sometimes have content that's really close to the line, and yet our rules, when applied, will say, "In this case, we don't consider this bullying," and everybody in this room would look at it and say, "Oh, it's clearly bullying, but our rules don't cover it because we've written the policy to cover the majority of cases."

So anyway, the rules are fairly detailed and objective. If a reviewer thinks that the prescribed policy outcome doesn't make sense, then they can escalate it up the chain. It would come to my team, and yes, we will sometimes ... We'll look at it. We'll say, "Well, we're going to make a call that we think is consistent with

the additional context we have." Senior leadership will be involved in those conversations sometimes. We also have a policy that says if something is in the public interest, but otherwise violates our policies, we may leave it up.

The most common scenario for that is if something is nudity. We typically wouldn't allow, for instance, an image of a prepubescent child with genitals showing. But let's say that this is a photo after an atrocity, and there's a victim of a bombing, and this is being shared to spread awareness, and there's child nudity visible, but it's very clear that this is for newsworthy purposes. In that case, we might override the policy.

Michael Isikoff: Larger question here, which is given that so much of the world now communicates through Facebook, and Google, and Twitter, Michael Chertoff, should we be comfortable that we're letting them decide, Monika and her cohorts, and the other social media companies, decide what we can read and what we can't?

Michael C.: Well, I would say this. I would say first of all, it's better than having the government decide, because the government's going to have an interest in a certain way. But I do think it's challenging, and one of the things I would say in general, and I understand what Monika's trying to wrestle with here, is on the one hand there is some editorial responsibility. You can't incite violence. You can't deliberately and systematically propagate things that are hateful. But we still basically have a default position in the US in favor of free speech as far as content is concerned.

I think it's completely appropriate to disclose who's saying things, and to point out where there are things that are ... or have counter veiling issues. That's part of the marketplace of ideas. But it's really easy to go down the slippery slope of beginning to say, "Well, this is fake," and pretty soon it's someone's going to decide what they like and what they don't like.

I will tell you if you want to go to a place where if you want to read their literature, they will absolutely tell you that it's appropriate for the government to control content, it's in Russia, where they define cyber warfare as to include information that they don't like. So I think it's not a great situation, and ideally people would self-educate, and we have to do that, but I think that the approach they're taking is a pretty balanced approach.

Michael Isikoff: Monika, you had something you wanted to add.

Monika Bickert: Yes. I would really agree with that, and I would note that speaking to an American audience about this is different than when I speak elsewhere. More than 85% of the people using Facebook are outside the United States, and when I'm having conversations in the rest of the world, sometimes the instinct is, "Well, if it's illegal under our government's laws, or if our government says that it shouldn't be up there, take it down." So we do have the process in place in

specific countries where a country gives us legal processes and says something is illegal, that we may block it in that country only. It is often not the outcome that you would want.

What we try to do in crafting our policies is make sure that we're not doing it in a silo. So every other Tuesday we have a meeting at ... global meeting, lots of people from different teams across the company, operations, engineering, legal, and so forth, but we're also engaged with more than 100 groups and experts outside the company to get their feedback on specific policy issues. So, for instance, next Tuesday's meeting, maybe we're considering what we're doing with photos of fetuses. This is a real issue. I mean, we deal with all sorts of odd issues like this. What we would do is reach out to groups and experts on free speech, on pro-life, pro-choice, and make sure that we're understanding how people see this issue, and how we can best craft a policy for a global population that's using our service.

Michael Isikoff: You also just published new guidelines on misinformation, I believe. Tell us about that and how that works. That sounds like a variant of fake news, but I gather it's something more specific.

Monika Bickert: Yes, this is a ... Our recent announcement was about something we're trying to get ahead of, and I'll be candid in that this is something that we're still trying to figure out. In general, if we have people that are sharing news that may be false, the approach is what I described earlier. The fact checkers, and then if something appears to be false, reducing the distribution, sharing information, not removing it. We are, however, thinking that we will see situations where there is violence on the ground that is closely linked to speech such as a doctored video or photo, things that are sometimes referred to as deep fakes.

So you've got a situation, let's say, that there's some tension in a region, and you've got ongoing riots, and somebody puts a photo up and says, "Look what the police just did in this region," or something that is intended to stoke violence, and we're putting in place a framework for having trusted partners in areas that we could reach out and confirm is this linked to ongoing or imminent threat of real world violence? And is this content false? And if so, we'll actually remove the content. We have a-

Michael Isikoff: Yeah, that's really important, because there's an ... One of the concerns I think people have is an operational impact where somebody does, in fact, say, for example, "Oh, there's a storm here. Run there." And actually it's the reverse, and I do think we've seen examples of this. So that's a very important capability.

I want to get to questions, but before I do, I have one last question for you, Assistant Secretary. I went over your testimony last night, and in it you referred to the NPPD, the National Protection and Programs Directorate-

Jeanette Manfra: It rolls off the tongue.

Michael Isikoff: The NCCIC, the National Cybersecurity and Communications Integration Center, the EIS, the Election Infrastructure Sub-sector, the EAC, the Elections Assistance Commission, the GCC, the Government Coordinating Council, the EISSSP, the sector-specific plan, the ETF, the Election Task Force, and my favorite, MS-ISAC, the Multi-State Information Sharing and Analysis Center. On behalf of everybody here at the ASF, I'd like to ask you, is there an assistant secretary for acronyms?

Jeanette Manfra: I wish that was my job.

Michael Isikoff: That's usually the Department of Defense, actually.

Jeanette Manfra: Yes. We have our own language. If I could say one thing, National Protection and Programs Directorate, that is the name of our agency within DHS that does cybersecurity and critical infrastructure protection. We continue to try to work with Congress to change our name, because we need an active Congress to change our name.

Michael Isikoff: What do you want to change it to?

Jeanette Manfra: Cybersecurity and Infrastructure Security Agency, and this was back-

Michael Isikoff: You got the acronym for that?

Jeanette Manfra: CISA, of course. So, actually Under Secretary Spaulding started this in the last administration, and we're continuing it. We do have a bill passed in the House, and one on a committee in the Senate, so we're really hopeful that we can get that changed. But it is really important. The jokes on the acronyms, completely get that. I think you all had to-

Suzanne S.: We do.

Jeanette Manfra: Have a special lesson on all of our acronyms.

Suzanne S.: Yes.

Jeanette Manfra: But to have an agency name that reflects what we do. It's hard to go around telling people that we work for NPPD, and, yeah. So if I could just put a plug in for that.

Michael Isikoff: Questions. Gentleman all the way back there.

Male: Thank you very much for sharing your thoughts with us. I'm [inaudible 00:56:11], security analyst for ZDF German TV. This is a question for Monika. Given the rise of antisemitism around the world, specifically in Europe and also in parts of the US, can there be such a thing as unintentional Holocaust denial? I'm, of course, asking that question because of the remark that Mark Zuckerberg

made. How much of a role does intention play in the application of the guidelines. Also, the most recent guidelines you just referred to.

Monika Bickert: Great question. So generally our approach is if people celebrate the Holocaust, if they try to justify the Holocaust, if they defend it in any way, we would remove that. We would remove any content that mocks survivors or victims of the Holocaust as well. We also would remove Holocaust denial content in countries where governments have asked us to do so because it's illegal. So, for instance, in a country like Germany, we would remove it. Now, in a country like the United States, where, in fact, it's constitutionally protected speech, we will apply those other policies. If people are celebrating it or defending it, we would remove it.

But we do not generally remove content just because it is factually inaccurate, and that's true whether people are talking about any world event, or any other situation. We don't have a policy on Facebook that requires you to be truthful.

Male: What about people who have postings denying the Armenian genocide?

Monika Bickert: The same policy would apply. So there's no requirement to have your facts right. However, if people are celebrating violence, encouraging violence, justifying violence, or mocking victims of violence, any of that content would be removed.

I should also say that sometimes we'll see content that is coming from ... Again, this distinction between content and bad actors. Often, the content that you'll see is being shared by people who are hiding behind fake names, and we do have a policy on Facebook that requires you to use your real identity. So oftentimes accounts or networks of accounts that are using inauthentic means will also be removed.

Michael Isikoff: Other questions? Over here.

Joe Simitian: For all of the panelists, Joe Simitian, Santa Clara County Board of Supervisors. That's the county in Silicon Valley with roughly two million people. There are 3,000 counties that have election responsibilities. What's the single best piece of advice any or all of you could give counties to deal with the continuing threat of foreign interference with our elections?

Kim Wyman: Oh, I'll start. I think it's really about partnerships in the counties, and even the local towns and cities that do elections across the country, working with their Secretary of State office and partnering, because for example, in my state you have King County where Seattle is that has about 1.2 million registered voters, and I have Columbia County, that has about 1,500, and their capabilities in terms of IT and even just election administration are so widely different, but the responsibility's the same.

So we're really partnering with our counties. I'm using the federal money that we received recently from Congress on the [inaudible 00:59:33], we got about $8 million to help beef up those smaller counties, and help with sensors and firewalls, to training and doing tabletop exercises. I think the thing that local jurisdictions should be doing is not only working with their Secretary of State's office, but when they have opportunities to work directly with, say, the MS-ISAC, and be able to be one of the counties that's reporting information and getting information, that's just one more strength that they have, and one more tool in their toolbox. Each county and jurisdiction's going to be different, but it's really about utilizing those partnerships.

We're actually pioneering a partnership with the Washington National Guard, because they have so many members that work at wonderful companies like Microsoft and Amazon, that they have this great knowledge and I have a great cybersecurity team. So they're going to be helping us with our continuity of operations plan that we already have with them, to take it one step further and do training and some evaluation of our counties and the state.

Michael Isikoff: Anything you want to add?

Jeanette Manfra: Sure. I would just reinforce ... really important to work with your state. As you mentioned, there's thousands of jurisdictions out there. Some are counties. Some are townships. Being able to touch every single one of them is pretty impossible, so it's really important to work with your state. Best practices ... We've done a lot of assessments with the election community, with federal government agencies, state and locals, everybody.

So we continue to see the same kind of challenges, and they're not real sexy to talk about from the cybersecurity perspective, but it's having good patch management processes in place. It's ensuring that your systems are configured correctly. It's ensuring that you don't have unsupported operating systems. It's those things, and we're continuing to talk to people about that. A lot of those, it does take some investment, but it's worthwhile investment. It'll be more helpful in the long run.

The last thing I would say, and I'll turn it over to Tom, is report anything suspicious that you have. I think a lot of people have this perception that the government has this perfect picture of what everybody's trying to do. Of course, if only we had all the classified briefs to tell you about it. That's just not true, and we need to have partnerships with those who actually have visibility on the systems. We don't see everything that's going on in your systems. We need to work with vendors. We need to work with the owners and operators.

The best thing that you can do is if you see something, say something. We talk about it in the physical space. It's the same thing in the virtual space as well. The more trust that we can build, the more the people are willing to share, the more that we can start to correlate amongst ourselves what's really going on, because

you may not think it's a big deal, but if you share it, we may be able to tie it to some other things.

Michael Isikoff: We probably have time for one or two more.

Tom Burt: Another thing, really quickly, just to add to that, which would be true for whether you're a county, or a state, or really any organization. If you read the indictment that just came out last Friday, you'll see that by far and away, and this is true just in general. The primary vector for getting into these networks is phishing. That's how most nation-state actors do their work, and they're very, very good at it, and what that means is the number one thing you need to do is have two factor authentication on every device and every account that communicates with your system.

That's hard work because people like to bring their own devices to work, or work from home with a different device, but every device that communicates with your system needs to have two factor authentication because that is a huge ... not a perfect, but a massive defense to phishing campaigns.

Michael Isikoff: If only the chairman of the Clinton campaign had known that two years ago, things might have been very different. The woman over there.

Stacy Omer: Hi. I'm Stacy Omer. I'm with FireEye. My question is for Assistant Secretary Manfra. Going back to election security, the grants that were included in the omnibus last year, two part question. First, do you think states are using the funding the way that it was intended? And second, I've realized Congress will have to authorize it over and over again, but do you foresee that becoming part of the department's larger portfolio of grants?

Jeanette Manfra: So to clarify, it's Election Assistance Commission that runs that grant program. I think it's very broad how states can use it, what the Government Coordinating Council that Secretary [inaudible 01:03:58] was referring to before, what they did is put together guidance and best practices on ways to use that. It's not requirements, but it's best practices. I think we see a lot of states using that money thoughtfully. Everybody's different in what they're trying to shore up, but I think we see a lot of states being very thoughtful about how they use that money.

Michael Isikoff: Over here. Well-

Female: [crosstalk 01:04:34].

Michael Isikoff: Yeah.

Bryan Weir: It's a race. Bryan Weir. Monika, do you feel like ... I was just thinking about the examples you were giving on misinformation, manipulative video, wrong video, and the Secretary's amplification of that. Do you feel like you're held to a higher

standard than the other media in that regard? There's certainly a lot of criticism that has been directed at Facebook. [inaudible 01:04:58] other thing, there's a magazine cover recently that was not accurate, either. I mean, is your standard higher? Is it the same?

Monika Bickert: I don't know about that. I mean, it is a different kind of service, but I think what we're seeing is that we have so many people who are coming to Facebook every day. More than two billion people use the site monthly, and more than a billion every day. So we have so many people that are coming and sharing things that are important to them. They want to see real stuff, and it's important for us that we get it right. There is a lot of tension between the sort of American model versus how some other countries expect us to operate, but what we're trying to do, generally, is just give people a lot of information so that they can tell when something might be fake, and then remove the obviously fake accounts.

Michael Isikoff: One question I actually meant to ask you earlier and neglected to. We had a discussion early on about what the Homeland Security folks were seeing in terms of cyber intrusions this time around, but what about on the social media front? Are you seeing the same sort of Russian malicious actors trying to exploit your platforms, or spreading the same sort of messages that they were doing in 2016?

Monika Bickert: With regard to information operation specifically, keeping in mind that we're a very global company, and so we're looking at the elections in ... the recent one in Mexico, the upcoming ones in Brazil and India. We did see another batch of IRA accounts that we removed back in April. This was a couple hundred IRA accounts and pages. They were not targeting Americans. This was content that was Russian language in Russian speaking countries, but we are watching for that activity, whether it's against Americans or others.

Michael Isikoff: But you have or have not seen it so far this year?

Monika Bickert: Well, that was back in April. That was-

Michael Isikoff: Targeting Americans.

Monika Bickert: Targeting Americans.

Michael Isikoff: Yeah.

Monika Bickert: I think our ... Of course, we're keeping our eyes open, but I think right now the new tools that would identify and remove fake accounts, like the IRA was running, combined with the new requirements for transparency in advertising, are such that I think we're not seeing that same conduct that we saw before.

Michael Isikoff: Any others? Over here.

Bob Rose: Thank you. Thanks, Michael. Bob Rose. Jeanette, this is kind of directed at you. There are lot of ways to effect the outcome of an election that go beyond in choosing of the systems. What's being done by DHS as it relates to false news generally going beyond Facebook, talking about the availability of when the polls are open, who's eligible to go, lying about a candidate? I mean, there are a lot of social media false news kind of ways to effect the outcome of an election, Jeanette. So what's DHS doing to try to deal with those?

Jeanette Manfra: And followup? Okay.

Male: You know, it's ... I have the private sector side of that. I just want to tie it in. Considering that I think I heard Facebook say, "We don't label things fake. We simply give you related articles if you wish to pursue and in fact figure out for yourself if it's fake." The question then is, following Bob's question, is the private sector up to defending our country in this way?

Jeanette Manfra: I'll go first.

Michael Isikoff: Well, it's directed to you.

Jeanette Manfra: Yeah.

Michael Isikoff: At least the first one was.

Jeanette Manfra: I can't answer for Facebook. So there was a few different parts of that question. As mentioned, we're very focused on sort of the actual voting process itself, what the state and local communities run, and, yes. So working with the Election Administrator community in how best to communicate to the public, which they already do, but to the extent that we can help provide additional products, resources, ensuring that if we did, say, see some campaign that was trying to misdirect people to the wrong polling locations, or something for that example, we'd work with that community to ensure that they were aware of that, and they could alert their voters to what was really going on, and ensure that they had the correct information.

For us, I think the most credible messaging comes from that local or that state organization that runs the voting process. That's who voters are going to turn to to understand exactly where they should vote. But I think it's important, and we've been talking about this a lot. Ensuring that voters understand that you have the right to a provisional ballot, that you ... Even if somebody were to mess with our voter registration databases, it doesn't matter. You can still vote, and there's a lot of things that states have put in place in addition to that, but you still have those basic rights. And just ensuring that that gets out there.

So as much public communication as we can, and to the extent that we learn that an entity is trying to misdirect, or cause misinformation to voters, we would work to combat that with that community.

Monika Bickert: As to the second question, I'd say let's distinguish between two things. One is when we have coordinated information operation sharing this information. There's a variety of tools we're using to detect and remove that, and I should also say there's a lot of industry collaboration, and we have a lot of partnerships where we're talking to academics, we're listening to governments, and trying to identify and remove that faster. Then there's the situation where you have individuals sharing a story that they think is true that our fact checkers think is not true.

We hear from people regularly that having a private company decide what is true, what you shall believe and what you shall not believe, is not something that they want. In fact, we hear concern even about using third party fact checkers to make the decisions about when we should demote something and provide related information. So what we're doing there to mitigate those concerns is the fact checkers ... Any organization can apply to be a fact checker if they are Poynter approved, and they adhere to the International Fact Checking Network code of principles. Once-

Michael Isikoff: Wait. The International Fact Checking code of principles?

Monika Bickert: Checking Network code of principles. Yeah, these are-

Michael Isikoff: I didn't know it existed.

Monika Bickert: It does exist, and what we're seeing, I think, is that as the concerns about false news grow, there is a real appetite for organizations who will meet a very high standard in determining whether or not ... They'll go back and they'll fact check things. They have to write and justify their opinion on why something is true, or false, or somewhere in the middle, and based on those rankings, we will decide whether or not we should provide that additional information.

Male: So in coordinating these things, you will label something fake news?

Monika Bickert: We'll take them down.

Male: Take them down.

Monika Bickert: So the IRA accounts? Those all come down because they were inauthentic. We are sharing ... We have something called ThreatExchange where hundreds of companies ... and this has been in place since 2015, but the scope has expanded. Hundreds of companies participate in sharing information about attacks they are seeing on their networks. We're now seeing a much greater collaboration among industry partners in the way that we've seen in the past with child safety and with counter-terrorism. Now, election integrity and combating false news, this is sort of the new ground where industry is really coming together.

Michael Isikoff: Well, I think ... Do we have time for one more, or ... We don't? We don't. All right. Well, I want to thank our panelists. I just want to say ... I also would invite the audience to take everything they've said here today and then apply the international code checking of professional inspecting-

Monika Bickert: The International Fact Checking Network code of principles.

Michael Isikoff: Yes. Okay. All right. Thank you very much.