James B. Comey
Director
Federal Bureau of Investigation

Symantec Government Symposium
Washington, D.C.
August 30, 2016

The FBI's Approach to the Cyber Threat

Remarks as delivered.

Good morning everybody. Thank you for the introduction. Thank you for the opportunity to share some thoughts with you. Let me start by thanking Symantec for putting this event on for the 13th year, and for the work you do—and the attendees do—to keep so many of us safe from the threats that the FBI worries about every single day.

What I want to do this morning is give you a sense of how the FBI is thinking about those threats—some sense, from our perspective, as to what we think all of us can do together. Then to focus a little more on the FBI, and explain to you how we're trying to contribute to reducing the threats across a variety of bad actors. Then I want share, because I can't get on the stage without talking a little bit about the problem we call Going Dark, which is encryption. And then I'd like to take your questions. And I'm hoping you're going to think up a question that has nothing to do with Secretary Clinton's e-mails.

Let me start with the threat. How do we slice up the stack of actors that all of us in this world have to worry about? Obviously, we start at the top of stack with the nation-states. Think China, Russia, Iran, North Korea—entities that are getting much more sophisticated, much more aggressive in state-sponsored intrusion activity, which I'll say more about in a minute.

Next level down the stack, we would put the multinational criminal syndicates that are getting increasingly specialized in their roles, and increasingly sophisticated. People who are interested in stealing information just to make money to sell it to the highest bidder, the way criminals have always done it.

Next level down in the stack would be the purveyors of ransomware, which is spreading, from our optic, like a virus all across this country and all across the world. Where, for people running a business, it becomes a challenge between choosing paying to get on with your business, or resisting the spread of that virus and helping us fight it and root it out.

Next level down in the stack, we put the hacktivists, which is a motley crew of people with all manner of motivations—political, personal, philosophical, some that are hard to figure out at all—who are interested in information to embarrass, to expose, in their view, to send messages. And it's not about money for them.

At the bottom of the stack, which may surprise you, we would put terrorists. The reason they're at the bottom of our stack is terrorist organizations around the world, especially the group that calls itself the Islamic State, are proficient at using the Internet to spread their message of hate, to recruit, to communicate for operational purposes. They are literally able to buzz in the pockets of fellow travelers or would-be terrorists 24 hours a day. And that has an enormous impact on the FBI's counterterrorism work.

But what we don't see them doing yet, and I underline yet, is moving towards and developing the capability for computer intrusions. But logic tells us that has to be the future of terrorism. As we make it harder and harder for them to get physically into this country to kill people and to do damage, surely they are going to turn to try to come in as a photon and do damage through the Internet.

That's our stack of actors that we worry about. Let me say a few words about how we see them operating.

The overarching theme is increasingly sophisticated, larger-scale attacks from all of those actors, combining multiple techniques, and especially combining inside knowledge that's harvested through social media; that's harvested through all the ways to come to understand the potential human vectors that they might use to get into our organizations. Because all of you in this room know this, as we make our systems harder and harder for people to get in from the outside, the weak link always remains our people. The threat actors know that, so they spend a tremendous amount of time trying to understand how they might get in through human beings; through spoofing the existence of a particular human being; or through actually recruiting someone who is

disgruntled, who's unhappy, who's looking to damage an employer, or maybe to make extra dough on the side.

What is this stack after? That's obvious. They're after information. They're after access. They're after advantage, whether that is political or economic or ideological. We're worried of course not just about the loss of data in pursuit of those goals; we worry every day about the potential for the manipulation of data to accomplish the same illicit ends.

The impact of the attacks—you're in this room because you understand the impact of these attacks, so I won't spend a lot of time on this—they are more than just attacks on our infrastructure. They are attacks on our employees and our customers. They are attacks on our reputation, on our economy, on our security, on our basic freedoms. The Sony attack was an attack aimed at free expression. It was the act of a bully looking to silence speech in the United States, and around the world, by intimidation and harassment, in that case, of Sony Pictures.

What can we do? We can't possibly prevent every attack, especially the more sophisticated actors. But we believe that this behavior, no matter where it comes from in that threat stack, is deterrable. These are not people who are committing computer intrusions high on crack or inflamed by having found their significant other in the arms of a stranger. These are people who are thinking, coldly and dispassionately, at a keyboard as they act. And that offers us an opportunity to change behavior. That is an audience that is potentially deterrable, because they're not drug-addicted or desperate in the way that a bank robber might be or a mugger might be.

To do that, we need to be more predictive, less reactive. And we as a government need to recognize that the answer is not just us—it's the government and all of our private sector partners. We think there are three joint goals that all of us have in this regard; three things we all must do together. And then I want to talk to you about how we think the FBI in particular can contribute. But all of us together can do three things.

First, we can reduce vulnerabilities. We in the government can equip you in the private sector to understand actors and cyber criminals and their techniques, their tactics, and their procedures. You in the private sector can help those of us in the government understand the same thing. Together we can use that information to harden our targets. We can make, with that

information, a decision to have cyber security be a priority at all levels in our organizations.

There is a risk that leaders sometimes will think of cyber security as something that is a one-among-other risk factor. It's kind of off to a side, and we turn and have a conversation about it at our quarterly meetings. Folks need to understand that cyber security must be an integral part of everything we do, in any kind of enterprise, whether it's government or private, no matter what type of work we do. Because we are living our lives in the digital space, cyber security affects every aspect of an enterprise.

It is not just about our systems. It's about our people, about our processes, about our technology, about the way in which we interact with the world. Cyber security has to be part of every single thing we do; it should be part of nearly every conversation in an enterprise.

That's the first thing we can all do together, is try to share information to raise the focus and reduce our vulnerabilities.

Second, we think we can all work together to do a better job of reducing the threat. For the reasons I said, we think this is behavior that is deterrable; that we can, by together acting, hold people accountability in a way that will change behavior, and I'll say more in a second about how the FBI is trying to do that.

Third, we think we can do a better job collectively at mitigating the damage. We in the government, and in the private sector, can help people understand better, quickly: What just happened? And what's the path back to restoring our processes and our business?

That's what we think everybody can share in terms of goals. The pieces that we the FBI can uniquely contribute, we break down into five parts of our strategy, and I want to share that with you now.

The first thing we're trying to do is focus better on people. We mean this in two different respects. Focus better and deploy in a smarter way the people that already work for the FBI, and do a better job of stealing your talent to work at the FBI.

First, focusing better inside the FBI. The way in which the FBI has done its work for over a hundred years is physical focus. We ask ourselves: So where did "it" happen? Wherever "it" happened—whether that's a bank robbery, or a

fraud, or a drug deal, or a payoff to a corrupt official—that's where we do the work. The bank robbery happened in the Chicago suburbs, and so the Chicago Field Office will be responsible for that bank robbery. That makes good sense, and has made good sense for a century.

The challenge we face today, with a threat that comes at us at the speed of light from anywhere in the world, is that physical place isn't such a meaningful way to assign work any longer. Where did "it" happen when you're talking about an intrusion that's coming out of the other side of the globe, aimed at multiple enterprises either simultaneously or in sequence? That "it" is different than it ever was before.

So we've changed the way we're assigning work. We have now created a Cyber Threat Team model, where we assign the work in the FBI based on ability. Which field office has shown the chops to go after which slice of the threat we face?—that stack—and then assign it there.

This does two things for us. It allows us to put the work where the expertise is, and it creates a healthy competition inside the FBI. Everybody wants to be at the front of the list to own important threats that come at us. We assign, in the Cyber Threat Team model, a particular threat. Let's imagine it's a particular threat that comes at us from a certain nation-state actor set. We assign that to the Little Rock Division because the Little Rock Division has demonstrated tremendous ability against that threat.

But we're not fools about important physical manifestations, because that threat is going to touch particular enterprises around the country. And the CEOs of those enterprises and their boards are going to want to know, "Has the FBI been here to talk to us? And what's the nature of the investigation? And how is it going?" To make sure we accommodate that need, we're going to allow up to four other offices to help the team that is assigned the threat in Little Rock. If a company is hit in Indianapolis, and one is hit in Seattle, and one is hit in Miami, those field offices will also be able to assist in the investigation, but the lead will be in Little Rock. Then, the air traffic control for all of that to make sure we are not duplicating effort, or sending confusing messages, will come from the Cyber Division at headquarters.

We're trying this. We've been doing it now for about a year in a half. Seems to be working pretty well. It has set very, very healthy competition inside the FBI, which is good for us. But we're confronting a challenge and a way of doing work that we've never seen before, so we're eager to get feedback and then

iterate as make sense. We want to be humble enough to understand that just as our world has been transformed in our lifetimes, the way in which we do our work is being transformed. We have to be open to changing when it makes sense.

So the Cyber Threat Team model is at the core of our response. Also at the core of our response is a “fly team” of experts that we’ve put together that we call the CAT team—the Cyber Action Team. Just as in terrorism, we have pre-assigned pools of expertise that can jump on an airplane and go anywhere in the world in response to a terrorism threat, we’re building that, and have built, that same capability in respect to cyber, so that, if there is a particular intrusion—let’s say Sony in Los Angeles—we have the talent, the agent talent, the analyst talent, the technical talent, that’s already assigned to the Cyber Action Team that’s ready to deploy at a moment’s notice to literally fly to Los Angeles to support the investigation.

Second, I said we’re focusing on trying to steal people you’re trying to hire. To be able to staff those Cyber Action Teams and the Cyber Threat Team model in a good way, we need the talent. This is an enormous challenge for us, as for everybody in the government who’s sitting here, because we do not have the dough. We cannot compete on dough. The good news is we can compete on mission. We try to portray our private sector colleagues as engaged in a soulless, empty exercise, and then convince their talent to come do good for a living. We’re seeing how that’s going. We’ve met with limited success, so far. The good news is, the more we show people the nature of our mission and just how fun it is, how rewarding it is to have as your mission, as the FBI does, protecting the American people and upholding the Constitution of the United States, that attracts a lot of talent.

One of my children described to me what our problem is in recruiting. She said, “Dad, the problem is you’re the man.” I thought that was a compliment, so I said, “Thank you, I really appreciate that.” She said, “Dad, I don’t mean that in a good way. I mean you’re the ‘Man.’ Who would want to work for the ‘Man’?” I think she’s right. But I said to her, “You know, if people saw what this ‘Man’ and ‘Woman’ of the FBI was like, and what we do, and the challenges we face, I think they’d want to come work for us.”

I don’t want to share too much about our recruiting strategy, because our interests are not fully aligned, whether you work for the government or for a private entity in this room. But we are working much harder to make sure people understand what it might be like to work for this ‘Man’ and this

‘Woman’ and do this for a living. We’re working very hard inside the FBI, when we get that kind of talent in, to demonstrate more agility than we might naturally demonstrate when you’re 108 years old. There’s a challenge when you’re 108, you can calcify, and when a smart young kid comes in with a wonderful way of approaching a new problem, or approaching an old problem in a new way, you might try to crush that person’s spirit by saying, “No, we’ve never done it that way.”

We’re working very hard inside the FBI to be a whole lot cooler than you may think we are. We are not to bean bags and granola and a lot of white boards yet. But we’re working very hard at marching in that direction, so that when this talent comes into our organization we are open to having them make us better—in a way that connects us and them to our mission more closely.

We’re also doing things that we’ve never done before. We’re going to hire a senior-level data scientist, somebody who knows how to think deeply about the technical challenges we face together, who knows talent, who knows technology, who knows process. We’re looking to hire that person, bring them in at the shoulder of the assistant director of our Cyber Division.

Obviously, we’re trying to hire lots more cyber talent in our special agents. Here’s our challenge there: To have a cyber special agent, you need three buckets of attributes. You need integrity, which is non-negotiable. You need physicality. We’re going to give you a gun on behalf of the United States of America, you need to be able to run, fight, and shoot. So there’s a physicality required. And obviously there’s an intelligence we need for any special agent, but to be a cyber special agent, we need a highly sophisticated, specialized technical expertise.

Those three buckets are rare to find in the same human being in nature. We will find people of great integrity, who have technical talent, and can’t squeeze out more than two or three push-ups. We may find people of great technical talent who want to smoke weed on the way to the interview. So we’re staring at that, asking ourselves, “Are there other ways to find this talent, to equip this talent, to grow this talent?” One of the things we’re looking at is, if we find people of integrity and physicality and high intelligence, can we grow our own cyber expertise inside the organization? Or can we change the mix in cyber squads? A cyber squad today is normally eight special agents—gun-carrying people with integrity, physicality, high intelligence, and technical expertise. Ought the mix to be something else? A smaller group of this, and a group of

high-integrity people with technical expertise who are called cyber investigators?

We're leaving our mind open to the fact that we've never faced a transformation like the digital transformation, and so the FBI wanted to be open to being different in the way we think about our people. Lots more to come there.

The second thing we're trying to do: We're trying to shrink the world in two different ways. We're trying to shrink the world inside the government, so that all of us in the government who are responsible for the threat—some aspect of the threat, whether it's detection, whether it's response, whether it's mitigation—that we are working much closer together.

You may have read that the president recently issued Presidential Policy Directive 41, which is fabulous mostly for people outside of the government. What it does is it confirms the way in which we've been acting, but makes it clear to you all outside the government what the rules of the road are, so that you understand that the President has said, "Okay, Department of Justice, you will have the lead through the FBI and the National Cyber Investigative Joint Task Force in responding to threats and investigating threats. DHS, given your incredible capability with respect to threats, you will be response for threat mitigation. You will work to reduce impact, to mitigate vulnerabilities, and to identify and assess risk. And then Director of National Intelligence, because national intelligence is your job, you will be lead for our intelligence support, for making sure we have the best thinking pushed into both threat response and the mitigation efforts."

All that's important to say, but here's the most important message: it shouldn't matter to anybody outside the government who you call when you have a problem. Our job should be to figure out who should do what. And what Presidential Policy Directive 41 does is it clarifies for us exactly what the lanes of the road are that, frankly, we had evolved over the last several years on our own.

The second way in which we're trying to shrink the world is we're trying to forward deploy far more cyber agents and cyber analysts and have them sit with our foreign partners. Although we face a digital threat that's moving at the speed of light, the human connection between investigators shrinking the world, so that we can detect and deter and incapacitate bad guys better, is at the core of our strategy.

The third thing we're trying to do that I alluded to earlier: We're trying to impose costs. We think this behavior, this intrusion activity—whether it's by nations states or hacktivists or thugs and criminals—is deterrable. The first thing we want to do is we want to lock some people up, so that we send a message that it's not a freebie to kick in the door, metaphorically, of an American company or a private citizens and steal what matters to them.

If we can't lock people up, we want to call it out. We want to name and shame through indictments or sanctions or public relations campaigns, who is doing this and exactly what they're doing. About a year and a half ago, when the Department of Justice first indicted Chinese actors for stealing the enterprise of American corporations, stealing their innovation, a whole lot of people said, "Aw, you're just shouting to the wind. That seems like a silly empty gesture."

Looking back now after a year and a half, I don't think so. I think we have managed to send an important and chilling wind through that. Even though you may be sitting halfway around the world, it makes big difference to have your face on a "Wanted" poster. You might dream of going abroad yourself, you might dream of sending your kids to be educated and you want to go see those kids, and you know those people from the FBI, maybe they're not all that smart, but boy are they dogged. It took them 50 years to give up on D.B. Cooper, who jumped out of an airplane over Washington state. The long arm of the law is not only long, it's very, very patient. Trying to send that chill wind is the same reason we brought the indictments against the Iranian actors responsible for the wave of DDOS attacks in 2012 and 2013.

These kinds of activities have an impact on the individual actors, and they have an impact on governments, which we have seen. All this helps us grapple, step by step, towards a set of norms that leads to changed behavior—especially with the Chinese, where we have seen progress in the way in which we understand the framework. They are serious people with whom you can have a conversation to explain this framework. Nations states gather intelligence. They always have. We are trying to get information about other countries, other countries are trying to get information about us. We try to detect it, we try to thwart it, we try to stop it. But what nation-states must not do, cannot do and be part of the community of nations, is steal stuff to make money. That is outside the framework of acceptable nation-state activity—and we are making progress in having people understand that that's a framework that makes sense.

So whether through indictment or prosecution or sanction or publicity, we are working very hard to make people at keyboards feel our breath on their necks and try to change that behavior. We've got to get to a point where we can reach them as easily as they can reach us, and change behavior by that reach-out.

The fourth part of our strategy is: We must help our state and local partners be more effective in responding to all manner of complaints from their citizens about cyber crime that we can't get to. We simply cannot at the federal level handle every case. We have to help our state and local partners, with training and equipment and task forces, respond to the overwhelming cry from citizens for help.

There are people every day who are asked to wire me money in Nigeria. I am not the "president" of the Federal Bureau of Investigation; I am not in Nigeria; do not wire me money. But there's citizens everyday who are scammed in similar ways. We have to help our partners give them justice.

The last thing we need to do as part of our strategy should be obvious to you: we have to work better with the private sector to address these threats. All the information, all the evidence we need, sits in private hands in the United States—and that is a wonderful thing.

But it's an enormous challenge. We have discovered that the majority of our private partners do not turn to law enforcement when they face an intrusion. That is a very big problem. It's fine to turn to one of the many excellent private sector entities that will help with attribution and with remediation. That's good. But we have to get to a place where it's routine for people who are victimized to turn to us for assistance. We know your primary concern is getting back to normal when you run any kind of enterprise, especially a for-profit business. But we need to figure out who is behind that attack, and it is in your interest.

I know people sometimes say, "My interests are not aligned with the federal government. I need to get this thing over with and get on with my business." Sometimes people think that, even if it involves paying a ransomware ransom. I actually think our long term interests are the same. You're kidding yourself if you think that problem is going to go away and not return to re-victimize you. We must work together to defeat these threats.

So what's our strategy for getting you in the private sector to talk to us in the federal government more? We're going to hound you and explain to you over

and over and over again why it's in your interest, and why, as a matter of practice, we can work well together. We're going to convince you that we will not re-victimize you if you contact us and seek help. We will treat you, as we have for a century, as victims of crime. In working with all victims, our paramount goal is not to re-victimize this poor person, whether it's a victim of sexual assault, whether it's a robbery victim, or whether it's a company that has suffered an intrusion.

We also understand concerns about competitive advantage. We know that you are trying to get out from under the burden that has disrupted your operations, that has affected your supply chain, that risks affecting your reputation, that has confused and concerned your employees and your customers. We understand—and I in particular understand your concerns about liability, given that I was a general council for two different companies before coming back to this work, which is much better than any private sector work.

We have been at this a long time. And although we strive very hard to be humble, a true statement is that we have gotten good at it. We have gotten good at minimizing your disruption, minimizing disruption and pain to your employees, and protecting your privacy and your legitimate concerns about competitive advantage. We will not share your data about employees or operations. We will have adult conversations constantly with you to tell you what we're going to do with the information you give us, so that you can make risk-benefit decisions about what information to give us. We will not allow you to be blindsided, because we understand that if we do that, you're not going to talk to us anymore.

Your main question is: What do we need you to do? We need you to talk to us; to get to know us and understand what we're like and how we do this work. We need to make sure you understand how important it is to your competitive advantage to integrate the FBI into your risk-assessment plan. You spend a lot of time, no matter where your facility is, making sure the fire department has a basic understanding of the layout your building, so that in the event of a disaster they can save lives. I suggest you do the same with respect to your cyber threat and your risk-assessment plan.

We were able to respond within hours and help Sony investigate, attribute, and mitigate, because they had taken the time before the fire to get to know us. Not the details of their business plan, not any secrets of their proprietary information. We knew their CISO. We knew the basics about their network.

We knew who the key people were and what their key facilities and locations were.

Armed with that, in a situation with smoke all over the place, we were able to walk to the right place and get the right work done very, very quickly. I believe it is in your competitive advantage to make sure that we have that opportunity if a disaster hits your company. My suggestions to you is, if you are a CISO in a private enterprise and you do not know someone at every single FBI office where you have a significant presence, then you're not doing your job well enough. I want you to know the commander's intent, our people are waiting for those phone calls to build those relationships.

I liken this experience, this building trust with each other, to a journey we went through between the FBI and the CIA over the last 25 years.

There was long a law on the books that allowed criminal prosecutors and agents to protect the equities of the intelligence community in the event there was a criminal prosecution that touched on intelligence equities. The Classified Information Procedures Act was passed in the 1980s. When people passed it they thought, "Ah, we solved that problem, the friction between intelligence and law enforcement." Nonsense. It required trust-building, case by case, person by person, so that, to take this example, the CIA understood that the FBI would not burn their equities.

A great example of this occurred in the summer of 1998 with the attacks on the American embassies in Kenya and Tanzania. The investigation that followed that involved both Agency people and Federal Bureau of Investigation people. The way we did it was, the people went on searches together to do search warrants in east Africa, we sent people from both organizations, so if something was found that later was going to be useful in a criminal case, the FBI agents would testify about it. It was never going to be necessary to talk about the CIA's activities or its presence. That was consistent with the law, but it required trust-building to get there. Three years later, FBI personnel testified about those searches in a federal courtroom in Manhattan and the CIA didn't have to be involved, consistent with law and our discovery obligations.

Those kind of things built a culture of trust. It's not enough to say, these are the rules of the road in a statute or regulation; we have to demonstrate it person by person, case by case. You're going to see that from us, trying to

work with you place by place, enterprise by enterprise, incident by incident, to demonstrate we know how to do this and we will do it well.

A brief word, because I can't resist, to talk about encryption and the problem we call Going Dark. The issue with Going Dark—which is the term we use to describe our increasing inability with judicial authority to get access to information that sits on a device or that is traveling in real time—the challenge we face is that the advent of default ubiquitous strong encryption is making more and more of the room that we are charged to investigate dark.

There was always a corner of the room that was dark. Sophisticated actors could always get access, either for devices or for live comms, to encryption. What has happen just in the three years that I have been Director, post-Snowden, is that that dark corner of the room—especially through default encryption, especially through default encryption on devices—that shadow is spreading through more and more of the room.

The conversation we've been trying to have about this has dipped below public consciousness now. And that's fine, because what we want to do is collect information this year, so that next year we can have an adult conversation in this country.

Here's why I think it requires an adult conversation. Our nation's founders struck a bargain 240 ago. In our great country, we have a reasonable expectation of privacy in all of our private spaces—in our houses, in our cars, in our safe deposit boxes, in our devices. That is a very important part of being an American. The government cannot invade our private spaces without good reason—good reason that is reviewable in court.

But it also means that with good reason, the people of the United States, through judges and law enforcement, can invade our private spaces. That is the bargain that has been at the heart of ordered liberty in this country since its founding.

To take the most common example: If law enforcement has probable cause to believe that there's evidence of a crime in some space you control—whether that is your bedroom or your car, or your safe deposit box, or your laptop—they can go to a judge, make a showing of probable cause, and get a warrant that is consistent with the Fourth Amendment of the U.S. Constitution, and then go look through your stuff. They can search wherever the judge says

they can search: in your closet, in your dresser drawers, under your bed. They can take whatever the judge says they could take.

Even our memories are not absolutely private in the United States. Even our communications with our spouses, with our lawyers, with our clergy, with our medical professionals are not absolutely private. A judge in certain circumstances can order all of us to testify about what we saw or remembered or heard. There are really important constraints on that, but the general principle is one we've always accepted in the United States, and it's been at the core of our country. There is no such thing as absolute privacy in America. There is no place outside of judicial authority.

That allowed us to achieve two things we love dearly, privacy and security. Widespread default encryption changes that bargain. In my view, I think it actually shatters the bargain at the center of our country.

There's something seductive about the notation of absolute privacy—even when I hear it, I love it. I have an Instagram account with nine followers; they're all related to me, except for one serious boyfriend who may someday be related to me, I let him in at my daughter's request. I don't want anybody looking at those pictures. There's nothing inappropriate, but it's private to me. It is seductive when I hear someone say, "Absolute privacy is the paramount value. Our devices are designed to ensure that privacy is absolute in America." Then, I stop and I step back and I realize, "You know, we've actually never lived that way. That is a different way to live." It changes something at the center of our country that is really important. For our case, it effects our national security investigations and it effects our criminal investigations.

So we believe in the FBI that we have to talk about it. And our role is limited. The FBI's role is not to tell the American people how to live, how to govern themselves. Our role is simply to say, "Hey, those tools you were counting on us to use to find people in criminal cases, in national security cases? They are less and less effective every day because of this challenge."

It's also not the job of tech companies—as wonderful as they are, as great as their stuff is—to tell the American people how to live, how to govern themselves. Their job is to innovate and sell us great equipment. The American people should decide, "How do we want to live? How do we want to be governed? How do we want to govern ourselves?"

To have that conversation in a mature way, we need space and time and we need information. We need to understand in the FBI, how exactly is this affecting our work, and then share that with folks.

The challenge all of us face in having this conversation is that there is an intensity of emotion around the issue that makes it hard for people to avoid demonizing each other and to have a thoughtful exchange. Some like to say that we are trying to weaken encryption; that we are trying to build back doors into everybody's devices. To be clear, we believe the issue is not "strong" versus "weak" encryption. We love strong encryption in the FBI. It enables us to better protect people from thieves, fraudsters, hackers, spies, terrorists of all kinds. We love strong encryption.

But we also believe that absolute user control of data is not a requirement for strong encryption. A whole lot of organizations—including our own—issue personal electronic devices to employees, and still retain some control over those devices for security and business reasons. If those organizations—including my own—are served with a warrant, those organizations are able to access the information and comply with the warrant. The ability to do so by design does not require "weak" encryption. That's the reason why I often describe this as a really hard problem, but actually not a technical problem so much as a business-model problem. That doesn't make it any easier to solve, but I believe that's a fairer description of the challenge we face.

We believe in the FBI that we need a conversation. If at the end of the day the American people say, "You know what, we're okay with that portion of the room being dark. We're okay with"—to use one example—"the FBI, in the first 10 months of this year, getting 5,000 devices from state and local law enforcement and asked for assistance in opening them, and in 650 of those devices being unable to open those devices." That's criminals not caught, that's evidence not found, that's sentences that are far, far shorter for pedophiles and others because judges can't see the true scope of their activity.

We should not drift to a place where a wide swath of America is off limits to judicial authority. Tech companies last year wrote a letter to the president that I found, honestly, depressing, a little disheartening. Because it was a letter that wonderfully described the benefits of encryption, and as I read it paragraph after paragraph, I thought, "Yep, absolutely, absolutely. That's really, really important. That's really, really important." And the letter ended without any acknowledgement of the cost of widespread ubiquitous strong

encryption, especially by default. My reaction to that was, either they don't see the cost, or they're not being fair-minded about acknowledging the cost, which is going to make the conversation even harder. And that's a bit depressing.

We need a conversation that starts from a place where we recognize that there are no evil people in this conversation. We share the same values. We all care deeply about the same things—privacy on the one hand, security and safety on the other. We may weigh them differently. I may see the world more darkly than somebody who lives in sunny Silicon Valley. I may over-weight the dark side. But we have the same values. That should allow us to have a thoughtful conversation without demonizing anybody or trying to bumper-sticker anybody. I hope you will participate in that conversation, and that we can have it next year when we're not engaged, as you may have heard, in an election.

To finish, I don't know whether we can stay ahead of the cyber threat. I think talking about it that way actually shows hubris. We can hope to mitigate the threat, reduce the threat, send messages that change behavior. In the face of a threat unlike any we've seen before, we need enough humility to be agile, enough humility to take feedback from our partners to figure out how we can be better. We definitely need each other.

Thank you for being part of that. Thank you for the help you have already given to the FBI, for the advice, for the feedback, for the assistance. I hope you will continue that, and together we will make our world a safer place.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu