THE ASPEN INSTITUTE

ASPEN SECURITY FORUM: GLOBAL

THE COMPLEXITIES OF TODAY'S SECURITY CHALLENGES

Banqueting House, Whitehall
London SW1A 2ER, United Kingdom

Thursday, April 21, 2016

LIST OF PARTICIPANTS

CLARK KENT ERVIN
Director, Aspen Institute Homeland Security Program

BROOKE MASTERS
Companies Editor, Financial Times

JAMES COMEY
Director, Federal Bureau of Investigation
United States

* * * * *

THE COMPLEXITIES OF TODAY'S SECURITY CHALLENGES

MR. ERVIN: Well, good evening everyone and welcome to the debut of the Aspen Security Forum: Global. I am Clark Ervin, the former Inspector General of the United States Department of State and the Department of Homeland Security and the Founder and Executive Director of the Aspen Security Forum.

For a number of years now we have hosted in Aspen, Colorado each summer the top national security officials in the United States Government, eminent commentators and analysts from outside government and noted print and broadcast journalists to discuss and debate the issues of the day in the field of national security.

The Aspen Security Forum, we are pleased to say, has become the premier national security forum in the United States. With the success of the security forum in Aspen we are opening a new chapter in its development by debuting here in London a global version of the forum. Rather than featuring mostly American officials and policy experts with only a smattering of foreign officials and commentators, Aspen Security Forum: Global is intended to feature primarily non-American officials and commentators focusing on national security issues from a truly global perspective.

Over time we hope that the forum will help to drive the global conversation on security issues in the same way that the Aspen forum has come to drive the national conversation on these issues in the United States. We want to give special thanks to RUSI for its support of the forum here in London this week.

We cannot be more pleased to debut the forum here in London given the special relationship between the United States and the United Kingdom coincidentally underscored this very week by President Obama's visit. And we cannot be more pleased to begin the forum tonight with a conversation with one of America's most respected

and admired national security officials who no doubt has one of if not the hardest jobs in Washington doing everything possible to prevent another terror attack on American soil, Director of the FBI, James Comey.

Formally introducing Director Comey and moderating this session is Brooke Masters who is the Companies Editor of the *Financial Times.* Previously she was the Chief Regulation Correspondent for the *Times*, for the *Financial Times,* covering the UK Financial Services Authority and working with reporters around the world to cover both global financial regulation and white-collar crime.

Before the *Financial Times* she worked at both the *Wall Street Journal* and the *Washington Post*. She is a graduate of Harvard and the London School of Economics. Please join me in welcoming Brooke Masters in conversation with the Director of the FBI.

(Applause)

MS. MASTERS: Well, thanks for that lovely introduction. It's a tremendous pleasure for me to be doing this with Jim who, we've known each other I think almost 20 years now, when he was just a semi-important prosecutor in Virginia tackling terrorists who blew up the Khobar Towers. So this is a man who not only is the FBI director, he has a long history of tackling the worst and hardest securities cases basically that America has ever faced. So we're incredibly lucky.

There's so many things we could talk about but I think we have to start with Apple. I mean, the whole question of encryption and the Apple phone has been dominating the headlines around the world. And, you know, everybody -- I have an Apple phone, I'm sure you have -- or maybe you don't have an Apple phone but just about everybody in the audience does. So tell us about this. First of all, how the heck did you get into that phone?

MR. COMEY: They make fine products. I'm not here to pick on Apple or any other manufacturer. The -- well, I guess you know some of the story obviously. We brought the litigation, the Justice Department did, as part of our investigation into the attack in San Bernardino, and as I've said many times and I'll say it again, we brought the litigation because we thought it was very important to get into the phone to competently investigate a terrorist attack.

And I've said before, I thought we should have been fired if we didn't try to understand what was in a terrorist's phone. We had that -- terrorist is dead obviously, we had a search warrant. The county, which was the owner of the phone, consented, but we got to a place where Apple -- and I'm not questioning their motives, where Apple was not willing to cooperate to help us get into that. And so the Justice Department brought the litigation.

We were able to get into the phone because in an odd way the -- all the controversy and attention around the litigation I think stimulated a bit of a marketplace around the world which didn't exist before then for people to try and figure out could they break into an Apple 5C running iOS 9. And those details matter obviously because that's the phone that the terrorist left behind. And as a result of the stimulation while the litigation was ongoing we didn't stop trying to figure out whether we could get in. But somebody approached us from outside the government and said we think we've come up with a solution and we tested it and tested it and tested it and then we purchased it. And we were able to -- once we knew it would get us into the phone we were able to withdraw the litigation.

And in my view that's a good reason, good thing for a couple of different reasons. First, we got into the phone, which is a very important part of the investigation. And second, litigation is not a great place to resolve hard values questions that implicate all kinds of things that all of us care about. And so it was

a -- and the emotion and the pain around that case was a bit of a distraction, frankly, from a more important conversation that I think we have to have. And so in that sense it's also good that the litigation was no longer necessary.

But I hope it doesn't lead people to stop talking about it. And from your question it's clear to me people aren't going to stop, they shouldn't. They should continue to talk about it because we have a problem where all of us share a set of values that are in conflict and we have to figure out how to resolve privacy and security on the Internet and on our devices with public safety, and they're crashing into each other in terrorism cases and really all the work the FBI does. And I don't know exactly what the answer is but we need an answer and we can't let ourselves drift. So I hope the conversation will continue.

So that's the story of how we ended up getting into the phone. And the investigation obviously continues. But this will be a feature of our work. There will be other litigation, I'm sure. But it will be a feature of our work increasingly over the months and years to come.

MS. MASTERS: So how much did you pay for the software?

MR. COMEY: A lot.

MS. MASTERS: Really?

MR. COMEY: Let's see, more than I will make in the remainder of this job, which is 7 years and 4 months, for sure.

MS. MASTERS: Wow.

MR. COMEY: And so it's a -- but it was, in my view, worth it because it's a tool that helps us with a 5C running iOS 9 which is a bit of a corner case increasingly

as the devices develop and move on to the 6 and 6S and what not. And iOSes change. But I think it's very, very important that we get into the -- that device.

MS. MASTERS: Are you crowdsourcing the solution to say an Apple 6 and a 6S?

MR. COMEY: No, we --

MS. MASTERS: Not yet.

MR. COMEY: No, we have not. And that would -- to my mind that would be a regrettable place to be --

MS. MASTERS: Really.

MR. COMEY: -- where, for two reasons, first it just doesn't seem to make a lot of sense to me that the way we're going to resolve a conflict that implicates values and our hardest work is that the government is going to try and pay lots of money to get people to break into devices and find vulnerabilities. That seems like a backwards way to approach it.

And second, it's not scalable. That is this problem is overwhelmingly affecting law enforcement. And so there are 18,000 law enforcement agencies in the United States, all of whom are going to find this problem affecting their work. And so us buying a tool for a 5C iOS 9 is not scalable. And nor could all of those departments afford to pay what we had to invest in this investigation. So I'm hoping that we can somehow get to a place where we have a sensible solution or set of solutions that doesn't involve hacking and doesn't involve spending tons of money in a way that's unscalable.

MS. MASTERS: Do you see a historical parallel that people could look to that -- have we had this problem before in any meaningful way?

MR. COMEY: I think we have all kinds of problems like this that we resolved in the past. The one

that was brought to my mind most recently was 20 years ago, which seems like a lifetime ago, banks were basically saying the world was going to end because the United States government and other governments were going to require them to scrutinize customer transactions and report those that were suspicious. There was lot of hue and cry at the time a generation ago about privacy and how would that work and how would we still be able to operate and what a terrible thing. It worked out just fine.

People were able to continue to supply banking services that were prudent and it actually made for better business for the banks. We dealt with this in the telecommunications context when Congress mandated that telecommunications companies in the United States provide access to allow court orders to be complied with. And at the time again there was a lot of concern how would that work, how would that affect our business. And it was able to be worked out.

And so I don't know what the future looks like, I'm keen to make sure that people don't think the FBI should say what the answer is here. I think our job is to say the tools you count on us to use in criminal cases, in terrorism cases throughout our work are less effective than you thought they were because of this problem and we don't think democracy should drift. But we also don't think the FBI should say here is how you should govern yourselves any more than companies should say that, right?

Apple is a fine company, the FBI is a great organization, neither of it should tell people how we should govern ourselves. This is a fundamental question about how we want to be. So I think our job is to say here is how it's affecting our work. And maybe at the end of the day the people in the United States say, okay, we're okay living with that diminution and your tools, you will find other ways, or maybe people conclude it's just too hard technically, which I don't buy, or maybe people conclude we ought to find some other way to see if we can optimize both of these values, but it's a conversation we must have. And I'm an optimist and so I hope we can have

it not just on Twitter, not just on bumper stickers and we could have it without anybody needing to hate anybody else.

I was speaking to a group of students recently and I said I hope we start this discussion from this place. I could be wrong. I could reason wrong, I could perceive wrong. I could be wrong. I hope you could be too. And if we start there we can have a better conversation. So I'm working very hard to make sure people understand Apple is not a demon, I sure as heck know the FBI is not a demon. We have a problem with a shared set of values that we have to sort out.

MS. MASTERS: Shall we shift slightly into cybersecurity?

MR. COMEY: Sure.

MS. MASTERS: And I mean part of -- this is actually sort of a natural evolution in that cyber terrorism and the use of the Internet to recruit as well as to conduct terrorist attacks is obviously very much on people's minds. I mean, how effective is the FBI against terrorism? How effective are institutions here in the UK? And how well do you guys work together?

MR. COMEY: Well, I think the counterterrorism work that we do in the United States, which is not just the FBI, there is a whole lot of other people that work on it, is very, very good. I never want to be satisfied that it's good enough. One thing that's for sure is that our country and the Brits as well as others took the pain of 3,000 people being murdered and responded to that by changing the way we are organized, we are resourced, we're deployed, we're trained. And we invested tens of billions of dollars to build a better counterterrorism capability. And I can only speak for the United States, which I know best. But the taxpayers' money bought something, which is a highly effective counterterrorism regime. And I think that's true in the UK as well.

But we're not perfect. I mean, we face a threat that is increasingly hard to see, sometimes impossible to see when encryption comes into play, that is changing and moving at tremendous speed. And we live, as the citizens of the UK do, in a country that's big and free and open and diverse with lots of movement, all of which makes our life challenging. So we are very good. We can never quite be good enough, frankly, given the nature of the threat.

The cooperation that we have in the US with our counterparts in the UK is simply extraordinary. It is -- it couldn't be more productive, it couldn't be closer frankly. And that makes good sense because the threat -- we actually don't conceive the threat as a threat in America and a threat in the UK, we see it as the same threat because we're always just a flight away from each other for terrorists as well a for good people. And so we are knit together very, very closely. And I think we're both very good. But again, you never want to say you're good enough given the nature of the challenge.

MS. MASTERS: Do you think something like what just happened in Brussels can happen here again soon?

MR. COMEY: Sure. Yes. It can happen anywhere. There are -- is probably a sliding scale of risk associated with that in different places. I think the risk is lower in the US for a variety of reasons but we stare at what happened in Brussels and imagine it as our future that we have to work against, that it could be that the threat they're facing on the continent and increasingly here in the UK is the threat that we could face 2 years from now. And we talk a lot, plan a lot and work a lot against that possibility.

MS. MASTERS: How has this threat changed in the 2-1/2 years that you've been the FBI director.

MR. COMEY: Fundamentally actually the shift from your parents' Al-Qaeda to the so-called Islamic State has all happened in my tenure. The Al-Qaeda model, so

long time ago, say 2013, was focused on sophisticated long-planned attacks with extensive surveillance, carefully vetted operatives aimed at the symbols of the West. So for the United States, Washington, New York, airplane base, national landmark focused. And in a way we had come since 9/11 to rely on Al-Qaeda's culture, which was they must do the big thing.

If they just shot a bunch of people in a restaurant, that would be a loss of face for them and a confession of weakness in a way. Maybe sometimes we didn't verbalize that but we actually relied upon that without knowing it maybe. That was the Al-Qaeda model. That changed starting really in early 2014 and accelerating 2014 with the growth of ISIL, and their change was fundamental in a number of ways.

First, their mission was simply to attract people to their so-called caliphate or kill. Come or kill was the message to the United States, come or kill. Kill anybody, kill anybody anyway, with a car, with a knife, with an axe, with a gun, it doesn't matter. If you can kill somebody in uniform, best of all. But just kill anybody in the name of the Islamic State if you can't come and become a soldier of the caliphate, that's the first big change.

The second is the way in which they communicated that message made Al-Qaeda look like your parents' Al-Qaeda. They crowdsourced terrorism by pushing out that twin-prong message, especially on Twitter, in a very, very slick way. And the message they were sending was one of ultimate meaning that to the people in this auditorium would seem stupid but that resonated with troubled unmoored souls and we got our share of them in the United States. And the message would appear on their hip or buzzing in their pocket on Twitter 24 hours a day, come or kill, find meaning, come or kill, find meaning. And then to make it more complicated, they would find people who are interested in traveling or killing on their behalf and move them off the open platform of Twitter if they were really live ones and willing to commit acts of violence,

they would move them to an encrypted app, a mobile messaging app encrypted end to end.

And so they're crowdsourcing terrorism, broadcasting a message of meaning 24 hours a day to troubles souls. And when they get one that's likely to act, that needle we've been looking for becomes invisible. That's a totally different model than we've ever seen before. And so they started investing in this 2014. We saw the payoff on this for them in the spring of last year, 2015, in the United States where 9 months of this relentless broadcasting of slick messaging all of a sudden we had people all over the United States moving quickly along the spectrum from consuming to acting.

And we had to lock up, to disrupt plots, dozens of people. And they were people that Al-Qaeda would never have used as an operative, drug users, pedophiles, people with criminal records, mentally ill people. People who were resonating with this message were people Al-Qaeda would never have used because Al-Qaeda would carefully vet their operatives. And so to disrupt we had to find and take them off the deck very, very quickly. So that was the payoff we saw. And we also saw a lot of travelers trying to leave the United States nothing like what the UK or Europe have seen, but a significant following to this. It's been interesting. The last 6 to 9 months the number of travelers, attempted travelers from the states that we have seen has been steadily coming down.

MS. MASTERS: Why?

MR. COMEY: I don't want to fall in love with that, those facts, because it could be that we're missing something, that they're going another way or they're going to Libya. But I don't think so. I think something has changed. And a number of possibilities, it could be the fad that is this death cult of ISIL has lost its power with audience in the United States. It could be the fact that a whole lot of people are getting a decade or more in federal prison for traveling or attempting to travel is making a difference. It also could be that parents and

siblings and teachers and religious leaders are more conscious of the risk in intervening with troubled people or some combination of all, could also be people have finally dawned on them that their so-called caliphate is hell on earth, especially for women and that -- or maybe some combination of all those things is driving down the attraction. I don't know.

But it's been going on long enough, almost 9 months now, the numbers have been down, that it's a trend that I think I'm comfortable talking about. We still see a slow but steady increase in the number of cases in the United States which we have in every field office of people where they're somewhere on the spectrum from consuming to acting. We're seeing fewer that were disrupting towards the acting end of it but so is a whole lot of people who are consuming this poison again in private in a way that's very hard for us to see. And so it's a -- remains a huge feature of our work.

MS. MASTERS: How do you deal with them when they're moving into that encrypted phase? Because presumably up to that moment you can kind of see what's going on.

MR. COMEY: How do we deal with them once they move into the encrypted phase?

MS. MASTERS: Yeah.

MR. COMEY: With great urgency because then we don't know are they going to kill people in a restaurant tomorrow or is it 3 weeks from now. And so we have to get much more aggressive in trying to introduce sources to them or undercovers. And it's a very resource-intensive effort, but that's how we react. If they disappear then we try -- obviously we try and use physical surveillance to keep an eye on them. But really in our work unless you've done our work, sometimes it's hard for folks to appreciate this, there is no substitute for us being able with lawful authority to get the content of their communication because metadata which will tell us where

they are, or physical surveillance which will tell us where they are doesn't tell us so who is involved in this, do they have weapons, do they have bombs, and is this about to go. And so we end up having to err on the side of acting very early in these cases because we're so worried about what we don't know.

MS. MASTERS: So in a situation like that, does the fact that something like WhatsApp is now encrypting everything -- I mean, I assume that must be of great concern to you at this point.

MR. COMEY: Huge concern. I mean, that's a living example as the Apple case was in San Bernardino of the problem we call going dark. All right. There are over a billion users of WhatsApp and there are a significant number of terrorists and criminals who use WhatsApp and that's a problem. It's wonderful for human rights activist or people who are in despotic regimes who want protection, all that makes good sense to me, but it comes with this significant cost. And that's the conversation I keep talking about we got to sort out. So how do we think about that? And is there a way to address the cost and trying to optimize the benefits.

MS. MASTERS: In this country obviously the Snowden revelations have made people very suspicious of government surveillance. How do you address the need obviously to follow these people and but at the same time reassure people that if you did get power to get into people's encrypted messages that it wouldn't get abused?

MR. COMEY: Well, that's where people need to demand the details, right? Again, the States is the world that I know best, there is a very complex regime of judicial approval, predication requirement and oversight in the United States for the FBI to conduct any kind of electronic surveillance. It is really hard for us to get permission to listen to someone's phone calls or to collect their online communications. That's as it should be. But that -- there is a -- there is an angel in those details which is sometimes I think people think, well, the

FBI will just go listen to my phone. Yes, if we're able to go to a federal judge and make a showing of probable cause that you are a foreign terrorist, a spy or someone engaged in serious criminal activity and you're using that device to do that. That's what we have to show based on sworn affidavits. As I said, that's hard, but that's as it should be. And so I think folks have to take the time to understand.

So how is it that the FBI conducts electronic surveillance and why do they do it. I think sometimes, again, that's where I talk about we can't have this conversation on Twitter because it requires people taking a deep breath and saying, so what are we talking about here and why is the FBI so worried about this. It's easier to try and paint the FBI or the FBI director as an enemy of privacy. I love privacy, I'm a huge fan of strong encryption. But we also have a responsibility to keep people safe. And there are really bad people in this world. And to keep people safe with appropriate oversight and predication we need to be able to know what they're talking about. That's what I'm so worried about. And I think that's why we have to continue to talk about this.

MS. MASTERS: On the other side of this one, electronic debate, is this idea of people using the Internet not just to recruit physical terrorists but to commit acts or either theft or terrorism. And there was that dam that somebody tried to break into. So how much help that is that situation right now, I mean how good are the real cyber terrorists and how worried are you about them?

MR. COMEY: There really isn't what I would -- what I would think you meant by cyberterrorism in any significant way in our world yet. By that I mean people using access that they obtain through the Internet to inflict physical damage or to destroy systems or to try and harm people. The terrorist world primarily hasn't evolved to that point. They're using the Internet to recruit, to communicate, to proselytize, to threaten, but they haven't yet gotten to the place where they are going

to try and use it to damage. Logic would tell me that's inevitable. We've worked really, really hard in the United States to make it difficult for a terrorist to physically come into the United States. Well, if terrorists can enter as a photon at the speed of light literally in ways that would be, are very difficult for us to spot and stop and so they will get there eventually.

The cyber threat to my mind primarily is in the espionage space and criminal. We've all connected our whole life to the Internet, and because it's where we bank and our children play and it's where our infrastructure is, anybody who wants to hurt our kids or steal our money or damage our infrastructure, that's where they go. And so cyber investigations and digital investigations are part of everything the FBI does today because that's where our lives are.

But again, the terrorist threat has not evolved to that point. And I hope a lot of terrorists aren't watching the Aspen Institute live feed, but it's a -- that's a snapshot of where we are right now.

MS. MASTERS: On the criminal side, you know, how much of it is people who are beyond the reach of the FBI at least easily because they're outside the U.S. doing this. You have the sense that they're the Russian and Middle East and Eastern European gangs trying to break into bank accounts, is that a stereotype or is that actually really what's happening?

MR. COMEY: No, that's a big feature of it, but it's obviously much more than that. The challenge of crimes committed through the Internet is normal conceptions of space and time and location that actually without us even realizing it normally governor work or explode it. Normally the FBI does work based on where it happened, right. Bank robberies in Chicago, so Chicago will work that bank robbery. Well, a cyber intrusion, where did it happen. The physical manifestation of it where the company is located that gets hacked may not be all that meaningful, and the criminal may be anywhere in

the world because the threat is moving at the speed of light, and so what's happened is, the criminal and the spies have shrunk the world. So they can be in a former Soviet Bloc country in their basement attacking a company in Indianapolis or attacking something in Australia or in London or doing all of it at the same time.

And so we have to think about it very differently, and part of our strategy, with our British colleagues especially, is shrink the world back, because we face a situation now where the bad people think it's a freebie to kick in the doors electronically of an American company or an American individual or the same in the UK and steal what matters most to them. It's a freebie, because I'm in my pajamas in my basement half way around the world. So we really have to get to a place where those actors feel us behind them. Metaphorically they feel our breath on their neck, because that's the only way we will change behavior. Fear will change behavior.

So we work very, very hard to shrink the world to catch criminals all around the world. We work very hard to send messages to nation states that are sponsoring this kind of activity that we see you, we know what you're doing, we're going to call it out where we can. We're going to charge your people who are engaged in pure criminal activity with crimes. And life is long, we have great patience and the world is pretty small.

So people say you will never get these actors that you indicted half way around the world, don't say never. We have many flaws in the FBI but we are dogged. And people like to go on vacation.

MS. MASTERS: Can you give us a couple of good examples of where you feel like you've had successes in making people feel you're the long arm of the law?

MR. COMEY: I think a number of Russian hackers, Romanian-based hackers have felt us, a number of them are in jail now in the United States because they've felt us. We had one go on to another country in the EU on his

honeymoon, and because we're so closely connected to each other addressing this in the EU as he was departing to go back to Russia, his spouse boarded the plane, he did not board the plane, and now he feels that actually, probably that literal breath on his back. And I think by naming the Chinese hackers who were not engaged in traditional state espionage but were stealing for private account, I think by indicting them and publicizing their pictures I think we sent an important message, and also helped the community of nations kind of grope -- grapple with and find a set of norms that will guide our behavior.

MS. MASTERS: How effective are your cooperation efforts with say Eastern European and the former Soviet Bloc countries, China?

MR. COMEY: Probably different across those, very, very strong with the former, sort of the Eastern European nations, because they don't want criminals, right. The Romanians are a great partner because there is a generation of folks of criminals that they've dealt with who got technical education under Ceausescu and then decided to use that to become criminals thereafter.

So they are very good partners, they want to share ideas, training, information with us so that they can lock up criminals who are committing crimes from their homeland. It's different with the Chinese, I mean it's a work in progress, I guess is the best way to describe it. I think we've made good progress in understanding the framework that we all should live with, and that's happened over the last 6 to 9 months, that is this understanding that states engage in intelligence collection. They have since they were states.

States do not and should not harbor, sponsor, benefit from purely criminal activities designed solely to help private enterprise in that country. And that framework, the agreement between President Obama and President Xi acknowledges that framework. And so that's a major step forward. And we're working to understand. How is the framework being applied, it's probably too early to

say, but that's light years ahead of where we were 2 years ago.

MS. MASTERS: Do you think in the end the Chinese end up being partners in this? I mean, the PLA is famously considered a source of cyber espionage and other nasty things.

MR. COMEY: I don't know is the answer. I hope that we become partners. Once we understand the framework, that this isn't about what states do to collect intelligence for national purposes, that we can all agree that nobody should be stealing the design for a particular product so that product can be manufactured in the country where it was stolen from and that we can become partners in investigating and stopping that which is purely criminal behavior. And I was just in China 3 weeks or so, and the conversations embraced that framework. And at least we're saying to each other the right things about our desire to stop this kind of activity. But again time will tell.

MS. MASTERS: Do you think the fact that so many crimes can be committed through cyber means now is affecting the kind of violent crimes you see? Are people shifting from robbing people on the streets to trying to break into their, you know, Kmart's computer files?

MR. COMEY: That's a good question. I think the people who would be grabbing people on the street and socking them over the head are too dumb to be the cyber criminals who are engaged in point-of-sale frauds. I think it's fraudsters have found other ways and easier ways to commit their fraud offenses. The street criminals are, remain street criminals, and I really don't see the two groups overlapping much.

MS. MASTERS: So it's more like the guys who might have been like selling those fake driveway things by walking to a door and now on the -- on computers? Those kind of people?

MR. COMEY: I guess so, yeah. But the -- look, it requires a nominal level of intelligence and technical ability. And so I think it's attracting the people who used to send you letters. People used to get letters from me from Nigeria saying I needed them to wire me money, now they get e-mails from me in Nigeria asking you to wire me money. I'm not in Nigeria, I don't need your money, do not wire me anything anywhere. And so they've simply shifted the vector they use to the place where we all live, which is online.

MS. MASTERS: From this side of the Atlantic, it seems like the U.S. is having a bit of a uptick in violent crime, partly I think we're all sort of fascinated with the gun culture, but also there's been this discussion about whether the breakdown of relationships between minorities communities and the police is having an impact as well, what do you think is going on?

MR. COMEY: I don't know, but something worrisome is going on. And I started seeing the data. At the middle of last year there was a spike in homicide occurring primarily in minority communities, so people of color being killed in most of the nation's 50 largest cities. And it started at the end of 2014 beginning of 2015. So the calendar was interesting, striking to see an increase in homicide all about at the same time.

And then the map was also confusing because the 37 or so cities that we're seeing this spike in homicide, which turned out to be the same at the end of the year, 37, I think it is, cites experienced a jump in homicide were around the country, but interspersed among them were other cities that were not or seeing a decrease.

And so I looked at that map and said, so what explains that calendar and that map, what does Sacramento have in common with Milwaukee, what does Orlando have in common with Dallas but not Houston and not Phoenix and so what's going on here. And I was hearing privately from police officers around the country, both leadership and line officers that their behavior was changing in some

way. And so I don't know whether that's what's going on. But I talked about this last fall because there is a danger in the United States because it's happening in those neighborhoods to those people that we could mentally drive around it and I refuse to let that happen, at least from my place. Something is going on. And a lot of people said to me, well, it's heroin. Well, in one part of the country. But methamphetamine is the problem in the other part of the country. Well, it's a gang. But that's a different gang in this city and that city. So the hard thing is staring at the map and the calendar, what is happening.

And a plausible explanation, I don't know whether this is true, is that an accumulation of marginal decisions, almost unconscious by police officers. Good policing involves getting out of your vehicle at midnight and walking up to a group of guys standing on a street corner and saying, hey, what are you guys doing, you live around here, and having a conversation, respectful, appropriate, up close. And what could be happening is that an accumulation of thousands of decisions to stay in your car and not be a part of something controversial is changing behavior, and then that behavior change is changing crime, I don't know. But we continue to see that effect. And so we'll continue to talk about it.

I've urged academics get into this, see if you can analyze this and see what might be happening here, because here is what we got to get to. Police leaders need to insist that their people engage in appropriate, respectful, transparent, up close policing. And communities, especially communities of color need to understand that's the policing that saves lives and they need to demand it from their police departments and also embrace that kind of policing. And I think if we can get to that place, whether or not that's the cause of this, we'll all be better off.

So there's something going on that still goes on that I think we've got to continue to talk about.

MS. MASTERS: Interesting.

MR. COMEY: And we have some guns in the United States.

MS. MASTERS: Just a few.

MR. COMEY: Yeah.

MS. MASTERS: Do you think that ever changes?

MR. COMEY: No, no. It's a part as you -- you know, because you're American, it's part of our the unpleasantness from 240 years ago, the -- embedded in part into our culture, the notion that -- and embedded into our constitution that the private ownership of firearms is at the heart of our legal culture or constitutional culture. And, you know, I mean, there is three hundred and some million guns in the United States. And guns don't have an expiration date on them, so there will be a lot of guns in the United States for the rest of my life and my children's lives.

MS. MASTERS: One subject that's very parochial for us but I think very much on people's minds is the question of whether Britain should leave the EU and obviously that's for people here to decide. But do you have a view whether if Britain decided to go it alone it would affect your ability to work with us or your ability to work with EU and for everybody to work together to stop international gangs, terrorism all of that?

MR. COMEY: I'm going to totally dodge that question.

MS. MASTERS: While we're on the subject of questions --

MR. COMEY: I think the President is coming, he'll cover that, I'm sure.

(Laughter)

MR. COMEY: But, as you know, the Bureau tries to stay out of all things that might be political, so no comment, Brooke.

MS. MASTERS: So while we are on the subject of things you want to dodge, Hillary's e-mails.

(Laughter)

MS. MASTERS: When --

MR. COMEY: Double dodge.

(Laughter)

MS. MASTERS: Yeah. Do you have any -- is there any timetable when we might get an answer on where this thing goes?

MR. COMEY: Yeah, there's no timetable on any investigation. But -- somebody asked me in the States about whether I -- I think the question was is the Democratic National Convention a -- I forgot what the question was -- a hard stop for you or is that a key day for you, are you doing this investigation aimed at it? And I said, no, right. We aspire to do all our investigations in two ways, well and promptly. Especially investigations that are of great interest to the public we want to do them promptly. San Bernardino, right, feel great pressure to do that well and do it promptly because people care about it. I get that people care about this investigation and so we're working very hard to ensure it's done well and promptly. But as between the two if we have to choose, we will do it well.

But again, we aspire to do it well and promptly and I -- I'm personally close to this investigation because I want to ensure that we have the resources, the people the technology and the space to do those things and to do it in the way I hope we do all our work which is competently, honestly and independently. And I'm

confident that it's being done that way. Yeah. So no comment.

(Laughter)

MS. MASTERS: Well, on that note I think we'll turn to the audience and see if --

MR. COMEY: Okay.

MS. MASTERS: -- I have failed to hit some topic that they are dying to hear about.

MR. COMEY: Okay.

MS. MASTERS: Can we start -- I know the director has some people who are part of his traveling press corps. Can we try starting with people who don't usually get to ask him questions? So the first couple at least let's do regular audience. Has somebody got a burning question they'd like to ask Mr. Comey? There are microphones going up and down, shall we go, there's a middle of the room there that went up very quickly.

MR. GARLAND: Hi, it's Duncan Garland. Can I ask the director whether he feels that the French and Belgian security services could have done a better job over the last 18 months and whether he would like the UK security services to do anything differently?

MR. COMEY: Whether I would advise the UK services do anything differently? Yeah, the honest answer is both I don't know and I'm sure there are things they could have done differently and that's always true looking back through it -- through the lens of a tragedy. And so I know that one of the things that we as a community of nations dealing with a terrorism threat are trying to do better is share information with each other, share it more quickly. I think we have in the wake of the Brussels attacks we are working better together today than maybe a year or two ago.

And so I -- the reason I said I don't know is I think it will take a whole lot more benefit of time in hind sight and a richer understanding of exactly what happened and what the services knew, to answer that one. And the reason I said I'm sure is in every case, there's never been a big thing happen in the United States that we didn't look back and said I wish we'd done this or done that.

With respect to the British counterparts, I don't have a suggestion because they're extraordinarily good. And I think about it the way that I just described it, which know they're good but also not fall in love with their view of things or their view of facts. So I don't have a suggestion. The overall suggestion I think for -- that I'd have for the community of nations is we have to make sure that we are connecting to each other.

Let me back up and say this again. After 9/11 what made the United States safer is we invested in knitting together everybody who might have information or capability with respect to the terrorism threat, and that was painful and required regulatory change, legal change, and most importantly of all, cultural change.

And that's a journey that was spurred, as I said earlier, by the death of 3,000 people in my country. And so I do think there is progress that could be made among the community of nations, obviously including the EU, to travel some of that road that we've traveled since September 11th to knit together in a better way. That's probably my overarching piece of feedback.

MS. MASTERS: Next.

MR. COMEY: Your call -- I'm not in charge of that.

MR. COMEY: Yeah. I'll do it. How about we do over here?

MR. THOMAS: All right so thanks very much. My name is Crawford Thomas. I work for the Clydesdale Bank. I've only actually just gone into the financial sector. I've 20 years working in intelligence within the British Army. And so it's all new. And I just -- what we're looking at the moment is obviously the reporting of any form of hacking or DDoS sort of attacks against the financial sector. How do you think that that sort of reporting of fraud should be looked at within the law enforcement as opposed to paying ransomware or malware coming into these organizations?

And I have a second question, do you see Anonymous in these hacktivists in the world today? Do you see their actions against terrorists in terms of bringing down their websites helping or hindering?

MR. COMEY: Yeah, the second piece first. I don't know enough at this point to answer that question. I don't have a high confidence read on that. And I'm not a fan of freelancers of any kind. And so that's probably the best way to answer that.

With respect to the first piece, I think I understand the question, I strongly encourage people who think they are victims of any kind of cyber attack, including ransomware which is spreading like a terrible virus in the United States and I think spreading around the world, to contact law enforcement. My advice for companies especially is you ought to know us before the way you know the fire department. All right, most companies, the fire department -- basically understands their physical plant and if there's an emergency who are the people to talk to and what are the protocols. Every responsible institution whether its public or -- I mean non-profit or profit institution ought to have a similar relationship with the people responsible for investigating cyber intrusions because speed matters tremendously.

Sony was a terrible attack. But one of the things we were able to do very quickly because we knew Sony, we knew their people, we had a familiarity that was

appropriate, able to respond very, very quickly. So my urging to folks is, you ought to build that relationship early and have it discussed. So what information are you going to need if we're attacked because what people will find out is -- a lot of -- I used to be a general counsel, and general counsels are conservative weenies, and a lot of those conservative weenies will say we can't, we don't -- the government wants too much. Interesting conversation, because we don't want much, we don't want content we want zeroes and ones. We want indicators, right, of attack and vector. And to come to the ransomware in particular my ask would be please don't pay a ransom without talking to law enforcement.

Now, we have a problem in the United States, an entity was locked up with a ransomware, not only paid the ransom, for reasons that aren't clear to me, publicized it. Well, you know what happens then, right, lots and lots of other places in that same industry are getting hit. So I would urge people to build the relationship in advance and then when something like that happens please talk to us before you do that because there may be answers that you haven't thought of to dealing with that. Then I'll stop this, but basic cyber hygiene, patching and having an affective back up that is not connected to your network is critical to dealing with this ransomware.

These punks will not have power over you if you have patched and you have an ability to recover to a backup. Right, they have nothing to demand of you -- because you're going to operate your business by moving over to your backup. Sophisticated companies get that, but a lot of smaller companies haven't focused on it. Sorry for the long answer.

MS. MASTERS: In the middle here.

SPEAKER: First of all, thank you very much for the interesting conversation today. So my question is about Syria, I just wanted to ask your view on the situation of the people who are coming to Europe. So what's your view on this situation and if this potentially

can bring additional risks to the European countries and how this can be tackled? Thank you.

MR. COMEY: Because my business is security I'll answer it through the security lens, and it's obviously very, very important humanitarian policy and political lenses that I'm not qualified to talk about. It obviously presents a security risk whenever you have a large flow of people who maybe undocumented or flowing in such numbers that they're difficult to understand who they are and what their story is, it poses a risk. There's no doubt about that.

And so to my mind the answer is what's already going on which is countries together devising the structures and the processes to get a better picture of the people and share everything that might be known about a particular person and their documents and to touch all potential sources of information about that person and the risk they may pose.

And this is an enormous undertaking. Again, it's something the United States government has devoted huge resources to over the last 15 years but we've never dealt with the kind of flow of a million or more people all in the same summer. And so I don't mean to sound glib, it's not an easy thing to deal with, but I know there's a lot of work going on now to again knit together the people who may be sources of information so you can know better as best you possibly can who these folks are and what risks they may pose to mitigate the risk. That's how I think about it.

MS. MASTERS: Okay. We got time for two more. Haven't done anybody in the way back, so how about right there.

MR. BUTLER: Thank you, Director. My name is Ed Butler (phonetic). I'm in the terrorism reinsurance market. I wonder if you could comment on the threat of dirty chemical and dirty radiological devices being used by terrorists.

MR. COMEY: A very narrow depot, it's -- there's a part of the FBI called the Weapons of Mass Destruction Directorate and I call them the people who don't sleep at night so I can sleep at night. It is something we worry about, watch for, have put in place, again through our partners around the world, trip wires to try and understand whether terrorists are endeavoring to get chem, radiological nuclear devices for any purpose. And so it is a threat that lives with us every day. And I don't assess the threat -- I guess I would stop there, it's something we worry about every day because it is a very, very narrow hole. But given the consequences it's something we have to invest the resources in that we do.

MS. MASTERS: One more. So I think this side of the room hasn't gotten to talk very much, so back there maybe.

SERGILL: My name is Sergill (phonetic). I'm from Brazil. And after the Paris attacks there was a threat to Brazil recently confirmed by the Brazilian Intelligence Agency. And I would like to ask how in danger you think we are?

MR. COMEY: In Brazil?

SERGILL: Yeah, the Olympics is like in 3 months --

MR. COMEY: In connection with the Olympics?

SERGILL: Yeah.

MR. COMEY: Yeah. I don't know what's been confirmed, so I'm going to stay away from particulars. It's something that we in the United States intelligence community try to look for and watch for so if we see any indication of a threat that's either in Brazil or aimed at Brazil we share it. We've built very close relationships even despite -- and this is true around the world, even though our political tensions, the security services,

given the nature of our business, which is keeping innocent people from being harmed, tend to have consistently good relationships. So we've long had good relationships with our Brazilian counterparts. And so we are being very, very attentive to whether there is any threat information.

I think the Brazilians are putting lots of resources against it. They've engaged I know our British colleagues and people in the United States for training and support. The challenge of any event of that size and scope is the physical scale and the number of world travelers that are coming. But my sense is that the Brazilians are focused on it on the right things in the right way. That's probably all I can say at this point about that.

MS. MASTERS: So I think that brings us to the end. Thank you, Director Comey. I think we've learned a lot about encryption, the difficult choices you face. And I guess we all hope that you succeed. Thanks, very much.

MR. COMEY: Okay, you too. Thanks Brooke.

(Applause)

* * * * *