

SENATE COMMITTEE ON THE JUDICIARY HOLDS A HEARING ON OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

December 09, 2015

SPEAKERS:

SEN. CHARLES E. GRASSLEY, R-IOWA
CHAIRMAN

SEN. JEFF SESSIONS, R-ALA.
SEN. ORRIN G. HATCH, R-UTAH
SEN. LINDSEY GRAHAM, R-S.C.
SEN. JOHN CORNYN, R-TEXAS
SEN. MIKE LEE, R-UTAH
SEN. TED CRUZ, R-TEXAS
SEN. JEFF FLAKE, R-ARIZ.
SEN. DAVID VITTER, R-LA.
SEN. DAVID PERDUE, R-GA.
SEN. THOM TILLIS, R-N.C.

SEN. PATRICK J. LEAHY, D-VT.
RANKING MEMBER

SEN. DIANNE FEINSTEIN, D-CALIF.
SEN. CHARLES E. SCHUMER, D-N.Y.
SEN. RICHARD J. DURBIN, D-ILL.
SEN. SHELDON WHITEHOUSE, D-R.I.
SEN. AMY KLOBUCHAR, D-MINN.
SEN. AL FRANKEN, D-MINN.
SEN. CHRIS COONS, D-DEL.
SEN. RICHARD BLUMENTHAL, D-CONN.

WITNESS:

❖ FBI DIRECTOR JAMES COMEY

GRASSLEY: Before I give my opening remarks and Senator Leahy gives his opening remarks -- and my opening remarks are a little longer than normal -- I would like to say that there is a vote at 10:45. And I hope that between the Republicans and Democrats that we can keep the meeting going while we go over to vote at 10:45. That's my intention. And we'll have seven-minute round -- seven-minute questioning for at least the first round. And if people want a second round, that's permissible.

Director Comey, we welcome you and thank you for coming. The FBI's mission is to protect us from most dangerous threat facing our nation. The deadly attacks in Paris last week and -- or last month and California last week confirm that radical Islamic terrorism continues to be such a threat, regardless of whether that's politically correct or convenient for our president.

ISIS is a determined enemy executing a plan to gain and hold territory, enrich itself, inspire followers worldwide and launch deadly attacks against the West. And the American people are very worried not just about terrorism, but about our president's inability or unwillingness to rally the country, to lead our international partners to develop a credible strategy to destroy ISIS and to execute that strategy.

We are now paying a price for that weakness. At almost every turn, events have proven the president wrong about ISIS. In August 2012, he drew a red line warning the Assad regime not to use chemical weapons in Syria, but the president backed down after Assad gassed his own people and ISIS blossomed in the chaos that followed.

January 2012, the president referred to ISIS as a JV or junior varsity. It promptly spent the next six months conquering territory across Syria and Iraq. In August, that same day, our president conceded that he didn't have a strategy to defeat ISIS. A year-and-a-half later, he remains without a coherent one. Even former secretary Clinton admitted other day that we're not winning the fight.

The president has been hoping that ISIS will go away because its existence doesn't fit a preferred political narrative. But hope is not strategy. Hope is not a plan. And hope is not action. And all the while, the drumbeat of attacks on the United States continued. In May, there was an attack on the convention center at Garland, Texas. In June, police were forced to shoot a knife-wielding ISIS supporters on the streets of Boston. In July, we had the attack on military facilities, Chattanooga.

Director Comey as of October reported that the FBI was engaged in approximately 500 -- or 900 active domestic investigations against suspected ISIS-inspired operatives and other radicalized extremists. And he estimated that approximately 250 Americans have left the United States and travelled to Syria to fight with ISIS, or tried to do so.

Nonetheless, in November, the president assured us that ISIS was contained. But the very next day, it inflicted the deadliest Islamic terrorist attack in Europe in over a decade, a coordinated assault across Paris that killed 130 and injured over 350. A few weeks later, in San Bernardino, two of its apparent supporters executed the deadliest such attack on the homeland since September the 11th.

Unfortunately, our president has responded to this crisis by trying to divide us, deride us and distract us. In fact, he's doubling down in this strategy. After reports suggested that one of the Paris terrorists possessed a Syrian passport and entered Europe as a refugee, many expressed concern about the procedures used to screen refugees coming to the United States from Syria.

Director Comey expressed similar concerns in October. He warned that there are gaps in the information we have to vet people coming out of a war zone. And he warned that letting anyone coming to the United States carries some risk. We can point to the brothers who bombed Boston Marathon as an example of terrorists who were granted asylum here.

Our president responded to the concerns expressed by many Americans by mocking them for being afraid of widows and orphans. But events continue to prove our president spectacularly wrong. As it turns out, women are radical Islamist terrorists, too, apparently to the president's surprise. We now know that Ms. Malik, one of the San Bernardino attackers, arrived in the United States on a fiancée visa. This is yet another example of the failure of the screening process for those entering the United States. Our government apparently didn't catch the false address in Pakistan that she listed on her application.

To top it all off, earlier this week, we learned that the National Counterterrorism Center has identified individuals with ties to terrorists in Syria who are attempting to enter the United States through the refugee program. I guess that was one intelligence report the administration couldn't shade to fit its preferred conclusions.

Now, it's always -- bears repeating, legitimately so, that Islam is not our enemy. Radical Islamist terrorists are our enemy, however. The vast majority of Muslims in this country and around the world are non-violent and law-abiding. We all should oppose in no uncertain terms any violence or intimidation against Muslims for practicing their religion.

But I fear that one of the reasons for the regrettable backlash against Muslims in this country is the public's frustration with the president's repeated failure to acknowledge the actual nature of the threat that we face, his reluctance to utter the words "radical Islamic terrorism."

Our president has also concluded to divide us, deride and distract us with the issue of gun control. To the president, radical Islamic terrorism is never to blame, but the constitutional right to own guns always is. But terrorists aren't deterred by gun control. Strict European gun control laws did not stop the Paris attack. California's assault weapon ban didn't stop San Bernardino's massacre.

Now the Obama administration argues that allowing foreigners to buy guns who enter the United States through the visa waiver program is a problem. I agree. But at the same time, the administration's apparently -- the administration apparently is fine with allowing refugees, asylees and people on deferred action and other non-citizens who are not legal permanent residents to buy guns. That makes no sense. With a few exceptions, we need to prevent all these people from buying guns.

GRASSLEY: The administration's current fixation on guns and the visa waiver program can be explained, though, because it's another area where the administration's actions have made Americans less safe. In fact, an opinion from Obama's Justice Department required the Bureau of Alcohol, Tobacco and Firearms to change its policies to prevent persons arriving from visa waiver countries to buy guns and the administration's (ph) removes the long-standing requirement that non-citizens at least establish residency for 90 days in the state where they want to purchase guns.

These 90 days could be crucial in a terrorism investigation. So when we address the issue of foreigners in the United States buying guns, we need to be comprehensive about it, not just clean up the mess that this administration created.

Finally, our friends on the other side of the aisle have attempted to divide us, deride us and distract us with proposals to deny the right to purchase firearms to those on various terror watch lists, including no-fly lists. The incident in California and the terrorists connected with it were apparently not on any terrorist watch list. So such a proposal wouldn't have stopped that attack.

In addition, the president's claim that, quote, "people we don't allow to fly could go into a store right now in the United States and buy a firearm and there's nothing we can do to stop them," end of quote, just isn't true. The FBI is notified when somebody on the no-fly list attempts to purchase a gun and can take steps to ensure that a gun doesn't fall into the wrong hands. So the president and others have been misleading the American people on that matter.

But the more fundamental point is, while these lists are useful in keeping us safe, they are the result of the executive branch's unilateral decision to put people on them without any notice or opportunity to be heard. As a result, they can be unreliable.

And it isn't just constitutional to continue to condition a fundamental right to keep and bear arms on an administrative list that lacks that kind of due process. We couldn't consider conditioning any other constitutional right such as freedom of speech or religion or unreasonable searches and seizures on such a process.

That's why it is so surprising that this president, a former constitutional law professor, and so many of his political party would support a scheme. The fact is, law enforcement hasn't raised gun purchases by people on terrorist watch lists as a huge problem. And I know Director Comey knows that -- how to tell us when you have to confront a serious obstacle in keeping us safe.

At our hearing in July, we heard all of the talk from Director Comey about going dark, a problem in the increased use of encrypted communications by terrorists, and these most recent attacks will be -- I'll be interested in hearing from our discussion with technology companies that he's had about -- and how that's proceeding.

I also look forward to discussing a range of other issues with the director today. One if the FBI's treatment of whistleblowers. I hope I have the support of the director in strengthening the whistleblower law for the FBI. I also have questions about the FBI's investigation into former secretary Clinton's e-mail arrangement, the FBI's potential role in facilitating the ransom payments, that -- its use of spyware and the ongoing efforts to correct injustices that result from flawed forensic work.

I apologize for a longer statement, but I also think that these are things that we don't discuss enough, and we have the opportunity today to discuss them.

And now it is Senator Leahy's turn. Please take all the time you need, and I know you will anyway.

(LAUGHTER)

LEAHY: Well, the...

(UNKNOWN): (inaudible)

LEAHY: The Federal Bureau of Investigation, as we know, is entrusted with enormous responsibility, not only enforcing our laws but protecting the nation. No matter what the threat, no matter what the motivation of those threatening us, the FBI is told, Keep us safe. On any given day, FBI agents around the country investigating cases involving not only terrorism but violent crime, gangs, cyber crime, identity theft, fraud, human trafficking, hate crime, child exploitation.

And they know there's no simple answer. For example, one of the greatest terrorist attacks ever in this country by Timothy McVeigh, none of us said after that, Well, we've got to start excluding people who've served in the military or people of Timothy McVeigh's religion.

Instead, we went and found out what he had done and how we might stop others from doing the same thing. The events of the past six months have underscored the varied nature of the threats the FBI faces. This past June, nine African-American church-goers were murdered by a white supremacist during a bible study in Charleston. The day after Thanksgiving, three individuals, including a police officer, were shot to death inside a women's health clinic in Colorado Springs. Last week, 14 county workers in San Bernardino were murdered in a shooting rampage.

None of these seem related. All of them had different causes and motivations among those shooting. The director may not be able to share all the details about these investigations today, but I believe we can agree there's one common motivating factor behind each of these heinous crimes, and that's hateful extremism.

The one in -- the churchgoers who were murdered, the women in the -- the people in the women's health clinic and the people in San Bernardino, just hateful extremism coming from different directions.

So I think it reminds us to be vigilant against all forms of violent extremism, and I would hope that nobody underestimates the incredibly difficult job of protecting the country from terrorists' threats. We can try to put all the blame on any one person. That's fine, but it's not one person. It's all of us.

We have to support the law enforcement and intelligence officials who work to protect our nation by giving them the tools and resources they need to do their job effectively. And as we've heard from many law enforcement officials, we have to continue the very hard work sometimes of building trust in our communities among neighbors and with law enforcement so we can all share the responsibility of keeping our communities safe.

At the same time, I wish we would all categorically reject the divisive and corrosive rhetoric of fear that only serves to undermine us as a nation. We know what happens when leaders succumb to the politics of fear and lose sight of our fundamental American values.

Fear is what drove the government to violate the Constitution and imprison thousands of Americans of Japanese descent during World War II. Fear is what fueled the justification for

torture by the CIA which, Director Comey, you objected to when you were at the Bush Justice Department, and I applaud you for that.

And I know the director reminds all of his new agents that the rhetoric of fear led J. Edgar Hoover to target Martin Luther King, Jr., and others during the 1960s. And if we give in to this sort of fear, then that way, the terrorists and extremists win. They want us to be afraid. They want us to be a nation divided.

Groups like ISIS, for example, actively promote the narrative around the world that Muslims are not welcome in the United States. And certainly, some of the -- what I've called reprehensible and even unconstitutional comments by some allow them to spread that false notion around the world.

When there is talk about rounding up all Muslim Americans or creating a registry based on religious beliefs or shutting our borders to all Muslims, that's a sort of xenophobic, hateful rhetoric that just plays into our enemies' hands. It also demeans us as a democratic nation founded on the principles of freedom, equality and liberty.

We Americans are better than that. Let's not -- let's not succumb to fear and give an image that is not the great country that brought my grandparents and my great-grandparents here.

We're a courageous and strong country, and our strength comes from our commitment to the morals and principles that continue to keep our country great and a beacon of democracy to the rest of the world.

LEAHY: The Senate at its best -- at its best -- can be the conscience of the nation, and recent events demand that we start trying to be at our very best. We're not afraid of terrorists. We're not -- we should not let our country be defined by irresponsible fear-mongering.

And while the focus of today's hearing will naturally be on the recent terrorist attacks, and justifiably, we should continue the committee's bipartisan oversight of the FBI in other areas.

Three years ago, the FBI learned that flawed microscopic hair comparisons analysis was used in thousands of criminal prosecutions. Now, frankly, I'm not satisfied by the FBI's efforts to (inaudible) who might be affected by faulty evidence. The FBI should be sending agents out to gather the relevant information. The lives of potentially innocent Americans, including some on death row, depend on this.

In addition, I'll continue to work with Senator Grassley to ensure that whistleblowers at the FBI are afforded adequate protection.

I thank Director Comey for coming before the committee today. I've known the director for years. I know he shares my respect for the Constitution and my faith in American people that we can rise above the divisive rhetoric of fear because we're Americans. We should be better than that. And I believe we are.

Thank you.

GRASSLEY: Since this is an oversight meeting, I'd like to swear. Director Comey, do you affirm that the testimony you're about to give the committee be -- let me start over again. Do you affirm that the testimony you're about to give before the committee will be the truth, the whole truth and nothing but the truth, so help you God?

Thank you. I assume the director of the FBI needs no introduction, but I'd like to read a short introduction. It's a pleasure to introduce to you the committee. Director Comey became the director of the FBI 2013. He previously served as deputy attorney general and the U.S. attorney in New York and an assistant U.S. attorney in Virginia. He's graduate of William & Mary and the University of Chicago law school.

Welcome. Proceed with your testimony, however long you want to take.

COMNEY: Thank you, Mr. Chairman, members of the committee. It's good to be back before you.

As every member of this committee knows, the FBI has a very broad array of responsibilities to address a staggering array of threats that face our country in terrorism and counterintelligence and in criminal matters.

The key to us doing that well is the great people of the FBI, and I so appreciate your support for them. They are the magic of the FBI. The best part of my job is to get to know those people and to watch them work. And so I'm very grateful for the support of this committee for those good folks.

What I thought I would do is start with our top priority, which is counterterrorism, and tell you how we're thinking about it and tell you a little bit more about how we're approaching the attack in San Bernardino.

The members of this committee know very well that the terrorist threat we face today comes at us from a number of groups, most prominently today from the group that calls itself the Islamic State. The threat from the Islamic State has three dimensions. One, they aspire to send operatives to attack the United States and its allies.

Second, they aspire to attract people to come to the so-called caliphate to fight and achieve glory somehow from being in that savage place. And last, where they can't send operatives or attract travelers, they hope to inspire or direct -- and the two terms bleed together -- people to engage in acts of violence their home, to radicalize in their home and to kill innocent people on behalf of these terrorist groups.

In Paris, we saw one dimension of that threat, which was the sending of operatives to attack and kill innocent people. In San Bernardino, we saw last week a different dimension of the threat, which is the homegrown violent extremist, the radicalizing in place in order to kill innocent people on behalf of a foreign terrorist organization, to claim a foreign terrorist organization and try to give it credit for acts of violence.

To find homegrown violent extremists, to find those that are radicalizing and being inspired by these terrorist groups is a very, very hard thing. All of you know from overseeing our work, we work at it every single day, and we use all the lawful tools that you have given us on behalf of the American people.

Critical to our finding those people who are radicalizing in their homes is tips from the community. We have worked very, very hard to develop good relationships in communities all across the country, especially in Muslim communities, where we have terrific relationships. And those good people so often tell us when they see something that doesn't make sense. We are very grateful for that help.

We also want those folks to know that one of our responsibilities is to investigate civil rights cases and hate crimes. And we want people to know if you think someone is terrorizing you or threatening you based on your national origin or your religion, please tell us so that we can investigate that. We're all in this together.

San Bernardino involved two killers who were radicalized for quite a long time before their attack. In fact, our investigation to date -- which I can only say so much about at this point -- indicates that they were actually radicalized before they started courting or dating each other on line. And on line as late as -- as early as the end of 2013, they were talking to each other about jihad and martyrdom before they became engaged and then married and lived together in the United States.

We also believe they were inspired by foreign terrorist organizations. We're working very hard to understand exactly their association and the source of their inspiration. We're also working very hard to understand whether there was anybody else involved with assisting them, with supporting them, with equipping them.

And we're working very, very hard to understand, did they have other plans, either for that day or earlier, and that work continues.

Critical to that work is the support we get from state and local law enforcement through our Joint Terrorism Task Forces. Those 100 or so task forces are the backbone of this country's counterterrorism response. We are extremely grateful for our help from state and local law enforcement. And if you needed any confirmation of the quality and talent of the people in local law enforcement, you saw it that day in San Bernardino, when highly professional officers stopped what might have been more tragedy and more violence.

As you mentioned, Mr. Chairman, I do want to give you a very brief report in my opening about where we are with respect to the challenge of encryption to our hardest work, to our counterterrorism work and our criminal work.

As you said, since we were last together, we've had good conversations with the folks in the tech sector in lots of different parts of this great country of ours. And those conversations have convinced me of two things, which are both good news.

The first is we care about the same things. The tech companies and the FBI and everybody else involved in this discussion both care about safety on the Internet. We understand that encryption is a very important part of being secure on the Internet.

We also all care about public safety. We also all see a collision between those things right now. We see that encryption is getting in the way of our ability to have court orders effective to gather information we need in our most important work. And we all agree we have to figure out whether we can maximize both of those values, safety and security on the Internet and public safety. That's good news. We're not at war. We care about the same things.

The second piece of good news is all of those conversations have actually convinced me it's not a technical issue. There are lots of folks who've said over the last year or so we're going to break the Internet and we'll have unacceptable insecurity if we try to get to a place where court orders are complied with.

I actually think it's not a technical issue. There are plenty of companies today that provide secure services to their customers and still comply with court orders. There are plenty of folks who make good phones and are able to unlock them in response to a court order. In fact, the makers of phones that today can't be unlocked, a year ago, they could be unlocked. So I really don't think it's a technical issue.

And people also, I think, better understand today the government doesn't want a back door. The government hopes to get to a place where if a judge issues an order, the company figures out how to supply that information to the judge and figures out on its own what would be the best way do that. The government shouldn't be telling people how to operate their systems.

So we are in a good place in terms of what we understand about our values. We're in a good place, I think, where we realize it's actually not a technical issue, it is a business model question. Lots of good people have designed their systems and their devices so that judges' orders cannot be complied with for reasons that I understand. I'm not questioning their motivations. The question we have to ask is, should they change their business model? That is a very, very hard question. Lots of implications to that. We have to wrestle with it because of what's at stake.

I'm limited what I can say at this point about Paris and about San Bernardino, but let me give you a recent example. In May, when two terrorists attempted to kill a lot of people in Garland, Texas, and were stopped by the action of great local law enforcement again, that morning, before one of those terrorists left to try and commit mass murder, he exchanged 109 messages with an overseas terrorist.

We have no idea what he said because those messages were encrypted. And to this day, I can't tell you what he said with that terrorist 109 times the morning of that attack. That is a big problem. We have to grapple with it.

And I very much appreciate this committee's support for grappling with the hard questions around this. We must resolve the collision of those two values.

COMNEY: And then I'll finish, Mr. Chairman -- I apologize for running over my time -- with a word to the folks who may be watching us at home.

I know and the members of this committee know how unsettling seeing this violence in Paris and in San Bernardino is to the good people of this country. My hope is that they will not allow themselves to be paralyzed by fear but instead to channel that fear into something healthy, which is an awareness of your surroundings.

In case after case after case, we see that when someone radicalized, somebody saw something, either on line or in a school or at home, and didn't tell us about it.

We hope that what people will do is not imagine these savages of ISIL or of al Qaeda as something bigger than they are, not imagine them in the shadows -- that's exactly what these savages want -- but instead, simply be aware of your surroundings. If you see something, just tell us. We investigate in secret so that we do not smear innocent people. We will not race next door and bang on your neighbor's door.

If no harm was there, no harm will be done. But if it was something, we may be able to stop them -- something significant. So my request of the American people is, don't let these savages paralyze you. If you see something that seems out of place, tell one of us.

Thanks to the work of this committee and a whole lot of people in our government, we are better organized today than we were on September 11. If you tell a police officer, if you tell a deputy sheriff you saw something that doesn't make sense, we will get it to the right place. We will check it out. We will see whether it was something.

You, I hope, will go on with your lives. You pay us to do counterterrorism. We're not perfect. We are good at this. We cannot allow ourselves to be paralyzed by what these people are hoping to achieve. That's what I hope the American people will take from the unsettling experience of watching what goes on in San Bernardino and Paris.

And with that, I apologize for going over my time, and I look forward to our questioning.

GRASSLEY: No need to apologize for going over your time. And your reputation in both Republican and Democrat administrations is to call it like it is. And the American people are lucky to have a person like you, particularly because you have a 10-year term to really do your job right.

Director Comey, earlier this week, we learned that the National Counterterrorism Center has identified individuals with ties to terrorists in Syria who are attempting to enter the United States through the refugee program. You have acknowledged that there are gaps in the information that we screen -- in screening Syrian refugees.

But isn't it true that it isn't -- it's not just a lack of information that we have to worry about with people coming from Syria. After all, ISIS controls a large part of the country, including former

Syrian government offices and facilities. Presumably, it has the personal information of many innocent Syrians. It has virtually unlimited funds.

So now my question. Are you concerned that ISIS has the ability to create fraudulent passports or other identification documents for its operatives that has a practical -- that as a practical matter, it would be almost impossible to detect?

COMNEY: Yes, Mr. Chairman, the intelligence community is concerned that they have the ability -- the capability to manufacture fraudulent passports, which is a concern in any setting.

GRASSLEY: OK. Next point dealing with terrorists and the purchase of firearms -- last week, our president stated that there are individuals who can't get on planes, but they can go to a gun shop and buy a firearm and there -- and quote -- and he said nothing we can do to stop them.

But -- and correct me if I'm wrong -- the FBI is notified when someone on the terrorist watch list attempts to purchase a firearm and a NICS (ph) check is requested. And the FBI has multiple avenues that they can pursue.

These are some of these avenues -- delay the firearms transaction, and if the person is actually a terrorist, the FBI can arrest them for any crime for which there is probable cause. And in addition, the FBI can intervene and directly confront the individual. The FBI can also put the suspect on what's called around-the-clock surveillance.

My question -- aren't these some of the tools available to the FBI to stop a suspected terrorist from buying a gun?

COMNEY: Mr. Chairman, you're right, there are a variety of things that we do when we are notified that someone on our known or suspected terrorist database is attempting to buy a firearm.

The FBI is alerted when that is triggered. And then we do an investigation to understand, are there disqualifiers that we're aware of that could stop the transaction? And if the transaction goes through, the agents who are assigned to that case, to that subject, are alerted to it so they can investigate.

GRASSLEY: Yes. I thank you very much for that clarification. So there are, then, actually many things that can be done, done right now, to stop one -- someone on a no-fly list from buying a gun. And then that leads me to say that our president is misrepresenting the facts and misleading the American people on that point.

Next question In July, you testified before this committee about going dark. And you've already commented on some of this, but I want to be more specific. And members from both political parties expressed serious concerns about the use of strong encryption by terrorists and criminals.

I followed up with questions for the record, and I asked for data about the scope of the problem. At that time, the administration declined to ask for legislative solution. And I asked for time to

work -- and the administration asked for time to work with technology companies. But the attacks in Paris and California have generated increased alarm about the problem.

So question -- when is the FBI going to respond to my questions relating to that hearing? And that's not the most important point that I'm trying to bring out here.

Could you update us about what is known about the role encryption may have played in these attacks? And I know you've already said that you're limited in what you can say, but whatever you can tell us, do it.

And finally, what is the state of your conversations with the technology companies to address that problem? And you may have expressed that in your opening statement, the last part.

COMNEY: Thank you, Mr. Chairman. At your request and the request of other senators, we are collecting data concerning the ways in which encryption is affecting our ability to implement court orders for data in motion -- that is e-mails or phone calls -- and data at rest that is sitting on devices. And I don't know exactly when I'm going to get that to you, but that work is in progress. And it will show there's a significant impact and growing across our work, both terrorism and in criminal cases.

With respect to our conversations with the -- well, first of all, the second piece, with respect to its role in cases, I don't want to talk about Paris yet or San Bernardino because we're doing a lot of work with respect to those now. There's no doubt that use of encryption is part of terrorist tradecraft now because they understand the problems we have getting court orders to be effective when they're using these mobile messaging apps, especially that are end-to-end encrypted. We see them talking about that all over the world. It is a feature of -- especially of ISIL's tradecraft.

Last, the conversations with the companies have been good. Like I said, they really have made clear to me that we're not at war with each other. We care about the same things. It's also made clear to me that it's really not a technological problem. We're not going to break the Internet or expose us to tremendous insecurities of different kinds by requiring -- getting to a place where companies comply with court orders because lots of good companies do today.

It's a business model question. Good people have made a decision to design products and sell products where court orders are ineffective. And I'm not impugning their motives. I understand they see it as a competitive issue or they think it's just the right thing to do.

The question we have to ask ourselves is, is there a way to get folks to change their business model so that judges' orders will be complied with? And if that can't be done voluntarily, what are the other alternatives? And these conversations continue within the executive branch and with our private sector partners.

GRASSLEY: I could start another question now, but it'd take too long for you maybe to answer. So I think I'll go to Senator Leahy so we can kind of keep on time here.

LEAHY: Thank you, Mr. Chairman. I just want to follow up on a question that Senator Grassley asked you about the FBI being notified if somebody on a no-fly list or that type of list was buying a weapon. If they buy it at a gun show where there's no reporting, you're not notified, are you?

COMEY: That's correct.

LEAHY: And if they buy it on an Internet sale, you're not notified, are you?

COMEY: Correct.

LEAHY: And even if they go to a gun dealer who has to notify you, you're notified, but there's not an awful lot you can do about it, is that correct?

COMEY: Unless, as I said, we find some disqualifier, but if -- under the law. But if we don't find one of those things, there's nothing we can do to stop it.

LEAHY: So the president's statement that you've -- somebody on a no-fly list or on these watch lists can go and buy weapons in the United States is correct?

COMEY: There's no prohibition connected to the no-fly list, that's correct.

LEAHY: Thank you very much. I just wanted to make sure that was -- that was clear.

Now, you talked -- right after you were confirmed, you spoke about the detrimental impact of sequestration, a hiring freeze on criminal and counterterrorism investigations. I happen to agree very much with what you said. But I understand you're still in the process of trying to replace all the agents who were lost due to sequestration, is that correct?

COMEY: That's correct. We're still trying to dig out of that hole.

LEAHY: So when you can finally hire, you've got to train them, then you've got to get them into investigations. So this sequestration -- I don't want to put words in your mouth. But is that having a long-term effect on the FBI's ability to fight crime and terrorism?

COMEY: Yes.

LEAHY: Thank you. And what would be the impact on the FBI if Congress could not come to an agreement on an omnibus appropriation bill and instead pass another long-term spending resolution?

COMEY: Well, if we return to the impacts of sequestration that were kicking in when I started this job, it would be a disaster because we're just digging out of the hole. To return to a place where we have to ration gas and shut down Quantico and choose which people to interview based on how much gasoline we have in our tanks -- that doesn't make any sense to me. So it would be a big, big deal.

LEAHY: Without going into it here (inaudible) some of the worst- case scenarios you described to me privately, and they are chilling.

Now, we've had a lot of talk about our refugee system. I just want to clarify a few facts. The refugee program presents the longest and most complicated path for entry into the United States, and refugees do not get to pick which country they're sent to.

They are vetted more intensely than any other category of traveler. The vetting is conducted before any refugee can get on an airplane to come here. The process can take years.

That's why I agree with former national security leaders like General Petraeus and Secretary Hagel and General Brent Scowcroft who wrote to Congress that turning our backs on refugees would be contrary to our nation's tradition of openness and inclusivity and would undermine our core objective of combating terrorism.

Now, the House has just passed a bill that would require you to personally review, along with the secretary of Homeland Security and the director of national intelligence, each and every refugee application. Is that really feasible?

COMNEY: Well, first of all, if the intention is for me to do it personally, that would be very, very hard. But even -- as I understood the ask, it was could I certify to there being no risk associated with an individual. And again, the bureau doesn't take possessions on legislation and we don't get involved in policy decisions. But that practically would be impossible.

LEAHY: So it would make our refugee program impossible also?

COMNEY: Logically, if someone could only come in the country if I were to certify to that, it would -- it would.

LEAHY: Thank you.

We often hear from law enforcement the hateful and ignorant anti- immigrant rhetoric undermines community trust, ultimately harms the ability of law enforcement to do its job. As a same concern, we hear some say we should close our borders to all people of a certain religious faith or track people because they have certain religious beliefs.

I worry these kind of proposals feed what are the real lies that ISIS spreads, that the U.S. is anti-Muslim and they use that as a tool to recruit new members. Is that correct?

COMNEY: The notion that the U.S. is anti-Muslim is part of ISIL's narrative and al Qaeda's narrative and other terrorist groups.

LEAHY: Thank you.

Earlier this year, this committee in a bipartisan fashion approved a sentencing reform bill that reduces -- it doesn't eliminate but reduces the mandatory minimum sentences. I've said

oftentimes publicly that I'd like to see an end to all mandatory minimums, but at least it's a good step in reforming our criminal justice system.

Attorney General Lynch, Deputy Attorney General Yates (ph), former Attorney General Michael Mukasey and other law enforcement leaders have stated their support for this compromise bill.

Do you agree that it strikes a reasonable balance?

COMEY: Well, Senator, as you know, we don't take positions on legislation. But because I spent my career as a prosecutor, it's an area of interest of mine. I actually read the bill, and my reaction was it's reasonable. The things that are discussed in there are reasonable.

I have found mandatory minimums -- and we may disagree on this. I have found mandatory minimums to be an important part of making some of the most important cases I was involved with. But I think that the reform, as I understand it, seems reasonable to me.

LEAHY: The Fraternal Order of Police has strongly opposed a mens rea provision to this. And we don't have one in the bipartisan bill, which was negotiated, Republicans and Democrats. They say such a provision in this bill -- doesn't mean we can't look at mens rea in other criminal bills than this one, would be a poison pill. Do you have any views on that?

COMEY: I don't. I know it's a subject of interest. I don't know it well enough to comment. I was wracking my brain. I don't think I ever prosecuted a case that didn't involve a mens rea requirement, so I don't know enough to say.

LEAHY: And lastly, you know, I keep pushing for the bulletproof vest partnership bill which Senator Campbell (ph) of Colorado and I started. You have the resources to equip your agents with body armor. Would you agree that it's really important that local law enforcement have body armor?

COMEY: Very much.

LEAHY: Thank you.

Thank you, Mr. Chairman.

GRASSLEY: Senator Leahy, you probably asked the right question and the director answered it right. But also, the director answered my question right about whether the president was misleading. And that's because in the president's televised address -- and I think it was thoroughly vetted -- stated that someone on the no-fly list could walk into a gun store and buy a gun, and there was nothing that could be done about it.

So the president said nothing about going to a gun show or the Internet to buy a gun. And the director agreed with what I said about that at that time.

Now, the order is going to be...

COMEY: Mr. Chairman, could I...

GRASSLEY: Yes?

COMEY: I just want to make sure that I wasn't heard to be saying I think the president was misleading. I'm not trying to take shots at anybody. I was trying to answer the questions about what are our capabilities in that regard.

GRASSLEY: Thank you very much. I made the statement. You didn't make it.

The order at the fall of the gavel is going to be Graham, Cornyn and Lee. And then after the gavel came down, Hatch, Flake, Perdue and Sessions. And then I'll have Senator Leahy tell me who the next Democrat will be.

LEAHY: That'd be Senator Feinstein.

GRASSLEY: Senator Feinstein after Senator Graham.

GRAHAM: Thank you, Mr. Chairman.

I want to echo what the chairman said about your service as FBI director. I think we're lucky to have you. If I buy a gun on the Internet, is it delivered to my home?

COMEY: If you buy a gun on the Internet?

GRAHAM: If I try to buy a gun on the Internet, where do I pick it up?

COMEY: I assume it's shipped to you. But I don't know for sure, actually.

GRAHAM: OK. Well, let's find out the answer to that. OK. Do you agree with the following statement? There are more terrorist organizations with men, equipment and safe havens along with desire to attack the American homeland any time since 9/11?

COMEY: I agree.

GRAHAM: So do you agree that the budget cuts that Congress has imposed in the past has reduced your ability to defend this nation?

COMEY: I agree.

GRAHAM: Do you believe that the budget cuts that will go back into effect in two years will dramatically harm your ability and your agents' ability to defend this nation if sequestration kicks back in?

COMEY: I agree.

GRAHAM: Thank you. All right. Do you agree that rhetoric coming from political candidates running for president wanting to shut America down based on someone's religion empowers the enemy?

COMEY: I'm trying to avoid taking shots at anyone, as I said. I -- I...

GRAHAM: Well, just strike presidential candidates and put a widget.

COMEY: Yes. I do believe that our ability to get cooperation in the United States, which is my primary responsibility, our primary responsibility, depends upon people trusting us and having a level of comfort with us. And estrangement gets in the way of that.

GRAHAM: Do you agree with me that if you're a soldier, diplomat or FBI agent, serving in the Mideast right now, fiery rhetoric from here at home can put you in jeopardy?

COMEY: People who know better than I have said that, and so I credit that.

GRAHAM: Was the woman shooter in San Bernardino radicalized before she came to America?

COMEY: It looks like she was. So far, the -- what data we've collected, the intelligence indicates that she was before she connected with the other killer and came here.

GRAHAM: Is there any evidence that this marriage was arranged by a terrorist organization, a terrorist operative, or was it just a meeting on the Internet?

COMEY: I don't know the answer to that yet.

GRAHAM: Do you agree with me that if it was arranged by a terrorist operative or organization, that is a game changer?

COMEY: It would be a very, very important thing to know. That's why we're working so hard to understand it.

GRAHAM: Well, that's the biggest focus, I think, of how it would change game, that they could actually arrange a marriage of two like-minded individuals, use the fiance visa system to get into the country. So that's a good answer.

ISIL -- is it their goal to strike the American homeland?

COMEY: One of their goals, yes.

GRAHAM: It's not their only goal, but it's one of their goals. Is that correct?

COMEY: That's correct.

GRAHAM: Do you believe ISIL cells are already here in America?

COMEY: I don't have reason to believe that. It's something that we constantly look for and...

GRAHAM: But do you have any doubt they're trying to create one, if they don't have one today?

COMEY: No. They're trying to do two things. They're trying to motivate people already in the United States to become killers on their behalf. And they would very much like to -- they aspire to be the leader in the global jihad, send people here to conduct attacks. It's that second piece we have not seen yet.

GRAHAM: And that's what you have to guard against every day. I mean, they have to be right only once. You have to be right every day.

COMEY: That's right.

GRAHAM: And the less resources you have and the harder time -- the longer it takes you to find out what's going on -- if you can't listen to the conversations in a constitutionally appropriate way, then the enemy has an advantage over you, is that correct?

COMEY: Correct.

GRAHAM: Is it fair to say that they wake up every day in Raqqa, Syria, thinking about ways to hit us here?

COMEY: Some of them do, for sure.

GRAHAM: Is it fair to say that the Paris attack was a very sophisticated, well-planned attack that came from Syria?

COMEY: Yes. It...

GRAHAM: Is it fair to say that those people who plan their terrorist attacks would hit us here at home, if they could?

COMEY: Yes.

GRAHAM: How many countries does ISIL have a presence in?

COMEY: Sitting here, I can't give you a precise count, but it's...

GRAHAM: More than Syria and Iraq?

COMEY: Oh, certainly.

GRAHAM: I think there are a couple thousand now in Libya that took Gadhafi's home town.

COMEY: They claim branches in more than five, between five and ten. And the question of whether they have a presence is obviously something we're focused on here. But it's more than five.

GRAHAM: Can you give us any time period when you think ISIL will be destroyed?

COMEY: I cannot.

GRAHAM: Can you think of any means that we should take off the table that's constitutional in terms of fighting ISIL? Is there anything you want to take off the table in terms of fighting ISIL as long as it meets our constitutional requirements?

COMEY: Well, I think I'm only qualified to speak about the world that the FBI sits in, and we use all lawful tools that Congress gives us to try to meet this threat. So I would not take any tool off the table that is lawful.

GRAHAM: Right. And when it comes to tools, you're using all the ones you have because this is a very consequential fight.

COMEY: Yes.

GRAHAM: What do you think the likelihood of another 9/11 against the homeland will be if we don't destroy the caliphate in Syria and Iraq in the next year?

COMEY: That's certainly a hard question for me to answer. Their ability to have a safe haven from which to gather resources, people and plan and plot increases the risk of their ability to mount a sophisticated attack against the homeland.

GRAHAM: So the best strategy would be, at least in the short term, they're large, they're rich, they're entrenched, is to make them small, poor and on the run. Would that be a good approach to ISIL?

COMEY: That makes sense. And my understanding is that is the aim.

GRAHAM: Is it fair to say that other countries want to help America in this fight and we do not need to go it alone?

COMEY: Certainly, in dealing with the FBI, we have tremendous cooperation from a whole lot of countries. So yes, they are like-minded.

GRAHAM: Which country has the most gun control laws, France or the United States?

COMEY: I don't know.

GRAHAM: Would you check into that?

COMNEY: Sure.

GRAHAM: Because I just want everybody to know that gun control is a legitimate debate here at home. It's not part of a strategy to destroy ISIL, that the laws in France are very robust, but terrorists got the weapons. Don't mix the two.

Thank you very much.

HATCH (?): Ms. Feinstein?

FEINSTEIN: Thank you very much, Senator Hatch. And welcome, Director Comey, and thank you very much for your good work.

I was just reading a report "Isis in America," program on extremism from George Washington, where they say that 71 individuals have been arrested on charges related to the Islamic State since March of 2014 and 56 of them this year alone. Is that correct?

COMNEY: I don't know whether the precise numbers are right. But roughly, that strikes me as correct.

FEINSTEIN: OK. The last time you were here, you mentioned that you have an investigation going in every FBI field office in the country. Is that correct today?

COMNEY: Yes.

FEINSTEIN: OK. I wanted to ask you -- I was at home and I was watching on television when I saw press and others going through the apartment of the couple in San Bernardino that committed this terrible act. And I was appalled that it wasn't taped off because from an intelligence point of view, it immediately compromised any future intelligence gathering from any trace materials or anything else. How did that happen?

COMNEY: Yes. A lot of folks, I think, found that confusing. That is our -- out what I believe great criminal justice system in action in part. The way it works is we get a search warrant. It allows us to enter someone's residence. Our forensic experts and agents were in that residence for over 24 hours and combed through it and took everything that we could take under the search warrant and that was appropriate to take and recorded that which we needed to record.

Once we've exhausted that examination, we board the place up, make it secure. We have to post under the law an inventory of what was taken -- that's part of American law -- and then leave the residence. That part makes good sense to me.

The part I can't explain is why the landlord for the place allowed the boards to be pried off and for folks to go through.

FEINSTEIN: Let me (inaudible) Wasn't it important enough to have some law enforcement officer there to see that that didn't happen? I mean, after all, you know, 14 people were killed and

21 were injured. It seems to me that protecting that scene is really important. So I hope that there is some procedure whereby that doesn't happen again.

COMNEY: Well, the judgment of the investigators and our forensic experts was we were done with that scene. There was nothing else...

FEINSTEIN: (OFF-MIKE)

COMNEY: There was nothing else to be gained from that scene, which is why it was boarded up, and then the inventory was left. What happened next was strange and it struck me as strange on the TV that the landlord allowed the media to go through. But we had done our work in a careful, responsible way. Twenty-four hours is a long...

FEINSTEIN: Does it go back to local police jurisdiction?

COMNEY: No. It goes back to the owner and lawful occupant of the residence.

FEINSTEIN: So you relinquished the premises, regardless of whether somebody finds something that they want to come back and look for?

COMNEY: No, if there's a need for the investigation to continue to have access to the place, we will preserve the scene. We will put up crime scene tape. We'll post a guard on it.

But if we're done with someone's residence that we've searched, under the law, we return it and we post an inventory inside as to what was taken.

FEINSTEIN: Oh, boy!

Well, maybe we can talk a little bit about that, because from an intelligence point of view, I could see things in an investigation that would crop up that you might want to come back and look behind the picture frame on the wall because there's some message behind the picture that you don't know about when you went through the apartment initially, or some document. So it just doesn't seem to me to be smart.

But let me go on.

FEINSTEIN: With respect to encryption, Senator Burr and I on Intelligence are working on that issue. I can tell you that when I went and visited with the chief counsels of the big tech companies in my state about trying to get a bomb-making portfolio, 15 pages, off the Internet -- this was the bomb that goes through a magnetometer. And I pointed that out and I pointed out it had been tested and there was no interest in taking it down.

One company said -- Twitter -- "If we find something, we take it down, but we don't report it." In the intelligence bill which passed the Senate -- but this was taken out later in a need to pass the bill by unanimous consent -- we also have legislation that said that if you find terrorist information, you must report it to law enforcement.

Would you support that?

COMNEY: I know the administration and the Justice Department is formulating a view on that. And so that's for them to do. Operationally, it wouldn't have any bad impact on the FBI. And so I guess I've got to wait...

FEINSTEIN: The FBI wouldn't want law enforcement to know what's being said on the Internet that's terrorist-related or has complicity to commit an act -- I should say conspiracy to commit an act?

COMNEY: The more we know, the better.

FEINSTEIN: I would think so.

COMNEY: But I'm not in a position to offer a view on whether the Justice Department will support the legislation itself, I guess is what I'm trying to say.

FEINSTEIN: OK. OK. Fine. With respect to what you said on encryption, you don't want a back door, you don't want keys. It seems to me that the probable cause warrant process is the best process. You said here today enough to indicate that you would support that. Is that correct?

COMNEY: I'm sorry, support -- I'm not following. Support...

FEINSTEIN: Legislation which enabled a warrant with probable cause to be able to look into an encrypted Web, which you said the companies told you was possible.

COMNEY: Right. It's possible. Lots of companies do it today, provide secure services and comply with court orders. There are others who built their business models so that they say, Even if we want to, we can't. But the question of whether the answer is compelling them to do that by legislation is one that I can't answer sitting here. I think that's something the administration a couple months ago decided not to seek legislation now. But I also know there's continuing to be conversations inside the administration.

FEINSTEIN: Well, I'm going to seek legislation, if nobody else is. And I think -- I know Senator Burr thinks somewhat similarly. I'm very concerned about it because when I met with high tech, what they told me was there are parts now of -- when you talked to us about the dark Web, which I listened to very carefully, that they cannot unencrypt. And I can give you the names of the companies that said that to me.

And I have real concern about that. You know, I have concern about a Playstation which my grandchildren might use and a predator getting on the other end talking to them and it's all encrypted. And so I think there really is reason to have the ability with a court order to be able to -- and if you have cause to believe that criminality may be going on, to be able to get into that.

I suspect what happened was in the aftermath of Snowden, particularly Europe got very conservative with respect to encryption and the companies back away. Now that's changing with Paris, and God forbid what might happen in the future.

So what I'm trying to say is I think this world is really changing in terms of people wanting the protection and wanting law enforcement, if there is conspiracy going on over the Internet that that encryption ought to be able to be pierced. Do you agree?

COMNEY: I agree. I would very much like to get to a world where if a judge issues an order, companies are able to comply with it, either to unlock a device or to provide the communications between terrorists or between drug dealers or kidnappers. I very much would like to see that.

FEINSTEIN: Good. Thank you very much.

Thank you, Senator.

SESSIONS: Thank you, Senator Feinstein. Director Comey, thank you for your leadership. I believe you're a person that's well qualified for this job and understand the seriousness of your role and have the background and experience to do it well.

You know, you testified before the House committee on October 22nd, and you said, dealing with prisons and punishment, you struggle with the term mass incarceration, quote, "because it conveys a sense that people are locked up en masse."

But in reality, every case is individual. Everyone has a lawyer. Everyone has a judge. Everyone had to be proven guilty. And isn't it amazingly true that we're now over 95 percent of criminal defendants plead guilty in federal court?

COMNEY: The days of trials seem to be a bygone.

SESSIONS: So I think that's a testament, don't you, the good investigation and solid cases that are being brought?

COMNEY: I think at least in part, that's driving it.

SESSIONS: I think so, too. Now, since I was prosecuting, maybe since you were prosecuting, the guidelines, sentencing guidelines, under the Supreme Court, have become advisory, not binding. Attorney General Holder has altered traditional Department of Justice policy and declared that prosecutors don't have to charge the most serious offense.

The sentencing commission has reduced the guidelines that within (ph) in their power to do so. Senator Durbin and I worked together on legislation that reduced the penalties for crack cocaine rather significantly, more than a lot of people understand. And now we're considering additional reform in sentencing.

And I -- you said, I thought wisely, that -- you expressed concern about the increase in violent crime and murders around the country. Instead (ph), it would prompt you to be, quote, "thoughtful" about criminal justice reform proposals and noted, quote, "We have hit historic lows in violent crime recently. And if we let it slide back, we will need to explain to those who come after us what we did or didn't do to let that happen," close quote.

Would you kind of explain the trends in crime and punishment and why you shared those words?

COMNEY: Yes. What I was getting at, Senator, is our world with respect to violent crime is a world that was hard to imagine 25 years ago, and a whole lot of hard work went into getting us to an historically peaceful America. A big part of that, I believe, was law enforcement's work.

And I also believe every sentencing I ever went to in a way was a tragedy because a life was being wasted, but that work had to be done to protect those neighborhoods. And what I was urging folks to do is -- I think Harry Truman said the only thing new is the history you don't know -- is for folks just to remember we used to be in a very different place.

And there are reasonable reforms, as I said earlier, we can put into place, but we have to remember where we once were, and I wouldn't want to do anything without understanding the history that lets us slide back to that place.

And I was saying that in the context of a worrisome spike in homicide in over 30 of the nation's top 50 cities that's occurred this year. That's hard to explain, but it's very worrisome. And I was simply sounding an alarm, saying we have to talk about this because we have gotten to a great place in this country. And this is worrisome and it drives us to need to be even more thoughtful about how we change our criminal justice system.

SESSIONS: Well said. I think this is -- I was there when the crime rate was high, and I've seen it decline as a prosecutor and subsequent to my time. And we made real progress.

I have a chart that shows the federal prison population and how it's been developing. And I hope my colleagues will look at this chart because we have the perception that federal prison population is surging. But in fact, it peaked around 2013 or so. It's been declining steadily ever since. And according to the Bureau of Prisons, they project the population in federal prisons this year to drop by nearly 15,000 additionally. So we're just not on a trend, a mass incarceration and surging federal prison population.

What about state prisons? There's many, many more in state prison than in federal prison, maybe 10 times or more. Let's see what's happening in the state systems.

SESSIONS: We've seen a rather dramatic increase -- decrease in penalties in states. And part of it's budget-driven. And people then begin to develop theories to justify reducing prison population based on budgets. And you have also a lot of people have always doubted the value of prisons. So we've seen a substantial decrease in state prisons, and I think that will continue.

So I guess -- and since we know there's a pretty high recidivist rate for prisoners -- and I'm not trying to put you in a big argument here, but the fact is that more people that are released from prison -- aren't they in a -- aren't they likely -- aren't we likely to see an increase in the crime because the recidivist rate remains high?

COMNEY: I'm not an expert. As I think you said, I -- the logic of it would say, yes, there would be -- given the recidivism rate, which is one of the things that's exciting, I think, about the legislation Senator Grassley talked about, tries to get us doing a better job of reducing recidivism. But the math would say sure.

SESSIONS: And here the Association of Assistant United States Attorneys wrote us a letter and said this. "Every incremental weakening" -- questioning plans to further reduce sentencing. "Every incremental weakening of those mandatory minimum penalties will have a corresponding impact on the ability to successfully investigate and prosecute drug trafficking. The current proposal will significantly weaken the mandatory penalties and significantly deprive law enforcement authorities and prosecutors of the tools they need to successfully address drug trafficking."

Now, you said you could accept the changes. But those are -- that's a statement that's worthy of serious evaluation, would you agree?

COMNEY: Sure.

SESSIONS: Thank you, Mr. Chairman.

GRASSLEY: I've been told by Democrat staff that Senator Whitehouse is next.

WHITEHOUSE: Then I will go next. Thank you, Mr. Chairman.

Welcome, Director Comey. As the author with Senator Cornyn of the title you just said was exciting, I thank you.

I want to talk ask you about two things. One is botnets and the other is to follow up on Chairman Grassley and Senator Feinstein's concerns about encryption of communications.

Botnets first. Senator Graham and I have a bill that tries to enhance the department's authority to pursue the civil remedies that have allowed the Department of Justice to pull down botnets. One of the challenges that that effort has faced has been the legal requirement that the botnets have to be engaged in fraud an -- or wiretapping before the department can go and pull them down.

My sense is that a botnet is essentially like a weed. There is no such thing as a good botnet. They are either actively doing evil things or they are a latent mechanism for doing evil things later on and that a more rigorous effort to root them out of the Internet and create better Internet hygiene against botnets would be a good thing.

Now, when I had a vote organized on that, and there were various machinations in the Senate that prevented the botnet provision from coming to a vote. And behind that were some statements that I'm a little bit astonished by, but basically, that some botnets are actually good and we should protect them out there.

I see you looking very surprised. But let me ask you, could you react to that? Do you think I'm in the right place on this, that a botnet is either a latent or an active menace on the Internet and that we should be aggressively taking them down?

COMEY: I had that facial reaction because I don't know of a good botnet. Botnets are armies of zombies. So whether they're coming at you or whether they're standing still, it's still really bad. I don't know of a good purpose for an army of zombies.

WHITEHOUSE: Thank you very much. I appreciate it. I'm glad we're on the same wavelength.

With respect to encryption, we talk about it often as a technical question. And let me be the first to say I don't want a government back door, either. Nobody wants a government back door.

But as you say, when it's the business model of a particular company to disable its own ability to comply with a properly authorized subpoena or search warrant under our laws, that's a very different proposition. And it's that proposition that I want to speak to.

And I'd like to ask you to talk about two things. The first is, from the FBI's perspective, what do you think are going to be the worst and most dangerous consequences of that encryption, propagating and criminal use of it, or terrorist use of it?

And less from the FBI's perspective but more generally, since the FBI is a leadership organization within law enforcement, what do you think regular police departments and law enforcement officials around the country are most likely to see as the hazards of this encryption in their efforts to protect the public? So first the FBI, and then more general law enforcement concerns.

COMEY: From the FBI's perspective, we are increasingly seeing, inevitably will see entirely that criminals and terrorists and spies have an unparalleled ability to communicate with each other worldwide. Increasingly, we are unable to see what they say, which gives them a tremendous advantage as against us, right?

In the good old days, it was harder for them to communicate with each other. Today, they have a tremendous ability. Our ability to monitor them has not kept pace. In fact, it's going in the wrong direction. So our ability to find people hiding in the United States looking to do bad things, to root out all kinds of organized criminal actors, is steadily being impaired. That's the problem.

State and local law enforcement, the impact is for them almost entirely devices that cannot be opened with a search warrant. And I do very much agree it's a business model choice because the folks who are today selling those phones, a year ago their phones didn't have the capability. I don't remember anybody saying, I'm not buying their phones because they're insecure. It's not a

security issue, it's a business model issue. And there are good motivations behind that, but we have to talk about those.

And so they're encountering increasingly in kids missing cases, in drug cases and violence cases, devices that are a brick to them that hold all of the evidence that might help them figure out where a child is, untangle a kidnapping or figure out where a drug gang is operating.

That's their problem, less the data in motion problem for the state and local, but increasingly this -- they cannot reach the evidence that a judge would otherwise authorize them to get.

WHITEHOUSE: That's very compelling testimony. And I can share with you that the chief of staff to the president of the United States said that -- to me that one of the things that keeps him up nights is this encryption problem.

My concern is if these companies have already made the decision that it's their business model to prevent law enforcement from using subpoenas and search warrants in the traditional way, then they have a business justification, in their minds, for doing it. And if that's their position, how is talking to them going to change that? Where is the leverage point? What is the administration's process for trying to solve this problem?

COMNEY: Yes, I don't know that there's a leverage point that's going to flip it from one side to the other. I do think that all businesses are making tradeoff decisions. And at least in part what's motivated some of the companies to switch to this default encryption is they believe -- I'm not questioning their good faith belief -- that it's a competitive imperative, that customers want this.

And so the conversations are useful because I think we can show them there's tremendous harm associated with this, and the customers increasingly see that. And so my hope is they'll see that calculus differently and their customers will speak to them and say, No, I'll keep using your phone. It's a great phone, even if you would allow a judge to issue an order to unlock it in a terrorism case or in some other criminal case.

WHITEHOUSE: And presumably, if you could show that but for the phone having been turned into a brick as a result of the company's business practices and been protected from search warrants and subpoenas, a child was -- could not have been rescued who otherwise could have been and there's a fatality that has resulted. Presumably, they would see that as something less than great publicity for their choice.

COMNEY: Well, and I actually -- I mean, I wasn't just saying this. They do care about public safety. These are good people. What the conversations have helped them understand is the darkness that we see because good people don't spend all day long worrying about the things I worry about. What the conversations have helped them see is, Wow, there really is a real-life impact to this.

We're trying to find terrorist needles in a haystack. When we find one, it goes invisible because they're using end-to-end mobile messaging apps. That has real consequences. These good people

see that. That's where there conversations have helped. And where that's going to lead, I don't know yet.

WHITEHOUSE: Thank you. If we can help in any way, please call on us.

GRASSLEY: (OFF-MIKE) Lee is next. But before you go, then unless Durbin and -- and Schumer come back, it'll be Klobuchar and then the other senator from Minnesota.

(LAUGHTER)

GRASSLEY: I'm going...

(UNKNOWN): (OFF-MIKE)

(LAUGHTER)

GRASSLEY: And the reason I took time to do that, I'm going to go up to Budget and ask a question. So I hope everybody will observe the seven-minute rule.

LEE: Thank you, Mr. Chairman. As the other senator from Utah, I'm happy to comply with the seven-minute rule.

(LAUGHTER)

Thank you, Mr. Comey, for being her with us today. Thanks for all you do to keep us safe.

There's been some discussion, a little bit of confusion lately about the USA Freedom Act. In part, this has been precipitated by some of the discussions going along with the presidential election cycle that's in full tilt now. But to clarify, I have just a few questions about the USA Freedom Act and how it operates. First of all, the USA Freedom Act doesn't prohibit the government from gaining access to telephone metadata, correct?

COMEY: Correct.

LEE: It allows the government to get metadata, telephone records connected to any terrorist investigation, such that if the government wants to gather metadata connected to a particular phone number that it believes is connected to a terrorist investigation, the government can get that.

COMEY: Correct.

LEE: And the USA Freedom Act does not affect in any way the government's ability to gain access to any metadata that either originated -- as to a phone call that either originated outside the United States or that originated here and was directed outside the United States.

COMEY: Correct.

LEE: Did the enactment of the USA Freedom Act substantially affect the government's ability to prevent the San Bernardino attack?

COMNEY: I'm only hesitating because I don't want to talk about particular techniques we are using to understand that attack. That's why, I guess, Senator, I need not to talk about it in the context of that particular case.

LEE: OK. I would note here only that it is significant that only four days prior to the attack, the government had access to all of the records that it had access to, that it had access to for years prior to the passage of USA Freedom Act because there was a six-month moratorium between its passage and it kicking in. And I personally consider that highly unlikely, some would say mathematically impossible that it had any difference there.

And certainly, the government can still investigate the San Bernardino attack by going after records of the individuals suspected to be involved in that attack?

COMNEY: Sure.

LEE: Thank you. I want to talk a little bit about this encryption issue. I was pleased to hear you say, and I hope I understood you correctly, that you're not pushing for legislation that would mandate tech companies to put a back door, to develop a back door and make that available.

COMNEY: Correct.

LEE: What you are saying, as I understand it, is that some companies, many companies, could choose voluntarily to assist law enforcement in the execution of a warrant in helping gain access to any information they might have access to.

COMNEY: Correct. And those are the conversations we've been having.

LEE: And so -- but I assume in order to do that, would they have to develop their own back door that they could use internally?

COMNEY: Well, I don't know what in that context the term back door means. They'd have to figure out how, consistent with their security requirements, they could comply with the judge's order, as a lot of companies do today. So they'd have to figure out, under our system, what would be the best way to comply with the judge's order.

LEE: OK. Let's suppose that we have companies doing that -- perhaps some, perhaps all. Perhaps they're doing it because they want to do it, or perhaps at some point, assuming Congress were to pass something requiring them to develop a back door, a universal key that could be used to unlock the encryption. If U.S. technology companies started doing that, perhaps some of them, perhaps most, perhaps all, that wouldn't necessarily end the going dark problem, would it?

Because wouldn't we still have technology companies located outside the United States still manufacturing devices that wouldn't be subject to that requirement or wouldn't be subject to the same thing that would be convincing American companies to do that.

COMNEY: No, I think that's right. Both -- in two respects. Devices manufactured in other places might be different, and communications services from providers outside the United States might be different, which is what makes this such a hard problem. A big piece of it has to be international.

LEE: Right. So even assuming Congress were to enact something requiring the use of a back door, or the availability of a back door, a de-encryption key, if you will, it still would not solve the problem because there would be foreign manufacturers.

It also occurs to me that even assuming all U.S.-produced devices had a back door key of sorts, it's my understanding that it's still possible to design an app, that there are people all over this country and other places throughout the world who can with relative ease could design an application to be used on a smartphone, for instance, or perhaps on a computer that could provide encryption that couldn't be unlocked through an encryption key made by the manufacturer for the device in question. Is that your understanding?

COMNEY: My understanding is, I think, the same, that with respect to a device, if the manufacturer were able to, as they were a year ago, to unlock on a judge's order the device, there may still be apps on the phone that are strongly encrypted. And so the content in that particular app would not be available once you unlock the phone.

LEE: Correct. So if U.S. manufacturers were to start developing this back door key and they used it, they had it, they made it available to law enforcement under appropriate circumstances, presumably, those who were determined to go dark could and would start using an app that would itself not be subject to being opened by that same key.

COMNEY: Yes. I hate to keep doing this to you. I struggle with that term "back door key." What I'm talking about is, a year ago, the manufacturers of the leading phones of the United States could unlock them, if a judge ordered it. I don't know whether that involved a key or their software. Somehow, they were able to do that.

But you're right. If we return to that world, there could still be -- the sophisticated user could still figure out how to use something like True Crypt (ph) to protect other content on that device.

I think there's no way we solve this entire problem, right? Encryption's always going to be available to the sophisticated user. The problem we face post-Snowden is it's moved from being available to the sophisticated bad guy to being the default. And so it's now affecting every criminal investigation that folks engage in.

But I agree there's no way to solve this entire problem. I still think it's worth trying to solve a big chunk of it.

LEE: And so the big chunk of it here would involve U.S. manufacturers of U.S. devices, notwithstanding the fact that we still would have the risk associated with apps that couldn't be opened by means of the same methods that you're describing.

COMEY: Sure. There's others part of it that would be difficult to solve, too. You mentioned the international aspect of it. Part of the solution, I hope, will involve an international set of norms somehow because our partners in Europe very much face the same problems we do. And so they're very interested in having the rule of law nations figure out, So what should the rules of the road be with respect to encryption?

LEE: Right. OK. I see my time has expired. I do want to be clear. One of the reasons I asked the question is I -- one thing that I think we ought to be cognizant of is that we ought not put U.S. manufacturers in a position in which they'd be punished relative to other manufacturers, especially if U.S. manufacturers then saw a drop in sales because people, for whatever reason, preferred other products.

And we got to remember the limits on what we can do legislatively. If we were to mandate that legislatively, it wouldn't necessarily fix the problem.

I see my time's expired. And I believe Senator Durbin is next in the batting lineup.

DURBIN: Thank you very much, Senator Lee.

And thank you, Director Comey, for being here. I'd like to speak to you for a moment about the gun issue and terrorism. I want to know if you believe that terrorist organizations around the world are aware of American gun laws.

COMEY: As I sit here, I don't -- I assume that they are. And there's probably some specific I've told. I can't remember, sitting here. But I assume that they are.

COMEY: Let me just read a quote from one, an al Qaeda spokesman, Adam Yahi Ghadan (ph), American-born, who said in a 2011 video, and I quote, "America is absolutely awash with easily obtainable firearms. You can go down to a gun show at the local convention center and come away with a fully automatic assault rifle without a background check and most likely without having to show an identification card. So what are you waiting for?" That's what his quote was.

While fully automatic weapons are not readily available for civilian use, semi-automatic assault rifles are, and technology exists to convert them. There are reports that the San Bernardino shooters were trying to convert semi-automatic rifles into fully automatic versions. Can you comment on that?

COMEY: That is something we're looking at. There's an indication that they attempted to convert or did convert them successfully. And I can't give you the answer sitting right here.

DURBIN: I guess the point I'm trying to make for the record is that those who would do us harm know that it is easy to obtain firearms and weapons in the United States under our current set of laws.

DURBIN: I'd like to ask you a question based on your opening statement. And I think I understood what you said, is that you have found a public -- some type of utterance by the two killers that they were dedicated to jihad many years ago. And I want to ask you whether that statement was made prior to the granting of a fiance visa to the wife.

COMEY: Yes. And prior, frankly, to the rise of ISIL. DURBIN: And do you see any weakness in our system when it comes to visas or fiance visas that that sort of information was not known to us before she was granted access to America?

COMEY: I don't know enough to say.

DURBIN: We are discussing visa waiver programs now and how we can change them to make them better. Roughly 60 million foreign visitors come to the United States each year. I understand 20 million are from the 38 countries where a visa is not necessary. And one of the things that is being discussed is to require a biometric examination or investigation before the visa waiver traveler boards the airplane.

Do you have any thoughts on whether that would help to make us safer?

COMEY: I have not thought about it well enough to give you a reaction.

DURBIN: Well, I wish you would think about it, and I'm sure you will. And it boils down to whether or not prior to having access to an airplane, you present your fingerprints so that they can be checked against the information systems in Europe and in the United States.

Is there a good exchange of information, incidentally, between our European allies and the United States when it comes to such things as the fingerprints of suspected terrorists and known criminals?

COMEY: It is good. It has gotten a lot better in the last two years, and there's still room to improve yet.

DURBIN: I hope you can. I think it's very important. Let me ask you the question -- I want to make sure it's clear in my mind. If someone on the no-fly list walks into is a licensed firearms dealer in the United States, that in and of itself is not a prohibition against that person buying a firearm.

COMEY: Correct.

DURBIN: So even if that person is suspected to be a terrorist, they could purchase the firearm and leave with it, though your agents may then follow them or investigate them or keep an eye on them because of that purchase.

COMEY: That is correct. We have three days to review the background. And so a hit -- if someone walks in and they're on the no-fly list, we'll immediately be notified. We'll have three days to figure out whether there is some prohibition under the law that allows us to stop the transaction. If not, they will walk out with the gun if the dealer transfers it.

DURBIN: Absent some other disqualifier, the fact that they're on the no-fly list is not enough -- sufficient basis to deny the sale, is that correct?

COMEY: That's correct.

DURBIN: I'd like to bring this closer to home in terms of violence -- gun violence in my state. We recently traced the crime guns that were seized in the most violent sections of Chicago, and we found that 40 percent of those crime guns were coming into Chicago from gun shows in northwest Indiana, where there was no requirement for a background check before the sale was made.

Of course, it's not just firearms. It's ammunition, as well. And we have ample evidence that those who were engaged in this gun violence make the short trip over the border into Indiana, secure their weaponry and their ammunition and come back and kill people in Chicago.

What more can we do? We brought up the issue, and I won't engage you on it because I think you know the debate, about extending background checks to gun shows and Internet sales. What more can we go with this knowledge, though, that these guns crossing state borders into the city of Chicago and being used in the commission of crime?

COMEY: Well, under the current legal regime, we, and especially our colleagues at ATF, try to understand, are there straw purchasers involved in that? Are there gun show participants who know that they're selling to felons or prohibited persons and trying to make trafficking cases based on that. That's sort of the focus of trying to stop bad guys from getting guns at gun shows.

DURBIN: Is there any surveillance of these gun shows to see if there are out-of-state license plates or anything of that nature?

COMEY: I think if there's a predicated investigation of a particular dealer within the gun show, there's appropriate surveillance. But I'm not aware that there's surveillance generally of gun shows.

DURBIN: Thank you. The last point I'd like to make, in his opening statement, our chairman suggested that he would be open to the notion of prohibiting foreigners who are in the United States on the visa waiver program to purchase firearms. That is a provision which I have been offering. I would just say for the record I hope I can work with the chairman and get his support in making sure that this loophole is closed.

Thank you, Mr. Chairman.

GRASSLEY: On the visa waiver program and guns, what I was trying to say is I want to go further than that.

DURBIN: I'll be glad to work with you. Thank you, Mr. Chairman.

GRASSLEY: Senator Flake.

FLAKE: Thank you, Mr. Chairman.

Thank you, Director Comey. Let me -- encryption has been talked about some, but let me talk about some of the other vulnerabilities we have and difficulties tracking information.

I think we've discussed maybe this before, but the other ways for potential terrorists or terrorists to communicate here -- it's obviously not just e-mail, it's not just text messages. And I asked some that are familiar with the field, if you had a bet (ph) to communicate that you didn't want anybody to follow it, how would you do it? And some say, well, you get on an app or a game, words with friends, or some other game. And in the comment section -- or there's a way to communicate within that.

That is probably -- I mean, there's no way to use encryption right now for that. But it's just in the realm of a lot of data, a lot of communication, a lot out there.

Is that something that's concerning to the FBI? And how -- what are we doing, without revealing sources and methods and everything else, to deal with that situation?

COMNEY: Thank you, Senator. I don't want to say too much about it because I don't want the bad guys to get ideas they don't already have. But we have seen a number of cases in which subjects of investigations have communicated through gaming channels, either through more live action games or sometimes through app games on devices.

Sometimes, those do involve encryption, though. Those communications are encrypted in the gaming channel, which makes it as hard for us to intercept with a court order as another encrypted channel. So it's increasingly a feature of our work, I guess is what I'll say.

FLAKE: OK. All right. Thank you. We've seen high-profile data breaches, obviously, with OMB. What is the FBI doing to ensure that we don't fall victim -- a lot of information, obviously, held by the FBI is extremely sensitive. Are we taking the measures that we need to? And how can Congress help to ensure that that data is secure?

COMNEY: Well, we worry about this every day, and we try not to be overconfident. I think we have very good systems, but we can't be satisfied because, you know, as good as your system might be, if human beings have access to it, there's a vulnerability there.

So the FBI, especially since Snowden, has stepped up our game there to make sure we understand the potential insider threat. And so we focus on it from a technological perspective

and from a human vulnerability perspective an awful lot, is probably the best headline I can give you.

FLAKE: You've mentioned in your testimony that one of the areas of focus is to ensure that we deal with corruption at the border. Can you give us an idea what you're doing to combat that?

COMNEY: All of our field offices along the Mexican border have robust public corruption squads and efforts going on there because any time you have human beings in a role where there's potentially tremendous amounts of bad money, there's a risk of people being compromised.

And so it's from -- all the way the Gulf over to the Pacific Ocean in California by all of our field offices. We work it in partnership with DHS because a lot of focus is on, Is there corruption in the border control workforce, for example. And I think we've built over the last couple years a pretty effective relationship there.

FLAKE: Back to the visa situation. K-1 visa has come under scrutiny now. You mentioned in previous testimony in the House the difficulty in vetting refugees, for example, because of lack of information about their background. I assume if that's true in Syria, it may be doubly true in South Sudan or in Somalia or elsewhere, and so we have to rely heavily on interviews and assessments by field staff there.

What methods do we use there, lie detector tests, to try to vet whatever information is given? What do we have now, and what else can we do in that regard if there is a lack of information or data to check what they say against?

COMNEY: State and DHS would be better qualified to answer this than I. I don't think they -- in fact, I'm quite confident they don't use a polygraph in that context. It's a problem where you don't have data that you can vet somebody against, you have to rely upon a skilled interviewer in a consular office or some other place to see if they can detect deception.

And I know we have professionals doing it, but I don't know it well enough to tell you what particular tools they've considered using.

FLAKE: You mentioned -- and I think we've all seen the professionalism of some of the state and local officials dealing with the situation, for example, in San Bernardino. That's not always the case in -- elsewhere in the country, where we have local officials who maybe need training or expertise.

What is the FBI doing to ensure that our local partners are doing what they can to identify or to try to prevent or deal with these tragedies when they occur?

COMNEY: With respect to terrorism attacks?

FLAKE: Yes. Yes.

COMNEY: Yes. Well, the bedrock of our effort is our Joint Terrorism Task Forces and the relationships we've also built with state fusion centers to make sure that we give our local partners what they crave, which is good information about what the threat is, how they might check it out, and good training on how to respond when there is an incident.

We have invested a tremendous amount of effort and money trying to make sure we equip local state and local law enforcement to be able to respond well to these threats. We've just produced a video called "The Coming Storm," which is chilling but extraordinarily valuable, that through real-life movie actors shows how to respond to an attack, in that case on a community college, the best way to organize yourself, the best way to respond. I've heard great feedback from our state and local partners.

We've made tens of thousands of copies of this. I think every university police force should have it. Anybody who's responsible for protecting a community should have it and look at it.

FLAKE: Thank you, Mr. Chairman.

SCHUMER: Thank you, Mr. Chairman. First, thank you for having the hearing, to you and Senator Leahy.

And Director Comey, I'm an admirer of yours. I was before you took this position and more so now, and an admirer of the men and women who work in the FBI. I think you do a great job. So none of these questions are intended to impugn the hard work, integrity of all of you.

Look, we in New York, praise God, after 9/11 haven't had a successful terrorist incident. We've had a few in the country now. But it's because of the hard work of your folks and others on the Joint Task Forces that you mentioned, including the NYPD, who do a great job, as well.

Here are my questions. In your testimony this morning, you told us the San Bernardino attackers were communicating on line about jihad for some time. So this raises two big questions which I'd like to pursue. The first is how come we didn't know about these communications before the attacks? And the second is how did she get a visa? How did somebody who's not an American citizen pass a visa test when they were communicating about jihad on line before, no questions asked?

So Let's go to the first one. First, how do we know when terrorists are communicating on line, and how does it sometimes get missed? How in this -- I know you're exploring this and I don't want to step on any ongoing investigators. But in general, this is going to cause great consternation to the American people and I think to every one of us, certainly me.

Here we have somebody who was talking about jihad, two people, for a couple of years. And I always -- you know, I would -- I think most Americans have the assumption that we're on top of things like this.

COMNEY: And I can only answer it in general. I don't want to talk yet, if I could, Senator, about the particular case.

SCHUMER: OK. So let's take a hypothetical, OK? Someone's -- someone's talking jihad over and over again on line. Do we know of it in most cases? And what do we do about it?

COMEY: We will only know about it, if it's a private communication and not a posting on a public forum or on a public-facing social media site -- if it's a private communication, whether it's electronic it's or by the mail, we're only going to know about it if we have some reason to believe that it was going on that allowed us to get permission from a judge to intercept those communications.

That's where the community comes in. If folks tell us, I think this guy is up to no good, then we can start to look at it and use our lawful tools. But I know the senators know this, but we don't monitor, and we shouldn't (inaudible)

SCHUMER: What about non-American citizens talking to American citizens?

COMEY: Well, again, that is governed by the rule of law in the United States. And so we have to have predication, the FBI or intelligence agencies, to be able to intercept the communications of an American, whether they're communicating in the United States or overseas.

SCHUMER: OK. And in this case, was there any public -- OK, so let me ask it more generally. Let's say there is some public posting, OK, on a Facebook page or something like that, where either an American citizen or a non-American citizen communicating with an American citizen mentions jihad several times. Do we -- do we know about that? And what do we do about it?

COMEY: Often, we know about it either because a source of ours or an undercover of ours or a community member who sees it tells us about it. And then we can jump on it and use all of the tools...

SCHUMER: Do we have enough people monitoring these things so that when it's public, we know about it if no informant or neighbor has told us?

COMEY: The answer is certainly not, given the size of the communication networks we're talking about -- I mean, millions and millions of people talking to each other and making Facebook posts and whatnot.

SCHUMER: Right.

COMEY: It's impossible to monitor...

SCHUMER: But I would imagine on public postings, you could get -- we have computers, for instance, that stop child pornography with a certain image that's on there. Couldn't we get computers that spit out to us who publicly -- and we don't know if these communications were public or private. You haven't said, and I'm not asking you to do that in this particular case.

But couldn't we get a computer to spit out to us somebody who's talking about jihad, bombing, you know, some words like this repeatedly and to a variety of people?

COMEY: Well, I want to be careful what I talk about in open setting. But there are tools, but they are limited in a way you would want them to be.

SCHUMER: I see.

COMEY: But the United States government, unlike some other governments in the world, does not monitor the Internet.

SCHUMER: So final question. Could we be doing more in these types of situations?

COMEY: We can always be doing more.

SCHUMER: OK. And is resources a problem?

COMEY: Resources is a -- I believe...

SCHUMER: If we paid you unlimited money -- you know, we're not going to do that, but we could give you considerably more -- would you be able in more frequent cases when publicly these things are mentioned to be able to pursue them more thoroughly?

COMEY: Maybe, is the answer.

SCHUMER: OK. Well, I'd like to get a classified briefing from you or others on the details of this because it concerns me.

Second, the visa waiver -- the via program, not visa waiver. So let's just take a hypothetical. A non-American citizen has communicated on line and used, publicly, let's say, or now privately, I guess we could intercept them, but it's hard -- and used, you know, inflammatory words, language, intention. And they come here on a visa, and let's even assume now it's not in a visa waiver country. How often do we catch them?

COMEY: I don't think I can answer that sitting here. I don't know enough about -- I can't answer sitting here.

SCHUMER: Do you think we should know that?

COMEY: Well, I'm sure somebody does. We could get you an answer in a pretty good way terms of numbers.

SCHUMER: Because every -- after this hearing today, every American is going to be asking the question, how did this this woman come in a visa, fiance visa, I think it's called, I-K or K-1.

COMEY: K-1, I think.

SCHUMER: ... K-1, if she was talking publicly, again -- we'll get into privately in the classified briefing -- about jihad. Not this woman. Sorry. How could a woman -- strike this and use the word "A," or man, hypothetical.

COMEY: And again, assuming they're talking about it publicly...

SCHUMER: Yes.

COMEY: ... on an Internet forum or something?

SCHUMER: Yes. Shouldn't their -- that be somehow tied into our visa program?

COMEY: As part of the visa vetting process.

SCHUMER: Yes.

COMEY: Yes. I can't give you a good answer sitting here, frankly.

SCHUMER: No, but shouldn't it be?

COMEY: I don't know enough to say because I don't know exactly what investment would have to be made to do that work and what would be the payoff on the other side.

SCHUMER: Got it. Again, I'll pursue this further with you, both classified and non. And I thank you. My time is now up.

GRASSLEY: (OFF-MIKE)

CORNYN: Thank you. Thank you, Mr. Director. If the FBI had a telephone number from a known foreign terrorist and there were people in the United States making phone calls to that known number, there are procedures in place through the NSA and other agencies to check against that known terrorist number to see if there are telephone calls by Americans to that number.

Isn't that correct?

COMEY: Correct.

CORNYN: And it doesn't involve any content at that point, correct?

COMEY: Correct.

CORNYN: Congress just voted and the president signed into law a piece of legislation that prohibits the National Security Agency from maintaining the bulk telephone records. Does that -- does that develop entail greater risk or otherwise limit the tools available to the FBI to be able to discover those sorts of communications?

COMEY: I don't know yet because the USA Freedom Act framework is sufficiently new that I can't give you a high confidence answer on its effectiveness compared to what we used to have. In theory, it should work as well or better than what we used to have, but I don't know yet.

CORNYN: So it could entail more risk or no more risk?

COMEY: Correct.

CORNYN: You can't say?

COMEY: It could -- I just don't know at this point.

CORNYN: OK. I was shocked, as I bet a lot of other people were, particularly about your testimony with regard to encryption and its impact on the Garland shooting in my home state of Texas -- 109 encrypted messages that still today the FBI cannot gain access to. Is that correct?

COMEY: Correct.

CORNYN: And the only way you would be able to gain access to that, again, is not because you're monitoring private messages, it would be you'd go to court and show cause, meet the legal standard in order to get a court order to then give you access to those records.

COMEY: Correct.

CORNYN: And you said there are telecommunications -- there are phone companies, or I should say manufacturers, who are marketing their encryption as a way to gain market share in America, to advertise that these are private conversations that not even courts can order access to.

COMEY: I think there are device manufacturers who include that in their description of why their products should be used.

CORNYN: And you said encryption is part of terrorist tradecraft, correct?

COMEY: That's for sure.

CORNYN: To me, that's a staggering situation because it still persists today, correct?

COMEY: Oh, yes. And growing.

CORNYN: And so while we were all horrified and repelled by what we saw in San Bernardino and what we saw in Paris, there could well be similar communications -- not in those cases, but in other cases -- going on today, and the FBI would not be able to gain access to those communications between terrorists, even with a court order.

COMEY: That's correct. And strongly encrypted, end-to-end encrypted, even if a judge issues an order, if we intercept it, it's still encrypted and unreadable.

CORNBYN: Do you consider that a danger to the American people? Does that increase the risk of terrorist attacks that could go undetected before the carnage occurs?

COMBY: I do, which is why we've been talking about it for the last two years so much.

CORNBYN: Well, I appreciate very much your making this important point. But it concerns me a lot that Congress has not acted to do anything to give you the tools that you need. I appreciate the way you've tried to discuss this with the various manufacturers and other entities involved, but it strikes me as if they're gaining market share by advertising their encryption and saying that not even the federal government in a terrorist investigation can gain access to it, that that's a real problem.

And so I think you said you hoped to get to a place where the companies can comply with a court order. But do you think it would be useful for the Congress to actually try to do something about this, or should we just wait for the voluntary compliance by the industry?

COMBY: I think it would be useful, as Congress has done, for Congress to try to drive this conversation, to ask -- to draw people into it to figure out, So what can we do, because I don't want to hurt American business, but I also have a responsibility to try and protect the American people. And all of us care about the same thing. So I appreciate Congress trying to drive this conversation.

CORNBYN: Well, I think your testimony here today will help do that. I think it's surprised and shocked a lot of people.

I want to just close on this line of questioning, Director Comey. We're at a point in our nation's history where the public doesn't trust government. I think a Pew poll indicated less than 20 percent of Americans say they trust their government most of the time. And unfortunately, many Americans have lost faith in our national institutions, including our justice system.

And that's -- I know how much you care about that and how much you've dedicated your life to making sure that people can trust law enforcement and our justice system. That faith is endangered when attempts are made to pervert it in favor of the powerful who would like to create different rules for those who rule.

I know this is a sensitive matter, and I'm not going to ask you about the content, but I know the FBI is currently investigating the private e-mail server of the former secretary of state. And it's troubled me, and I know others, when some people have attempted to disparage or otherwise predict the outcome of the ongoing FBI investigation.

I know the president himself said that we don't get an impression that there was a purposely (ph) efforts to hide something or to squirrel away information. Does the president get briefings on ongoing investigations by the FBI like this?

COMBY: No.

CORNYN: So he would have no way of knowing what the status of the FBI investigation is.

COMEY: Certainly not from briefings from the FBI.

CORNYN: I know a former senior official at the FBI and the current president of the Law Enforcement Legal Defense Fund told The New York Times that injecting politics into what is supposed to be a fact-finding inquiry leaves a foul taste in the FBI's mouth and makes them fear that no matter what they find, the Justice Department will take the president's signal and will not bring a case.

But I just want to ask you to perhaps repeat something you said earlier, when you said that people at the FBI, including you, don't give a rip about politics. Is that your position?

COMEY: That is true through and through the FBI.

CORNYN: So for politicians of whatever level, whether it's the president of the United States or members of Congress or anybody else trying to lobby or intimidate or influence an investigation by the FBI, that does not work, at least under your leadership.

COMEY: It doesn't matter. I don't want to hurt anybody's feelings, but it doesn't matter what anybody thinks or feels about our work. We are competent, we are honest, and we're independent. We're going to do or work the right way, and we care only about the facts. That's who we are.

CORNYN: Well, that's certainly consistent with the way you've conducted yourself, I think, in your public life. And I think that will help restore in some small part people's confidence that there are people trying to do the right thing for the right reasons. So thank you very much.

COMEY: Thank you, Senator.

UNKNOWN: (OFF-MIKE)

KLOBUCHAR: Well, thank you very much, Mr. Chairman.

And thank you, Director Comey, for being here. I really appreciate it.

One of the things that we haven't gone into as much is the on-line recruiting of terrorists. Minnesota, as you know, has been very aggressive, our FBI and our local law enforcement, our U.S. attorney, Andy Lugar (ph), in going after cases of people who have been recruited, much of it on line -- not all of it, but much of it -- to join ISIS or before that al Shabaab. And I've seen these recruiting techniques myself. Your agents have shown them to me.

And I wondered what is being done about that. And you know, it may have played a role -- I know the investigation is still going on into the tragic shooting in San Bernardino, but what -- is this an emerging threat? What can be done? There's been discussion about getting the companies to take down these sites as much as possible. And just talk about a little bit about that.

COMNEY: Thank you, senator. ISIS tries to crowd source terrorism. They obviously, as we talked about, aspire to send operatives here. We as a country have made that very, very hard, although it's something we focus on a lot. And so they also try to inspire people to kill on their behalf.

They send a message in a very slick way that resonates with troubled souls, with people who are unmoored and seeking meaning in their life, kids a lot of times, or older people who have struggled in some way. And it is a very, very seductive message that by virtue of its quality and its quantity has a huge impact on the troubled mind because it's buzzing all day long, that these people can consume this.

And their goal is to draw folks into this closed circle on line where they're constantly bombarded with, This is the way to meaning, This is the way to meaning. And that shapes a troubled mind.

And so what we try to do is make sure we are aggressively investigating that to find those that are on that path, consuming and potentially radicalizing, and then work with a whole lot of other folks to try to help kids who might be vulnerable to it, and not just to their poisonous message but to all kinds of poisonous messages that inspire people to violence.

So we're about to come out with something called "Don't Be a Puppet," which is a -- I'm no judge of what's cool, but I'm told this is cool, almost like an on-line game for schools that kids learn, this is the way they come after you and here's how you resist it, whether it's al Shabaab or ISIL or some domestic extremist group. Those are the two ways we try to attack it.

KLOBUCHAR: Very good. And as you know, we have one of the sort of pilot projects on the Countering Violent Extremism group and have been used with our Muslim community, which we're very proud of in Minnesota, has been working to try to prevent these kids from getting involved in this in the first place. And I really appreciate the work that you're doing and I just encourage you to do more. We need more funding. We're hoping we can get some out of this budget for these projects to fight Islamic extremism. So thank you for that.

I know that Senator Flake asked you about cooperation with local law enforcement and heard you bring it up in your initial statement. Do you think they have enough resources to deal with what we are -- Senator Mikulski and I are introducing the COPS bill again to try to increase funding there. But could you talk about that?

COMNEY: Our state and local partners are strapped across the country, coming out of the painful cuts they've endured over the last eight years. And so they are still contributing their stars to our task forces. But I know what it costs them, because they're short handed across the country.

I -- I travel to our field offices. I've been to all of them once, now I'm almost halfway through the second time. Every visit, I talk to state and locals, and I hear this over and over again: they're asked to do more and more with less.

They're trying to become better at community policing. That's very hard when you're having to have officers cover twice the -- the territory they used to cover. They don't have time to get out of their cars and meet people. So it is a -- a constant theme I hear from our partners.

KLOBUCHAR: Thank you. And I -- I wanted to add -- a lot of my colleagues have asked you about encryption, and I know you were here before and talked about efforts to try to work with the phone companies.

I thought your testimony was very interesting today when you talked about the fact that some of us suspect it may not really be a technological issue as much as it is a business model issue.

But -- so, if that is all the case, and what -- what has been done to improve it since that time? Has there really been changes, except for discussions with the phone companies?

You said, in answer to one of the questions, that a good chunk of it could be resolved. How would we resolve that? Is it just simply the international norms you talked about, where you would have agreement between countries to when their -- our court orders, their court orders could be followed?

I'm just trying to get to a solution here as soon as possible. I keep waiting for the next ticking time bomb of something where -- you know, our law enforcement isn't able to access this. And as you know, it's domestic, as well. It's not just terrorism investigations.

Cy Vance has made this a crusade, going around, talking about the problem in again (ph) cases and some of the others. And I just remember, as a prosecutor, sitting in on wiretaps, seeing that kind of information. These were the old days, when people were using land lines or less sophisticated cell phones, and it was a major part of our investigations.

COMNEY: I think a big part of the problem can be solved if folks who are currently producing and selling devices that can't be unlocked by judges' orders or -- or communications that can't be intercepted by judges' orders were to change their business model in this respect, not to give us a key.

I don't want a key. I don't want to tell them how to do their business. But figure out how they could change their model so they comply with judges' orders.

As I said in my testimony, I actually don't think that's a technical problem. The -- the folks making the phones today, they were doing that a year ago, and nobody said their devices were insecure, so we ought not to buy them.

And so I'm hopeful -- I mean, I'm an optimist. I'm hopeful that people, now that they consider how big the threat is, will consider those changes and get us to a place where we can address a big chunk of it that way.

It's not gonna solve the entire problem, and I agree very much that you don't want to just chase the problem offshore, and so there does have to be an international component to this.

But a big start would be people acknowledging it's actually not a technical problem. We've chosen to operate our business this way -- for good reasons -- but that -- but we should stop

saying, "you're going to break the Internet if you ask us to do this" or "the director of the FBI wants to stockpile keys."

No, I don't. I don't want the key to anybody's house. You should figure out, when a judge says there's something in your house that this nation needs to be safe, you figure out how to come out of the house.

Use a window, use a door, use a slot, whatever keeps your house safe. We should not tell you how to do it, but we should get to a place where, when a judge says, "this is necessary," you are able to comply.

KLOBUCHAR: And you're talking here about court orders, and you're talking about an international norm, given that the world has united against ISIL and this kind of other terrorist evil, so some way that we can find international agreement on when this information is given in the -- to pursue these very important investigations.

COMEY: Yeah. I think reasonable people have said that's a part -- that should be a part of it. And I think they're right.

KLOBUCHAR: Great. Thank you very much.

HATCH: Thank you, Senator Klobuchar.

Mr. Director, we're really happy to have you here today, and I want to, firstly, express my gratitude for the work that you're doing, the work you have done in the past, and for the good way you approach law enforcement in this country. You're doing a great job.

Last week's tragedy in San Bernardino was the worst terrorist attack on American soil since 9/11. Now, the shooters claimed allegiance to ISIS, and ISIS has called them its followers.

I think it's important to call this attack what it is. Do you agree with me that this was an act of terrorism?

COMEY: Yes.

HATCH: Do you agree that it appears this terrorist attack was at least inspired by ISIS?

COMEY: We're still sorting that out, Senator. It was definitely claimed by the killers, at or about the time of the killing, that they were doing this on behalf of ISIL, and ISIL, then, has embraced them as followers. There's more work to be done to understand the motivations more clearly.

HATCH: (inaudible) hard to not say that ISIS had something to do with it.

COMEY: Right. ISIL inspiration may well have been part of this.

HATCH: Sure.

COMEY: But -- but these two killers were starting to radicalize towards martyrdom and jihad as early as 2013...

HATCH: I agree.

COMEY: And so, that's -- that's really before ISIL became the -- the global jihad leader that it is.

HATCH: Right. Within 24 hours of this terrorist attack, the attorney general stated that her, quote, "greatest fear," unquote, was the possibility that it could lead to an anti-Muslim rhetoric. And after 130 deaths in -- by ISIS in Paris and 14 dead Americans last week, my greatest fear is not rhetoric.

I mean, in all honesty, my greatest fear is more attacks and more dead Americans. If we were to put it this way, what would be your greatest fear after last week's terrorist attack?

COMEY: My -- my fear, which is not new -- it's been a feature of my work since I started this job -- is what don't we know, what can't we see. And that is the particular challenge of those radicalizing online, consuming propaganda, and trying to stay beneath our radar.

This confirms to us what we've said all along, as have many other cases. The reason we have cases in all 50 states is it is a very real concern that people are radicalizing in a way that's hard to see. That inability to see is my biggest worry.

HATCH: Well, I share that. Let me just say this. I'd like to follow up on Senator Lee's line of questions, regarding the so-called "dark problem."

I have two questions. First, with respect to control of encrypted data, U.S. tech companies do not want to be the middleman between law enforcement and technology customers.

How do you -- how do you reconcile this concern with the needs of law enforcement? And have you considered alternatives that would meet the needs of law enforcement, but not put the United States tech companies in the awkward position of middleman?

COMEY: I'm not sure I know exactly what they mean by middleman. I don't want anybody to be the middleman for law enforcement. But everybody in the United States has an -- I believe, an obligation to endeavor to comply with judicial orders in criminal investigations, whether you're a bank or you run a sandwich shop or you run a technology company.

And so I don't want anyone to be the middleman, but I want everyone to be in a position to comply with judges' orders. That's what the rule of law is about.

HATCH: Thank you.

Secondly, U.S. tech companies are not the only businesses that offer encryption to -- to countries -- to customers, rather. Businesses in other countries offer it as well.

Now, if we require U.S. tech companies to provide decryption keys, won't users simply look to technologies from other, non-U.S. companies to conduct their activities? And -- and how do you respond to that concern?

COMNEY: Yeah. That's a serious concern. First of all, I don't want anyone to supply encryption keys. But if we went to a place where American companies were required to figure out a way to comply with judicial orders, they do make a serious argument that what that would do is chase our business overseas.

I'm not in a position to evaluate that argument. A little part of me is skeptical that people would stop buying the great phones we make in this country because a judge might order access to it. But -- but I'm not really an expert on that.

So I do think a part of this has been an international compact of some sort. None of us want to hurt American business. But at the same time, there are costs to being an American business, right? You can't pollute. You can't employ children. There are certain things we've decided, as a country, we want to govern ourselves this way.

And so, in a way, I think we have to figure out what's right for America first, and then try and figure out how to reduce the harm that might come competitively.

HATCH: OK. I'd like to turn now to the issue of rapid DNA. Last week, I introduced bipartisan investigation with Senators Feinstein, Lee, and Gillibrand to update our nation's laws to take account of this exciting new technology.

Now, rapid DNA devices -- they're self-contained, they're fully automated instruments that can be placed in booking stations, and they can both develop a DNA profile from a cheek swab and compare the results against existing profiles in less than two hours.

Now, my bill, the Rapid DNA Act of 2015, would allow law enforcement officials using FBI-approved rapid DNA instruments to upload profiles generated by such devices to the FBI's Combined DNA Index System and perform database comparisons.

Director Comey, you've spoken in the past about rapid DNA and how this technology will help law enforcement. Do you believe that rapid DNA technology is important? How will it impact law enforcement? And do you believe Congress should pass legislation authorizing its use within standards and guidelines promulgated by your agency?

COMNEY: That authority that's in your bill would help us change the world in a very, very exciting way. That -- allow us, in booking stations around the country, if someone's arrested, to know instantly -- or near-instantly -- whether that person is the rapist who's been on the loose in a particular community before they're released on bail and get away, or to clear somebody, to show that they're not the person.

It's very, very exciting. We are very grateful that we're going to have the statutory authorization if that passes to connect those rapid DNA technologies to the national DNA database.

HATCH: Well, thank you. My bill, the Rapid DNA Act, will not affect when or under what circumstances law enforcement collects DNA samples. These decisions would be governed by state or other federal law. What it will do is affect where samples are processed and how quickly they're processed.

Now, Mr. Director, what would you say to individuals who may be concerned that rapid DNA technology will raise privacy concerns? And what would you say to individuals who may be concerned that this technology could affect the integrity of FBI's combined DNA index system, or CODIS? And I would note that my bill restricts access to CODIS to FBI-approved rapid DNA instruments operated in accordance with FBI-issued standards and procedures.

COMEY: First, you said it well, Senator. Folks need to understand this isn't about collecting DNA from more people. It's about the DNA that's collected when someone is arrested being able to be analyzed much more quickly. That can show us in some cases this is the wrong person or can show us in some cases this is someone we have to be very worried about.

That is good for our justice system as a whole. And you're exactly right. The national database, the CODIS database, is the gold standard. This legislation does not make it any -- water-down the standards that are applied before a DNA result can be pressed against that database. We're still going to have high standards. We're still going to require that this is the gold standard for identification in the United States.

HATCH: Well, thank you, sir.

Senator Franken is next.

FRANKEN: Thank you, Mr. Chairman.

Director Comey, first I'd like to thank you for appearing today. It's good to see you again and you do a great job, I think, as all the members of this committee agree.

Before I turn to my questions, I -- I want to extend my thanks to the bureau and to you and to your agents for assisting in the federal civil rights investigation surrounding the death of Jamar Clark in Minneapolis. I supported the decision of Mayor Hodges and Police Chief Harteau to call for an independent investigation.

In my view, a full, thorough and transparent accounting of the facts is necessary to get to the bottom of what happened in that tragic event and to restore trust between the north side community and the police and law enforcement. So I want to commend the FBI agents involved for their professionalism and for their commitment to seeking justice.

I wanted to just -- a lot of things have been discussed in this committee, including the going dark -- the encryption issue. And I just want to make sure that I have clarity on this, and maybe help other people clarify it for them.

Basically, tell me if I heard you right, that a terrorist in the United States could -- that there is a sort of distinction between -- there are two distinct related concerns that law enforcement has about encryption -- concern that the information sought by law enforcement is on an encrypted device -- we're talking about the phone; and the concern that encrypted -- that the information might exist within an encrypted app on that phone. And so, some of these apps are -- are available freely online and add an extra layer of encryption.

Can you speak to the bureau's concerns related to these issues? You're basically saying that there are sort of these two layers, and if you get rid of the first layer, you'll have more -- I mean, you'll obviously be -- be -- it will be a great deal more people that won't be caught up or that won't have that encryption. Is that what you're saying?

COMNEY: Yes. I think that what has changed -- encryption has always been available, always been available to the sophisticated user. "Always" meaning for decades. What changed over the last two years is encryption went from available to being the default. And so now, with some of the leading phones in the United States, that phone is encrypted by default.

So if we recover it at a crime scene, with a judge's search warrant order, we cannot open it. It's been designed that way.

FRANKEN: And I know you're not asking for a key. You're asking for the company to be able to follow the judge's order.

COMNEY: Right, which they could do. Two years ago, they could do it and did it routinely. And I think their devices were still considered pretty secure. But you're exactly right, there may still be within that device, especially for sophisticated users, other encryption tools that are on particular apps, or there's actually something too complicated.

FRANKEN: I -- can we get some data on this? I mean, last time we looked at this -- this committee looked at this, we had Deputy Attorney General Yates. And I asked her for more information about the scope of law enforcement's concern. Because I know there's -- a lot of this is about just normal crime, and not about terrorism.

And I think what you're suggesting is that a terrorist might be able to get that app, and that's why -- that foreign app -- and that's why we need an international agreement on this. Right?

COMNEY: Yes. I think this is -- you're exactly right. This is mostly a law -- a local law enforcement issue. But we are gathering the data that you asked for, and I'll have to get back to you on exactly when we're going to get it to you.

FRANKEN: And I know that you've mentioned it. OK.

COMNEY: Yes.

FRANKEN: I want to make sure I'm clear on something else from this testimony. I'm just sort of reviewing the whole day for myself. I understand if someone on a terrorist -- terrorist watch list tries to buy a gun through a licensed dealer, the FBI is alerted.

COMEY: Correct.

FRANKEN: And it can delay the sale for three days?

COMEY: That's -- under the law, we're allowed up to three days.

FRANKEN: So, OK. But ultimately, do you have legal authority to deny the sale?

COMEY: Not unless there's another prohibitor under the law -- (inaudible) or mental defective.

FRANKEN: OK. So at least you have that three days.

COMEY: Yes.

FRANKEN: If someone on a terrorist watch list -- this is someone on a terrorist watch list, in three days, if there's no other -- other indicator, they can get their gun. That, to me, is a problem.

Now, if some -- and -- and if someone on a terrorist watch list tries to buy a gun online or at a gun show, no one is legally required to notify the FBI.

COMEY: I believe that's correct. Yes.

FRANKEN: OK. So I have that correct.

So, to fix this, we're talking about keeping guns out of the hands of people -- of terrorists, and presumably people on the watch list are there for a reason, or maybe there's a false positive.

But it seems to me that we would have to be doing both -- having -- if we're really interested in keeping the guns from terrorists, we would have to enforce both; say you can't sell a gun to someone, or there has to be three days or some kind of look at that person; and also the gun -- the gun sale, the -- the sale at a gun show, the gun show loophole would have to be solved, too.

I mean, in other words, if -- if we're worried about guns falling into the hands of people on terror -- terrorist watch lists, we also have to close up the gun show loophole, as well as cleaning up this loophole, which is the terrorist watch loophole.

I mean, this -- in other words, this is a reason to do both, in my -- let me put it this way. You don't have to answer. This is the reason to do both.

OK. Thank you.

HATCH (?): Senator Perdue?

PERDUE: Thank you, Mr. Chairman.

Director, we're lucky to have you. Thank you for the sacrifice you make in doing what you do. I'm glad you're on the wall.

I'd like to go back and clear up, just to make sure I understood the testimony today as well. I applaud the FBI for being the first to call this an act of terrorism. Not that I want it to be an act of terrorism, of course, but you guys looked at the facts and said the American public needs to know the facts. Thank you for that.

But I'm a little confused. An act of terrorism -- I haven't heard today it connected directly to ISIS. Are you -- at this point, I know in this environment you may not be able to talk about that, and if not, that's fine. Can you talk about that? Do we have evidence that this was directly connected to ISIS's influence in the U.S.?

COMEY: There was some indication that they were, at least in part, inspired by ISIL, so yes. We're trying to sort out the -- what other contributions might there have been to their motivation. And we may never fully sort it out, because human motivation is hard. But at least in part, we see an ISIL inspiration.

PERDUE: So -- and may not want to comment on this either, and I apologize for asking these direct questions, but in the past, just -- just for the American people and for -- for Congress, the FBI has been a stalwart in helping to protect the American people over time.

In the past, and in -- on your watch, are you aware of planned attempts that have actually been preempted by the FBI that -- that we may never know about?

COMEY: Yes, many.

PERDUE: OK. Thank you.

And -- and speaking to the increase in the -- the -- the latest spate of ISIS attacks, is their planning getting better? Are their tactics getting better? Are their networks expanding?

I know that the Malik and Farook -- Farook team bought their weapons through a neighbor. My question is, is there a network issue here, and are -- are the networks growing in the U.S.?

COMEY: We're looking at -- obviously in San Bernardino to see, was there anybody else involved in assisting them. And so, separate from San Bernardino, we have not seen this. We have not seen ISIL cells or networks in the United States.

So far as we can tell, they have not succeeded in penetrating our borders with their operatives. That's an aspiration of theirs, we gotta worry about it all day, every day.

But instead, what they're doing is motivating individuals or very, very small groups of people to commit murder on their behalf. That's the crowdsourcing phenomenon we've been dealing with.

PERDUE: Well, thank you.

Can you confirm that ISIS adherents have attempted to gain access through the refugee -- refugee resettlement program? Do we actually have cases where, through the resettlement -- I think there are 2,200 people or so that have come in so far, and we're trying to bring another 10,000 in in the first phase of this. Have we actually had cases where we identified ISIS adherents in that first group?

COMEY: Not to my knowledge.

PERDUE: Are you aware that Canada is increasing their Syrian refugee acceptance rate from less than 5,000 to over 25,000, the latest number I saw? And with the border that we have with Canada, we don't talk about that border much.

Is the FBI aware of that? Are they paying attention to that, relative to what we need to do? To me, that's -- that vetting at Canada -- in Canada is just as important as our own vetting here, with our K-1 and our visa waiver program.

COMEY: Yeah. And they get that. The head of the RCMP is a friend and colleague of mine. He called me to tell me their government had made that decision, and to explain and to encourage us to work together to vet those people.

PERDUE: And what changes would you like to see in the K-1? I know with (inaudible) -- was -- Malik, was she actually given an interview in the K-1 process? Do you know -- do we know that?

COMEY: I don't know well enough to say at this point.

PERDUE: OK.

COMEY: I know the process requires it. We're still trying to fully understand exactly all of her contacts.

PERDUE: Are there changes you would like to see, the FBI would like to see, in the K-1 program or in the visa waiver program?

COMEY: I don't know enough yet to say, as a result of this case.

PERDUE: OK. And the last thing, real -- very quickly, in the Trans-Pacific Partnership, there is language in there that would prevent national laws being implemented in -- in countries that would require manufacturers to provide access to products and encryption technologies.

Some critics think that that would limit our own ability to -- to provide legislation that would give you a solution to the potential go-dark solution. Do you -- does the FBI have a point of view on that yet?

COMEY: We don't.

PERDUE: OK. Thank you, Mr. Chairman. Thank you, director.

GRASSLEY: (OFF-MIKE) Senator Blumenthal, and then Senator Coons, and, if you can stand me for seven more minutes, I have a second round of questions.

BLUMENTHAL: Thanks, Mr. Chairman. And thank you, Director Comey, for your excellent work and your great service to our country. Thank you to your family, and most of the especially to your wife, Patrice, who has done so much for the children of Connecticut, and now for others around our country.

I've just come from...

GRASSLEY: He's from Iowa, too.

BLUMENTHAL: Thank you, Mr. Chairman, for that correction.

I've just come from a hearing at the Armed Services Committee, where Secretary Carter was testifying. And I want to first make the point that we often thank our men and women in uniform, which I do readily and repeatedly, and I do again now.

But I also want to thank the very brave men and women who work under your command, who enforce our laws and help to keep us safe, along with all of our law enforcement men and women around the country, police at every level, and are, in a sense, also at war.

In fact, Secretary Carter said, and I'm quoting, talking about ISIL, "the reality is we are at war." That's how our troops feel about it, because they're taking the fight to ISIL every day, applying the might of the finest fighting force the world has ever known.

Do you feel that we are at war, also, within our borders against forces of terror that are linked to those forces abroad that our men and women in uniform are fighting?

COMEY: Very much, Senator. And our people feel that passionately. Our people are tired. I mean, we are working very, very hard. They're working very, very hard.

But what motivates them is, these people want to kill our people. We are at war with these people. And so stopping them is what -- is -- is the reason we do this work.

BLUMENTHAL: And the president well identified this new phase that, perhaps, is an old phase in larger scale: the phase of ISIL and ISIS reaching outside the theaters where they have fought so far, reaching into this country -- you've referred to "crowdsourcing" as the San Bernardino experience -- and outsourcing that threat to new recruits, to home-grown radicals, may be part of the threat here.

But you would agree that we face a war every bit as dire and dangerous here at home as we do abroad?

COMEY: Yes. The -- the threat, obviously, and the density of the -- of these savages is less here in the United States. But the -- the nature of it is very similar.

BLUMENTHAL: And I know that you've responded about the importance of cooperation in terms of information and other kinds of assistance that is provided by members of the Muslim community.

Just as cooperation and support is essential from nations that have a majority of Muslims abroad in our fight against ISIS and ISIL, they are our natural allies and friends and partners in this fight against extremist terrorism and violence abroad.

And I want to ask you about some of the statements that are made about closing borders and about religious tests at our borders, other kinds of religious tests that, in my view, are unconstitutional, but also strike me as unwise because we need that cooperation.

Are the statements themselves potentially inhibiting that kind of cooperation and support and help that we need?

COMEY: Thank you, Senator. I -- I'm -- I don't want to comment on anybody's statements. But -- but I can make, I think, the -- the point that you're interested in.

ISIL is trying to recruit -- recruit in Muslim communities. They're trying to motivate people who may be of the Muslim faith, who are unmoored in some way, to -- to -- to become part of their poisonous endeavor. The people who so often tell us about people like that are other Muslims who help us.

And so we've worked so hard over the last 15 years to build relationships of trust that allow us to find out who might be trouble and to stop it. That's in everybody's interest. And anything that gets in the way, that erodes that relationship of trust, is not a good thing.

BLUMENTHAL: And Muslims who live in our nation are fellow Americans, many of them, equally interested in preventing threats and violence as anyone of any religion.

COMEY: Our experience, they are -- what's wonderful about this country is we're incredibly diverse. They are part of that diverse polyglot, and they love our country, which is why they help us when there's a killer in their midst, or someone on the path to being a killer in their midst.

We have to continue this. As I said in the beginning, we're all in this together. We need each other.

BLUMENTHAL: Well, I -- I applaud your very clear and emphatic, unequivocal statement about that point. I want to shift to another terrorist act -- at least one that strikes terror, not of the same motivation, but involving the apparent racist-motivated violence in Charleston.

The FBI background system known as NICS was applied in the case of Dylann Roof's purchase, but only too late to prevent him from buying a gun.

The 72-hour loophole that I have tried to close enabled him to walk away with a gun that he sought to purchase. Thanks to that loophole, after the 72-hour period, since the background check was not completed, but would have precluded him from buying a gun, he was enabled to have that firearm.

Gun retailers have sold 15,729 guns in the last five years to individuals who were not legally allowed to purchase them. And about five months ago, I think you commissioned a study that was to last 30 days, to examine how Dylann Roof was able to buy that gun.

I think that report would help us in Congress to understand what went wrong and how to fix it. And most especially, if the 72-hour loophole enabled him to buy that gun, as appears to be from the facts that we have been told so far, the report would be very helpful.

So, my question is, can you update us as to the status of that report?

COMNEY: Certainly, Senator. And we'd be happy to get you a detailed briefing on it because the work was done, as I asked, in 30 days. And it did two things. It confirmed the facts as we understood them close to the murders in Charleston, that there was a mistake made by our processing clerks that was compounded by a mistake in the records of the South Carolina jurisdiction where he would have been -- where the prohibitor came from. And so that confirmed what we knew.

What it most importantly told us is: How can we get better? The law is what the law is. We have three days to process these thousands and thousands and thousands of them. And so we're working on a number of things to get better.

One, to improve the records that are put in by state and locals; to improve our technology; and to surge resources. The number of gun purchases continues to climb. It's climbed dramatically in the last week. We've got to make sure we have enough folks. If all we have is three days, we've got to make sure we have enough folks to do that.

And so those are the three buckets: better records; better technology; and more importantly, more human beings on the phones to process them more quickly.

BLUMENTHAL: So resources are really important -- resources in technology; resources in people; and resources in records that you depend on because many of them come from state and local authorities as well.

COMNEY: Correct.

BLUMENTHAL: My time is expired. This whole area is tremendously important. I want to thank you for being here today, and just to clarify racial and religious supremacists often use terrorist-type tactics, even though we would not call them terrorists today. But I appreciate the

attention that you're giving to the potentially white supremacist-motivated acts of violence in that church in Charleston.

Thank you.

GRASSLEY: Senator Coons?

COONS: Thank you, Chairman Grassley.

And thank you, Director Comey, for your service and for your testimony before this committee today.

I was very pleased to see in your testimony before the committee a focus on the violence reduction network, a Department of Justice initiative that is truly helping a group of now 10 smaller cities, like my home town of Wilmington, Delaware, that have seen a dramatic rise in violent crime and in homicides.

We are sadly on track for a record year of shootings and homicides, and I'm grateful for your focus and for the FBI's focus on providing technical and investigatory resources to help state and local law enforcement deal with this rise in violent crime in a few cities, and to learn from the policing examples of other communities and federal agencies that have real knowledge about how to better deploy investigatory resources.

So, tell me, if you would, how we can better support valuable programs like the VRN? And how, in your view, it's been most effective in connecting FBI resources to cities like Wilmington, Delaware?

COMEY: I'll start with the effectiveness point first. I think what makes it special is we bring together in a place like Wilmington everybody who cares about this issue or might have a specialty that's useful. And where I think we can bring a lot to bear is our understanding of technology and our analytic resources so that we help a local jurisdiction understand what is the pattern, what is the trend, and what are the pieces of information that we can lawfully gather that would be useful to you in -- inn focusing on it, because it's almost always small groups of predators, finding them and ripping them out of the community.

And that is a -- it's not rocket science, but it often brings rocket science -- rocket scientists to the fight in a really important way. I think the way you can support it is, as you just did, talking about its value and making sure that appropriators and others understand that when the department talks about this, it's making a difference.

COONS: Yes, thank you. I am an appropriator on the relevant subcommittee and have advocated for it with the head of OMB and the attorney general, but would be grateful for any other advice or insight you would care to offer about how we can sustain it, make it more effective.

Certainly, the work to reduce violent crime is far from over in my home town and in the nine other cities around the country. And I'm hopeful we'll sustain this program until we see some significant reduction in violent crime.

I'd like to mention another issue, if I could, about cybersecurity. The Senate recently passed the Cybersecurity Sharing Information Act, which permits DHS to scrub personally identifying information it receives from private entities, but only after it secures the approval of a number of agencies, including yourself in your role as director of the FBI.

Have you had any communications with other agencies yet about how this process will work? And are you committed to ensuring that DHS can actually conduct a robust scrubbing of personally identifying information?

COMNEY: We have -- I have not had any conversations about that. But the second part is easy -- we'll do everything possible to make sure that it works and works the way Congress designed it.

COONS: Well, thank you. I -- I'd urge you to engage in those conversations. I think this process is going to move relatively quickly, or so I hope.

In October, President Obama secured from President Xi of China a striking landmark admission that China had been engaged in economic espionage -- cyber attacks, something you've testified about here before -- and a commitment that those attacks would end. Yet, press reports suggests that literally a day after President Xi's visit, Chinese cyber attacks resumed.

Has the FBI detected any change in Chinese cyber espionage behavior following President Xi's promise? And what do you recommend in terms of action by the Senate to try and address this ongoing challenge to our nation's innovation and inventions?

COMNEY: It's too early to say. We're watching it very, very carefully. Given the long-tail nature of Chinese cyber espionage and theft, even if -- I'm not sure that I would expect a change, even if one was going to happen, that would be visible yet. And so we're watching this space very carefully.

We've had good conversations with our Chinese counterparts. I've told them -- I don't mean to be rude, but the FBI director is paid to be skeptical. I'm deeply skeptical. And so we will have to watch and see what the facts show us. But I can't say yet.

COONS: I think it's deeply disturbing and hostile behavior that we need to continue to be engaged. I've heard from far too many American companies that they've lost vital both economic secrets and from some federal agencies that they've lost vital national security secrets. And I appreciate your hard work on this.

Last, I'm the ranking member of the Oversight Subcommittee. And last month, we held a hearing at which DeKalb County Police Chief Cedric Alexander, who is himself a 30-year law enforcement veteran, testified that the notion that there is a so-called "Ferguson effect" is of no real significance. I was struck at that hearing, which Chairman Cruz called under the title "A

War on Police" -- that hearing actually produced no evidence that there is any meaningful organized war on police.

And as the co-chair of the Senate Law Enforcement Caucus, I know that law enforcement faces real challenges nationally every day. But I see little evidence to suggest that these issues stem from the calls of some in the civil rights community for greater accountability. In fact, my experience at the local level was that police officers are some of the greatest advocates for accountability because it makes them more effective police officers.

So, is it your view that the protection of American civil rights is actually inconsistent with good policing and officer safety? Or do you see them as being fundamentally in harmony?

COMNEY: Oh, they're fundamentally in harmony. Scrutiny and oversight and accountability are good for everybody -- law enforcement and non-law enforcement.

COONS: Thank you, Director. It's my view that in a democracy, the enormous power that we give to law enforcement and the very high expectations we have for them are only strengthened by accountability that then produces community engagement, community support. The agency I was fortunate enough to be closely associated with for a decade really was an early national leader in community policing and did I think an outstanding job at winning the trust of our community, and thus being effective at policing.

And I think there's a lot of work to go in terms of accountability and engagement and protecting civil rights, but I appreciate your response on all four of the questions I've asked today, and I'm grateful for your service.

Thank you, Director.

COMNEY: Thank you, Senator.

GRASSLEY: I've got three questions I would like to ask, and then, I -- I assume everybody's asked questions once, that nobody will come back.

I -- I want to start by underlining what Senator Cornyn said about the Clinton e-mail investigation. Almost a thousand e-mails containing classified information were transmitted through and in the non-government server system.

A former I.T. specialist at State Department, who also managed the private server, has avoided this committee's questions by relying on the Fifth Amendment right of self-incrimination, and in the course of the FBI's investigation, there might come a time when it refers the matter to the Department of Justice for prosecution of some of the individuals involved.

But, as you know, no matter what the FBI finds, a political appointee at the Justice Department will ultimately make the decision whether or not to prosecute. That's why some have called for a special counsel (ph) to be appointed for an independent decision.

So my question is, if the FBI refers the matter to the Justice Department, but the Justice Department refuses to prosecute, the public will not learn the facts that the FBI independent inquirer established.

So would there be a process by which you would inform the public of what the FBI learned, and what you do if the decision not to prosecute appears to be improperly influenced by political considerations?

COMEY: Mr. Chairman, I'm not comfortable answering a question about what might happen in that particular matter. I think it's important that I make sure I'm -- I'm making sure it has the right resources, the right people, and it's done in an expeditious, fair, and -- and competent way.

I don't want to speculate and down that road, if I could.

GRASSLEY: Could I remind you that, in the anthrax case, after the person that was suspected committed suicide, that the FBI did make that investigation public? So wouldn't there be a precedent for you making your investigation public?

COMEY: There's a variety of precedents for, in investigations, describing some or all of it to the public. I just don't want to start to speculate on this particular investigation.

GRASSLEY: OK.

State Department -- along the same lines, State Department officials have informed my staff that the FBI has seized or taken possession of the State Department computer used by the witness who was asserting the Fifth Amendment to this committee.

There has also been a public report that the FBI has taken possession of State Department e-mail servers. Is that correct? Has the FBI seized or taken possession of these State Department computers?

COMEY: I can't comment on that, given that it's an ongoing matter.

GRASSLEY: I'm not really asking you if -- what -- what this serves. I'm just asking you, do you have these tools available.

COMEY: Well, If I were to answer, I would be answering about what evidence we've gathered in an investigation.

GRASSLEY: OK.

COMEY: I -- I can assure you...

GRASSLEY: You don't need to go any further.

COMEY: OK.

GRASSLEY: That's -- I trust you.

COMEY: Yeah.

GRASSLEY: The American people rely upon you to investigate potential criminal conduct, and -- and in the course of that conduct, politics cannot interfere with your responsibilities.

In a 60 minutes interview, President Obama declared, in response to a question about Secretary Clinton's use of a private server, quote, "I can tell you that this is not a situation in which America's national security was endangered," end of quote.

How can you assure the American people that you will not let the White House influence the FBI's inquiry?

COMEY: I hope the American people know the FBI well enough, and the nature and character of this organization, to know, as I've said many times, we don't give a rip about politics.

Anybody's view about an investigation they're not involved in is irrelevant. We care about finding out what is true, and doing that in a competent, honest and independent way. I promise you, that's the way we conduct ourselves.

GRASSLEY: OK. Now I'd like to discuss whistleblowers, and the second of at least three questions I'd like to ask you.

In your confirmation hearing, you expressed strong support for whistleblowers and the need for them to feel free to raise their concerns up their chain of command. FBI policy encourages employees to report wrongdoing to their supervisors.

First question, do you support legal protections for FBI employees who follow FBI's own policies and report wrongdoing to their supervisors? if not, why not?

COMEY: I do, very much.

GRASSLEY: OK.

Under current law, FBI agents have no legal protection for reporting wrongdoing to their supervisors. Do you see any justification for not fixing that problem?

COMEY: I think it's very, very important that we create the safe zones that all of our people need to raise concerns that they might have. And so that is the way I not only talk, that's the way I walk at the FBI. And I know that we're having conversations about is -- are there additional protections we can offer. I think there might be sensible ways to do that.

I have some small concerns. I want to make sure that we don't create a system where, to get too deep in the weeds here, an FBI agent or FBI employee can report not just fraud, waste and abuse, but can get whistleblowing protection for reporting bad management.

That's potentially a huge range of things. So I want to be thoughtful about what we're considering whistleblowing as we do this. But I'm open to try and improve the way we approach it.

As I said, I have tried to really walk this talk by the way I've acted, the people I've met with, the way I've given out awards in the FBI. And so I will continue to try and work with you to try and improve that.

GRASSLEY: You've spoken repeatedly about ISIS's sophisticated, successful use of the Internet to lure Americans to Syria and to inspire tacks -- tactics in the United States.

This is very concerning, and I know that's the -- you speak from your heart on that. Other than addressing the problem by encryption, are there any other tools that would help the FBI identify and monitor terrorists online?

More specifically, can you explain the -- what electronic communications, transactions record -- or ECTR, I think that's referred to as an acronym, are, and how Congress accidentally limited the FBI's ability to obtain them with a -- obtain them, or the drafting error? Would fixing this problem be helpful for your counterterrorism investigations?

COMNEY: It would be enormously helpful. There is essentially a typo in the law that was passed a number of years ago that requires us to get records, ordinary transaction records that we can get in most contexts with a non-court order, because it doesn't involve content of any kind, to go to the FISA court to get a court order to get these records.

Nobody intended that. Nobody I've heard thinks that that's necessary. It would save us a tremendous amount of work hours if we could fix that, without any compromise to anyone's civil liberties or civil rights.

Everybody who has stared at this has said, "that's actually a mistake. We should fix that."

GRASSLEY: Yeah. This will be my last question.

I've -- you heard my concerns about non-citizens who are not legally permanent residents buying and possessing guns in this country. If you want me to ask this, then I'm not going to ask this other question. Let me go to this question.

In regard to your last response, you said you try to "walk the talk" on this. So why hasn't the FBI imposed discipline in any of some cases that are -- that I've been investigating? What message does it send to FBI employees when the FBI fails to hold retaliators accountable for their actions? That will be my last question.

COMNEY: Yeah, no, that's a -- that's a good question and a hard question.

I believe we do work very hard to try and hold retaliators accountable. Each case, the challenge of answering it at the abstract level is each case has to be looked at individually.

So I do think that we work very hard to try and hold people accountable. Now, often, when people know we're coming for them, they'll retire on us and leave government service, which is a challenge.

But it is not just that enforcement that matters. It's how do we act, how do we conduct ourselves. And -- and I don't want to brag on myself, but I will for a second.

We have annual directors' awards, and at the end of the directors' awards this year, I gave an award to recognize somebody for blowing the whistle on misconduct.

And I went back to the podium, and I said, "this matters. The reason I'm saving this one for last is, this matters." We're an organization dedicated to finding the truth in American life. We have to make sure we're open to seeing the truth about ourselves.

So, look, we're not perfect and I -- and I think we can benefit from working with you to get better, but I believe we have sent the message this matters.

GRASSLEY: Listen, you've been here a long time. I thank you for the time you've given us. Maybe some members will submit questions for answer in writing. I may even do that myself. I hope you'll respond appropriately and as quickly as you can.

Thank you very much for your service.

COMEY: Thank you, Senator.

GRASSLEY: We're -- we're done.

END

Dec 09, 2015 17:41 ET .EOF