V

REMARKS AT TUESDAY MORNING SESSION

By The Honorable James B. Comey
Director of the Federal Bureau of Investigation

The Tuesday morning session of The American Law Institute convened in the Ritz-Carlton Ballroom, Washington, DC, on May 19, 2015. President Roberta Cooper Ramo presided.

President Ramo: Ladies and gentlemen, it is my honor to bring to the podium the Director of the Federal Bureau of Investigation and Bill Webster. I would say, as they are walking up, that many organizations would be thrilled to have a Director of the FBI, a Director of the CIA, and a federal judge. And we are so efficient that we have those all in one person. (*Laughter*)

Ladies and gentlemen, Judge Director, Director Bill Webster. (*Applause*)

Judge William H. Webster (DC): Thank you very much, Roberta.

Well, it's been quite a number of years since we had the privilege of having Director Comey here—2004, as I've been told—when he was Deputy Attorney General. And we want to welcome you back and we look forward to hearing from you.

Thinking about that period of time, I'm told that during his confirmation proceedings, the earlier one, he was questioned I think about his steadfastness, and he said there were two areas at least that he would not compromise, and those were his devotion to and protection of his family and his personal integrity. In the years that have followed, he's been true to his commitment, and we've been the better for it.

He reminds me a lot of—I'm from Missouri, and one of our icon families out there is the Danforth family, the founders of Ralston Purina, who also produced a great chancellor of Washington University, Bill Danforth, and a great Senator, Jack Danforth. Their grandfather operated under the motto "I dare you," and said to stand tall, think tall, be tall.

This morning we have that model, 6 feet, 8 inches tall. (*Laughter*)

And we're glad to have him. We're really glad to have him.

Just a few words about his background, some of which is probably in your materials that you have. But Director Comey is a New Yorker, educated at the College of William and Mary and the law

school at the University of Chicago. He went right into public service at that time as a young lawyer in the Southern District of New York in the U.S. Attorney's Office, where it wasn't long before he gained recognition by taking on one of the FBI's top priorities, organized crime, in the famous trial involving the Gambino family.

Later on, he moved over to the Eastern District of Virginia where he had another significant trial as an assistant U.S. attorney, taking on those responsible for the bombing—years ago, but all of us remember it—of the Khobar Towers in Saudi Arabia. So his reputation as a successful prosecutor was well established. Then he moved back to New York as the United States Attorney.

Moving forward through the years, he has done many significant things, including five years in the private sector as a general counsel and senior officer of Lockheed Martin and other private companies.

Coming to the FBI at this time is a challenging world. The world is changing. The priorities are changing and the need to adapt to those changes has never been more significant, in my view, in all these years. We had priorities at the FBI initially—white-collar crime, organized crime, foreign counterintelligence. I moved terrorism into that subject matter in 1980. And the technological changes that have occurred and the threats worldwide—transnational threats, foreign fighters, and now cyber—present unique challenges to someone who believes strongly in leadership but leadership within the rule of law. That's why I think we have just exactly the right man at the right time.

I remember not long after he had been confirmed as Deputy Attorney General, the Attorney General was John Ashcroft, who was seriously ill. And one of the investigative programs that the FBI and others had been using was up for congressional renewal or rather for executive renewal. Those in the Department of Justice—and he was then Deputy Attorney General—were concerned that that program contained materials and procedures that were illegal.

Ashcroft was too sick to really deal with the issue, and he had ceded his responsibilities to his deputy. A call to the deputy was get

over here because they are coming over to the hospital to get the Attorney General's signature. And he managed to get over there in time to be there. And as I recall that story, the Attorney General raised up and said, "I've given the authority to the—he is the director now and he will make the decision. I hope you'll make the right one." And he did. And the program was not renewed.

That fits my model of the FBI, as I've just outlined. FBI: fidelity, bravery, and integrity.

As we go into this new cyber world, I can't think of a better person to lead us down that road—and he's just about finished with two years of service at the present time—than the Honorable James B. Comey, Director of the FBI. Please welcome him. (*Applause*)

Director James B. Comey: Thank you, Judge. Good morning, ladies and gentlemen.

My life contains a series of imposter moments. I hope that's true for you because I think it's a healthy thing. But I can remember vividly the first time I was in the Oval Office in the morning, briefing the President on the terrorism threat, and I remember looking around thinking I always thought it would be somebody better than me. (*Laughter*) If the American people knew, they wouldn't be all that comfortable.

This is one those moments for me. To be introduced by William Webster gives me an imposter moment. Bill Webster is what I aspire to be, a person of extraordinary character and grace and intellect. He is what I want to grow up to be. And the notion that he is introducing me makes me feel like an imposter, but it is one of the great honors of my life. So thank you, Judge.

I wanted to share with you thoughts about, at the suggestion of your staff, how the FBI Director's world has changed since Judge Webster occupied the chair that I sit in. And the obvious answer, the most prominent way in which it's changed, tracks the way in which all of our lives have changed. Since the Judge was Director, I think smart-

er people than I have said one of the true inflection points in human history has happened. The relationships among humans, and among humans and their governments, has changed fundamentally with the digital age that was probably a toddler when the Judge was Director and now is a full-grown adult with me as Director. And so I want to share with you just some brief thoughts about how we at the FBI are approaching that challenge, and then I'd love to take your questions.

First, let me make sure that we're thinking about the challenge the same way. When I say inflection point in human history, I believe that our entire lives have changed in the last 25 years. We have connected our entire lives to the Internet. I have five children. It's where my children play. It's where we bank. It's where our critical infrastructure is. It's where our nation's secrets are. It's where our social lives are. If I had a social life, I think it would be on the Internet. (*Laughter*)

It's where all commerce is. It's where all of the academy is. It is where everything is. That is incredibly important and wonderful.

But the FBI's responsibility is to try to protect people from fraud, to fight spies, to fight terrorists, to fight pedophiles, to fight all manner of threats to the American people that now all manifest themselves online because that's where life is. People want to hurt our children. They come where our children are. Our children are far less likely to be in a park today than online. They come where our money is, which is online, where our secrets are, where our infrastructure is, where everything is. This is for the FBI, as well as humanity, a singular change.

I think back to what I believe was the great vector change because cyber is, after all, just a vector. It's the way, in our view of the world, that bad things come at us. The great vector change of the 20th century that gave birth to the FBI was the confluence of the automobile and asphalt, because suddenly in the 1920s into the early 1930s, criminals could move at speeds that were unheard of and cover distances that were unimaginable. Two states in the same day. They'd do a bank robbery in Indiana, then do one in Illinois, maybe get to Iowa, moving at 45-50 miles an hour downhill. And suddenly the normal

boundaries were impediments to effective law enforcement. The county line, the state line. All of you remember the movies about if the robbers can just get to the state line. A national force was needed to respond to this entirely new way of bad guys acting. This vector change. And there was the first Director of the FBI, with a federal force already formed but really born with that vector change, to respond to a threat that moved at unimaginable speeds.

This vector change is that times a million, maybe times a billion because Bonnie and Clyde could not do a thousand robberies in all 50 states in the same day from their pajamas, halfway around the world. They did not move at 186,000 miles per second, which is the speed of the Internet. And so this vector change in the 1920s strained our notions of venue and physical jurisdiction. This vector change explodes them. And so I want to tell you how we are trying to deal with that change.

The first thing we're trying to do is adopt an attitude of humility. We stand here in the middle of the greatest change in human relations certainly in our lifetimes, probably ever. We have to approach it with a sense of humility. We don't know what the future looks like. We don't know what the best thing to do is. We have an idea for what seems reasonable, but we have to adopt an attitude of humility, take feedback and iterate, take feedback and iterate on a change that we've never faced before.

So with that posture, we have five elements to the way we are approaching this. And they are brief.

The first is we are trying to focus in a better way. I conceive of the cyber threats that come at us, the various threats that come at us through that vector, like a layer cake, an evil layer cake, which I've been mocked for calling it. The top level is nation states; just below them, terrorists; just below them, organized criminal syndicates; and then the remaining layers of the cake are all kinds of criminals and creeps and pedophiles and fraudsters and activists.

We are trying to focus our resources where we think our resources will make the biggest difference. We are international. We have a lot of technology we've invested in over the last decades. We are trying to bring that to bear at the top of the stack and focus on the nation states, terrorist use of the Internet, and the big syndicates, the worldwide botnets, the very sophisticated actors operating around the world. We are trying to focus so that we can make an impact.

The second thing we are trying to do, as part of that focus, is focus internally in a way that makes more sense. The Bureau's normal way of assigning work is first asking this question. Where did it happen? The bank robbery happened here. The bomb went off here. So that's where we will do the work. That field office will take the work.

But with this threat, the meaning in the "it" has changed or the whole sentence has changed. Where did "it" happen when you are talking about a threat that's moving at the speed of light? Is it meaningful to think about where it first manifested itself with a particular corporate victim or a particular individual victim? We think it's actually smarter to think about it differently and to assign the work not based on some notion that "it" happened in New York or "it" happened in Chicago, but by asking ourselves where is our talent in the FBI? Who has the chops inside the FBI to deal with this particular threat?

And so what we have done is we have divided up the nation-state threat, the terrorist threat, and the organized-criminal threat into various slivers and then had contests within the FBI to see where the best talent is to deal with that particular threat, and then we assign it to that office where the talent is. So we may assign a particular aspect of the threat that comes to us from China to the Little Rock division because they have some people there who are very, very talented at that particular threat. We will call that the "strat" office. And then we will allow up to four other offices to help with that threat. We call those "tac" offices.

This is a total change for the FBI. We are assigning based on ability, not based on some notion of physical venue. So far it seems to be

working well. We coordinate it from headquarters. We don't run the investigations from headquarters. And we are still about a year into that model and still getting feedback to see what makes sense. So focusing is the first element of our strategy, both in terms of what we will work and how we will work it.

Second, our strategy involves trying to shrink the world. This threat that's moving at the speed of light has reduced the world to the size of a pin. Beijing and Boston are fractions of a second apart on the Internet. And so we think, to deal effectively with this, we have to shrink the world back in a couple of different ways.

I have to forward deploy far more resources, both special agents and intelligence analysts, into the countries where the keyboards are being typed on so that we can build relationships with their law enforcement and their intelligence services that allow us to shrink the world back against the bad guys.

And the second thing we are trying to do is shrink the world inside the U.S. government. When I left government in 2005, I conceived of the government, especially the federal government's response to all things cyber, as like four-year-old soccer. I have five children and so I've watched a lot of four-year-old soccer. And so you can picture four-year-old soccer. Everyone knows the ball is the thing, and so there's a big clump of kids. They run all over the place. And the coach's job, which I've tried to do is, no, no, no, stop, spread out, spread out. In about 2005, everybody knew cyber was cool, and so there was a big clump of people chasing the ball.

Coming back, after almost a decade, I see us—and we have actually grown significantly just in the last two years. I see us understanding the importance of position on the field, getting that we have to spread out and pass to each other. I see us at maybe college-level soccer. The challenge we face is we are against an opponent that's moving at World Cup speed. And so we have to constantly improve the way we talk to each other inside the government. We have to shrink the

distance between agencies within the U.S. government to deal with the threat that's moving at light speed.

One of the greatest examples of the progress we have made is a task force called the National Cyber Investigative Joint Task Force, which sits outside of Washington, that the FBI is the lead of, but that is made up of 20 different agencies. We sit there together and visualize the threat and just talk to each other. What are you going to do? Okay. You do this. I'll do that. We coordinate campaigns against these worldwide threats there, and we share information there. That is a tremendous piece of progress in shrinking the world inside our government to deal with this threat. Lots more to do there to get to World Cup level, but we are making good progress.

The third part of our strategy is we want to try and impose costs. All of us in the government and I suspect in the private sector have a sense that actions taken through the Internet, whether they are criminal or they are nation-state actors trying to steal intellectual property, seem like a freebie to people coming into the United States. And it is not in the mind's eye of those people akin to kicking in the front door of Americans and walking out with your television set. But to us it is the same. The things that matter most to our companies and to our individuals—their identities, their innovation—are being stolen just as if those actors kick in the front door.

And so our thinking is we need to impose real costs on this behavior to try and drive change. We need, first of all, to lay hands on people who are at those keyboards. We need to lock people up and send a very strong message that it is not a freebie. And where we can't lock people up, we need to send a message, including to nation states, that this is not conduct consistent with an ordered global enterprise with positive relationships between nations, that there need to be costs. And sometimes those costs are simply a naming and shaming. Sometimes those costs are going to be economic sanctions. But the goal of the government and particularly the FBI is to impose some real costs to try and change behavior.

The fourth element of our strategy is—I mentioned the layer cake. The bottom part of that layer cake is landing on the desks of state, local, tribal law enforcement every single day. The frauds that we are not getting to, because of our focus on the top of the layer cake, are the responsibilities of detectives and district attorneys all over this country. Every piece of work that involves criminal investigation now requires digital literacy. I know there are folks here who used to be prosecutors, as I did. The good old days were that you would do a search warrant and you'd find one of those black composition notebooks where the knuckleheads would have written down who got what and how they divided it up. And Shorty got this and Joe got this. And you needed to photocopy that and put a sticker on it. You were good to go. Those are the good old days because today that information about Shorty and Joe is as likely—more likely, frankly—to be on a thumb drive, a mobile device, a laptop, an iPad.

To do any kind of criminal investigative work, you have to be digitally literate, and you need to be digitally literate in a sophisticated way to deal with fraud coming through the Internet. And so we are hearing from our partners in state and local law enforcement we need training, we need advice. And so one of the things we are working very hard on with our partners at the Secret Service is to push out training to our state and local law-enforcement partners to help them climb the digital literacy curve so they can deal with crime that's coming at them through the Internet.

Then the last piece of our strategy in some ways is the most important and most challenging. We have to become more effective at dealing with the private sector because it is where the victims are. So it's where the information that will help us solve crimes and address threats is. And it's where the brains are, about so many of these threats, where we can learn a tremendous amount from talking to very smart people in the private sector.

It's a wonderful thing that the Internet is in private hands in the United States. It should stay that way. But if we can't inside the government figure out how to work effectively with the private sector, I'm

a little bit like a cop patrolling a street with 50-foot-high solid walls on either side. I can tell you the street is safe, but I can't tell you a thing about what is going on in the neighborhoods and offer assistance to try to make those neighborhoods safer. We must find a way to make those walls not invisible but make those walls permeable, in some sensible way, so that we can share information more effectively to the private sector and the private sector can share it to those of us in law enforcement.

I know some of these challenges because, as the Judge said, I was the general counsel of two companies before coming back to this. And so I have asked myself out loud to my security people, you want to share what with the government? What are they going to do with it? What if we get sued over it? What if it hurts us in a competition? What control do you have over this? I know you are motivated by good things, but what's going on here?

And I have also been asked this question by leadership at companies. Why can't the government tell us more? The government is telling me things that I'm reading in the newspaper. What good is that? They tell me things that happened a month ago, six months ago. That is useless. So I feel that pain from the private-sector side. We simply must get better, faster, more effective.

So I think that involves at least three categories of improvement. The first is rules of the road. We, as a government, have to offer clarity to private enterprise as to what is going to happen to information that's shared with the government, who should you share it with, and so how does this actually work? And there is good work underway to try and give those rules of the road.

And I should point something out that I think gets lost sometimes in the information-sharing discussion. It's almost never the case that we need the content of people's communications. What we need are the digital fingerprints, the digital dust. We need to see the 1's and 0's that are the hallmark of the attacker. We need to know so is this a new thing or does this connect to something else we have seen before.

That's about the makeup of malware. That is not about content of memos or the content of e-mails.

We have to give better rules of the road to the private sector. We have to get faster at sharing information. We have changed tremendously since 2012 when the financial sector in the United States was getting hit by denial-of-service attacks. We learned some good lessons there. I think we have gotten faster, both the FBI and DHS, at pushing out indicators, warnings to the private sector. And we still have to get even better.

And then we also need to improve the techniques of the information sharing. It's not good enough for us to e-mail each other indicators when the threat is moving at light speed. We need to find machine-speed ways to share information. That's very, very hard, but not impossible.

The FBI has built something that we are now sharing with the private sector called the Malware Investigator. We have long had inside the Bureau a database where we input all the malware signatures that we see. And so when our special agents open an investigation, they take a piece of malware from a victim and they query the database like our fingerprint database, and they get a hit if it's something we have seen before, and they can connect various dots. We are trying to make that capability available to trusted private-sector partners. So if you are a private entity that we know and you have been hit, you can access that database yourself and get a result not in weeks or days, but within seconds, so you know this is this thing that also hit the oil and gas sector—okay, now I know who to talk to—or hit other parts of the financial sector. We are growing this Malware Investigator. It's one step, but to me it indicates the kind of thing we have to build.

So we are trying to focus, trying to shrink the world. We are trying to impose real costs to change behavior both of individuals and of nation states. We are trying to help state and local law enforcement deal with the wave of crime coming at all of us through the Internet

that we can't get to. And last, we are trying to be more effective with the private sector.

One of the things that make all of the above hard and especially our work with the private sector is what I call the post-Snowden wind. I believe that people should be skeptical of government power. I'm talking to a room full of people who represent, I believe, the absolute model of intellectual rigor and discipline when approaching government authority and the use of those authorities. I think people should be skeptical and ask hard questions.

What I see sometimes in the wake of the Snowden wind is skepticism being blown over to cynicism where people don't take the time to ask good questions and get rigorous, disciplined answers. So what are the government's authorities and why do they matter? And how are they overseen, and how are they used? But instead, there is just a whole lot of nodding about how awful it is and the government is out of control kind of stuff. That is a bad place for us to be.

And so I have worked hard, along with a lot of colleagues in government, to try and fight for the space in that wind to talk about what we do and why we do it and how we are overseen. I believe you cannot trust people in power. People sometimes say to me, well, you seem like a really nice person. I say, well, I am but you should not trust me. (*Laughter*)

You should, instead, ask how is he overseen? Our Founders understood this. That's why they divided power among three branches and set interest against interest. You should ask, so how are you constrained? How is the design of the Founders alive in your life? And that's a very good conversation to have. It's one I'm very proud of.

There's a reason. I've told my whole workforce this. There's a reason that I keep, under the glass on the right corner of my desk, the single-page application that J. Edgar Hoover submitted to Bobby Kennedy to wiretap Martin Luther King. It's five sentences long. It's utterly devoid of substance. And I keep it there not because I'm trying to pick on Bobby Kennedy or J. Edgar Hoover. I keep it there as a

reminder of the value of constraint and oversight, because that corner of my desk is where every single morning, including this morning, I review a stack of applications that are going to the FISA [Foreign Intelligence Surveillance Act] Court for permission, for a short period of time, to intercept the communications of people or institutions in the United States. And when I set that stack down there, those applications are not five sentences long. They are often—almost always—as thick as my hand or my wrist, sometimes—I don't have much of a bicep, but as my bicep. That is constraint and oversight. That is the design of the Founders laying upon us. It is a huge hassle, and that's a wonderful thing. And I set them there on top of that one pager to remind myself—and I tell all of my troops about it to remind them—that there is beauty in the constraint and oversight. You can't trust people in power. You've got to know how they are constrained.

What I worry about is in the wind that's been blowing since Mr. Snowden's so-called revelations. It's been hard to have those conversations. I hope you will fight to have those conversations, ask hard questions. I hope you will ask me hard questions here today. I think there is an angel in those details. The tools that I have, I have for a reason, and if I can't defend them and explain them, then I shouldn't have them.

I worry that in the current debate about so-called 215 [Section 215 of the USA PATRIOT Act, an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001)], the entire focus is on telephony metadata. That's an important subject. That's a useful tool to the FBI. But June 1st some critical tools of the FBI are going to sunset, and if I lose those tools, it is a huge problem. Two in particular.

We have the authority under Section 215 to go to a FISA judge and get an order in a case-by-case for particular documents or records. We use it fewer than 200 times a year, but when we use it, it matters tremendously.

Second, we have the authority to go to a FISA court when we encounter a spy or a terrorist who is dropping phones—dropping phones—dropping phones—and get a roving wiretap order just as we've gotten in criminal cases since I was a baby federal prosecutor in the 1980s. If we lose that authority and the 215 case-by-case authority, my work will be severely impacted. I worry that that gets lost in the discussion about telephony metadata, and I'm fighting for the space to talk about that, and I have about 10 days left.

I hope you will hold us accountable. I hope you will ask those hard questions.

Let me mention one other thing before I leave you. When I left government in 2005, we had a problem that we talked about a fair amount in 2005 called "going dark." It was blinking off to my periphery when I was the Deputy Attorney General. When I came back as FBI Director and increasingly over the last two years, it is blinking so brightly in front of me it's obscuring my vision. And here's what I mean by this.

As all of us increasingly live online and our papers and effects and our entire lives are there, increasingly in our public-safety work, which means both law enforcement and national security, we are encountering devices that cannot be opened with court order, communications that cannot be intercepted with court order. Today we face a threat in this country where ISIL is reaching in, trying to motivate troubled souls through Twitter, to find them and motivate them to kill in this country. And if they find someone they think is a live one, they move them off Twitter to an encrypted form of communication that with lawful authority and a court order we cannot intercept. And so I'm left looking for needles in a haystack where the needles are increasingly invisible to me.

I think that's something that a democracy has to have a serious conversation about. I am an enormous fan of privacy. But I believe, in the design of our Founders, is an understanding that ordered liberty requires a balance between privacy and security, that searching the

people's papers and effects requires predication and a certain process as our Fourth Amendment holds, and that if privacy becomes the absolute value, that is a world that I don't think enough folks have closed their eyes and tried to picture.

I hear a lot of times people say, no, privacy is the unalloyed value. There are tradeoffs. And, I ask folks, close your eyes and imagine the logic of that world. Imagine a world where all of life is online and I can't see pedophiles. I can't see terrorists. I can't see spies. I can't seize papers and effects with a court order with predication. I can't intercept communications.

I'm not trying to freak people out, but I think a democracy has to have a conversation about this because the logic of it is inexorable. We are drifting to a place of darkness, from my perspective, that is not healthy. It's not my job to tell people where we should be, but I think I need to sound the alarm to tell people we have to talk about this and where the right place to be is. I don't have an easy answer, but I see a problem that affects all of my work, and I see it growing every single day.

And so I hope that in this amazing organization you will, as I know you are with your data-privacy work, participate in that conversation and help us as a democracy figure out where we should be between two cherished values. We care deeply about privacy. We care deeply about security. I don't think they are mutually exclusive, but they have to be accommodated in a way that makes good sense.

So that is our strategy. That is one of the challenges that the cyber world poses to the Director of the FBI today that Judge Webster didn't face. He faced many different challenges. I'm not suggesting the job has gotten easier. I told him the other day Directors have gotten taller. I can't say they've gotten better. (*Laughter*)

So let me close by thanking you for giving me the chance to share thoughts with you. I thank you again for the difference you make in the life of American law. I know you know it, but as an outsider, I see

it very, very keenly. And I thank you for taking the time to do this. (*Applause*)

President Ramo: Well, the Director says that he has time for a few questions. So if a few people want to make their way to a microphone.

I will say, Director, I've seen a fair amount of four-year-old soccer myself, and what you failed to mention is there's nobody in the goal. (*Laughter*) And my four-year-old grandson told me just the other day he was going to make 100 goals, and he pretty much did. (*Laughter*) And so what I want to say, as an American and as a lawyer, is that I deeply appreciate it that we have you standing in front of the goal right now. (*Applause*) The judge at microphone 2.

Judge Paul L. Friedman (DC): I have a question. My name is Paul Friedman and I work here in the District of Columbia.

You also started a conversation recently about a different topic, and I don't want to change the topic, but I think this is important too.

Post Ferguson, Brooklyn, Baltimore, and other things, the strains between communities and law enforcement I won't say have emerged. They have always been there I think, but they have certainly come to the fore and in ways that need to be addressed. I think you began a conversation at Georgetown recently about this, and maybe you could talk a little bit about that conversation you are having internally and with law enforcement around the country.

Director Comey: Thanks, Judge. And I don't think you overstate it. I think the President described this as a slow-rolling crisis, and I feel it that way. I've been to all 56 FBI field offices. In each one, I meet with state and local law enforcement, and now I'm back again on the second tour to number 12. And what I feel is that in many communities there has long been a gap between law enforcement and the communities, especially communities of color. And what I see happening is the lines are actually starting to push apart even today. A new incident will happen that involves the community, and that line starts

to bend that way, and then a police officer—we had two killed in Hattiesburg, Mississippi a week ago, two killed yesterday, both at 2:30 in the morning, different parts of the country. That starts to bend this line that way. And there is no easy answer to that, but it's very, very worrisome to me.

It's the reason I spoke about it. I wrestled with whether to say anything because I thought the FBI is not really in the policing business, but the President asked me to go to the funeral of Detective Liu in New York. And I could feel this palpable pain on all sides, and so I thought maybe I could contribute something trying to frame it.

So what the FBI is trying to do is use our good offices to continue to drive that conversation. But all 56 of my field offices are going to host conversations this summer where they bring in communities, especially communities of color, and I especially want kids—not kids—I want college-level leaders and law enforcement to drive a conversation. I don't want to just drop the mike and walk away. We are in every community in this country. I want to use our offices to try and drive the conversation, because I really do think, as Bill Bratton says, a huge part of the answer is seeing each other, seeing the people we protect more clearly, trying to understand what it feels like to be a 19-year-old African American guy walking down the street on your way home from the library and encountering us. What does that feel like? But by the same token, get people to see us and what we see through the windshields of cars and the kind of people we are.

I believe it's hard to hate up close, and so I think where departments have done the best—I had a fascinating dinner with the sheriff and the chief in Los Angeles two weeks ago. They learned some hard lessons after the Rodney King riots, and they've invested in—they've adopted that "it's hard to hate up close" approach, which seems expensive sometimes to city councils and mayors, but they have spent the money. They have programs to get to know people and get cops out of their cars.

But this is a very complicated and hard conversation. We just have to have it. We have struggled as a country always to talk about race. I was really nervous about that speech because I thought, yikes, I'm an awkward, tall white guy. Can I really talk about race? And I was pleasantly surprised with the reaction. And I'm trying to make sure we continue that conversation.

President Ramo: So we will just have the people now standing. We will go to microphones 6, 1, and 4.

Ms. Judith A. Miller (MD): Hi. Good to see you, Director.

I've done a fair amount of work in the cyber area, and I just wanted to first compliment you on the efforts you've made to restructure the FBI and to do outreach. I think Jim Trainor in particular has done a really good job of trying to reframe how you all talk to the private sector. But I just wanted to give you a tiny bit of feedback and ask for a reaction.

I still think the sharing of information isn't really working well, even within the government, let alone with the private sector. And part of the reason for the private-sector issues, I believe, is that unless you get to Jim Trainor—or a couple of other people like him—who's in charge of outreach, among other things, in the cyber world in the FBI, people often get to other people within the FBI who don't have still much of a clue about how to respond and how to give assistance. So I wonder how you are thinking about getting this message to permeate through the organization now that you've got the basic structure in place.

Director Comey: That's fair feedback. By the way, I think that's accurate.

The answer is by simply pushing quality leadership, picking great people, and then making sure that all of my field offices understand the strategy and understand that—this all worked very, very well in the Sony case, by the way. Sony reached out very quickly to the LA field office and they responded in a fabulous way. I have to drive that mod-

el of engagement through all 56 field offices. And we'll get there. The strategy is fairly new, but your feedback is fair. It's not good enough yet.

President Ramo: The judge at microphone 1.

Judge Raymond J. Lohier, Jr. (NY): A lot of what you described by way of the cyber crime or anti-cyber crime effort relies critically on the cooperation and ability of other nations, it seems to me. That was certainly my experience. How cooperative have you found other nations in connection with combating cyber crime in the U.S., and how able have they been to combat cyber crime and to help the FBI combat cyber crime?

Director Comey: Thanks, Judge. The answer is everybody seems to get it. So it's not about enthusiasm. There are some countries in the world that may not be all that enthusiastic about working with us. I'm not going to name them here. But in the main, tremendous enthusiasm. But you identified the gap. They, like our state and local partners, are hungry for training. So I didn't mention this, but part of my forward deployment is to invest in training our foreign partners where the keyboards are to help them raise their expertise, both their technology and their talent. Thanks, Judge.

President Ramo: Microphone 4.

Unidentified Speaker: I'm also a judge. I'm from Texas and my court oversees training for all the prosecutors and judges in the state, and we also have a small grant that also helps with training law enforcement.

So my question is—and I've reached out to the FBI before to have assistance in training. And I was wondering, do you have a list or do you have experts that you could provide us to train on these issues like the digital literacy or the cyber stuff, anything like that? Is that possible?

Director Comey: Oh, we sure do. What I can do is one of my folks over there—just give them your information. I'll get you this. But

we have something called the Cyber Investigator which is a three-part course for state and local investigators, two parts online and one part in person. At the end of those three parts, we give you a certification. You are a certified cyber investigator. And so that's available to state and local law enforcement for free all around the country.

Now one of my challenges is I had no dough during the sequestration nightmare, and so we were rationing gas, literally rationing gas, and we stopped all of this. And so it's taken a while for people to realize it's back and alive. But one of the handsome men standing over there with the notebook, if you could just give him your information, we'll get it to you. (*Laughter*)

Unidentified Speaker: Just one other point, a little feedback. I am presently involved in a Citizens Academy that the FBI puts on. I'm from San Antonio. There are 40 people from all walks of life attending it, and it's excellent. And so that information needs to get out to the public. I just happened to see it on TV. But we just had a whole course on cyber information.

Director Comey: More to come. I'm trying to raise the profile of that. We run in all of our field offices something called Citizens Academy, where we invite people from all walks of life to come and spend—it runs different lengths—10 weeks—typically it's one day or one night a week—and get a good look at us. I'm very self-interested there. Everything the FBI does depends upon our being believed.

I told people my proudest moment in my two years as Director was when we sent dozens of agents to Ferguson, had them all dressed in business attire, and put raid jackets over the top. And they knocked on hundreds of doors. Everybody talked to us—white, black, old, young, man, woman. They talked to us. And so I've told the entire organization that is something priceless because you are believed.

The Citizen Academies are important because most people don't get to know us. Their impression of us is formed from TV. My kids are always saying, Dad, the Director on TV does all kinds of cool stuff. (*Laughter*) I said I don't do any of that stuff.

But most people don't get to form an impression of us. The reason I like the Citizens Academies is you form your own impression and then go out and live your life, and you will be able to talk to people behind our backs about us. And I'm highly confident you will see that we are flawed in all kinds of ways because humans are. We are honest and we are competent. And you will see that if you get a close look at us.

Unidentified Speaker: In that school, you are also very open, which is great. So thank you.

Director Comey: I'm trying to. One of my concerns is—I'll shut up after this. But one of my concerns is that the identity of the FBI in American life has drifted down since I was in middle school. Part of that is the competition in American life. But when I was in middle school, every boy thought about the FBI. I think one of the reasons is we had three channels plus PBS in Yonkers, New York. (*Laughter*) And one of them had an FBI show.

But I actually have a dream that one day every boy and girl—black, Latino, Asian, all people, all kids in middle school—will think about the FBI. That matters for a bunch of reasons.

But one is I also have another crisis I'm dealing with. My numbers of black and Hispanic special agents have been steadily coming down for over a decade. That is a crisis. And I'm going to leave in eight years. I will not leave unless that line is turned the other way. And part of the answer is having people get to see us and know us.

I only have one diversity problem. A lot of places have two. The FBI is a great place to work if you are a woman or a person of color. It is a great place to work. Almost nobody leaves. We've just got to get people to see us, to be interested in us, and to give us a shot.

President Ramo: Thank you.

I'm pretty sure you are not a judge, but just in case, the judge at microphone 3.

Mr. George M. Newcombe (CA): Thank you, Roberta. I'm definitely not a judge.

I have a question about encryption. As you rightly point out, the percentage of the traffic on the Internet each year that's encrypted is growing rapidly. Companies like Apple now permit—or their products effect—end-to-end encryption.

In light of the government's unsuccessful attempt in the mid-1990s to force a back door through the Clipper Chip, what do you propose to do? What power do you want? What changes would you like to see, to give the FBI and other agencies the ability, in the appropriate circumstances, to penetrate what otherwise would be impenetrable encryption?

Director Comey: The honest answer is I don't know for sure. I know the goal. The goal is that in the presence of a court order, based on a showing of probable cause, we are able to get access to stored information or data in motion. How to accomplish that is not clear to me. A lot of work is being done inside the government right now in the legislative and executive branch. The President is personally focused on this. It may take some combination of legislation, regulation, and consent. There are lots of people in the tech industry talking about, well, I wonder if we need some sort of international set of norms that will govern how governments interact with technology and information moving across technology. So I don't know is the honest answer right now.

Now one thing I do know is people often say, well, you're an idiot because you're against encryption and look at your website. You talk about how important encryption is. Well, I may be an idiot, but that's not one of the reasons. I'm a fan of encryption. I like that people lock their cars when they go shopping. I like that people lock their homes. I like safe-deposit boxes for your most important stuff. What we have to find a way to, though, is with appropriate authority, predication, and oversight, to be able to get access to information. I think

that's consistent with the concept of ordered liberty, as I said. So I'm not against encryption.

And then people often respond by saying, but it's too hard. It's too hard to figure out how to give government access in the appropriate circumstances. My response is, really? Really? We've got a lot of really smart people. There is no such thing as absolute security. So the question is, what is reasonable security in light of the need to offer judicially authorized access? And I think we've got a lot of smart people in industry, in particular. I don't think that's too hard to figure out.

But the honest answer is I can't clearly see how we are going to get to where we need to go, which is I'm trying to foster a conversation to involve a lot of smart people to figure it out. But the first thing I need to do is make sure people see a little of the darkness that I see.

President Ramo: Professor Hazard?

Director Emeritus Geoffrey C. Hazard, Jr. (CA): Mr. Director, you and people in the audience perhaps could suggest people we might consult with, to inform the ALI about the significance of the information-dissemination change that you have talked about for our projects, because writing law, we tend to look backward or around at the present, and when we think about the future, we get even fuzzier than you are. But we need to be more mindful of the implications that places, events, times now are very different than what we have imagined them to be, and it would be great if we could have some people, perhaps in your office or connected people in the audience, that could alert us, inform us, guide us along that line.

Director Comey: Well, thank you, Professor. I will follow up on that. My general counsel is an old friend of mine named Jim Baker, who is also an extraordinary lawyer who thinks well about these questions, which is why I asked him to come back because cyber is something he knows really well. So when I get back to the office, I'll put him in touch with you all. That's a great start. He can also help you find other people to talk about it.

President Ramo: Well, let me say a final thank you. I don't think anybody in this room, Director, will walk out the same person that we were when we came in. We are better informed. And I think the opportunity to hear you is our great honor, and we deeply appreciate it. Thank you for everything you've done.

(*Director Comey received a standing ovation.*)