



Georgetown University Law Center
Scholarship @ GEORGETOWN LAW

2017

General Counsel of the FBI, James Baker, in Conversation with Professor Mary DeRosa on the FBI and International Justice


Mary B. DeRosa

Georgetown University Law Center, mbd58@georgetown.edu

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/2220>

Georgetown Journal of International Law, Vol. 48, Number 3, 895.

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [International Law Commons](#), and the [National Security Law Commons](#)

TRANSCRIPTS

GENERAL COUNSEL OF THE FBI, JAMES BAKER, IN CONVERSATION WITH PROFESSOR MARY DEROSA ON THE FBI AND INTERNATIONAL JUSTICE*

Mary DeRosa (MD): Thank you, and I want to thank Jim Baker very much for coming here. We have worked together and known each other for many years. He is a remarkable lawyer and public servant, and we are really, very lucky to hear from you today. What we thought we'd do is go into depth on some particular issues that the FBI is engaged in internationally, and I'll ask Jim some questions, and at the end, we're going to leave a little time to open it up for questions, so you can think about your questions, but if the question you are thinking about has something to do with Hillary Clinton's emails, or investigations into Russian activities in the election, then probably you ought to think about another question, because, for obvious reasons, Jim is not going to be able to talk about those issues. But there is a lot he can talk about.

I thought maybe we could start with just a little background. People are very familiar I think with what the FBI does domestically and its presence and role domestically, maybe less so with the FBI's overseas responsibilities and footprint, so maybe you can give us some of that background to start off.

James Baker (JB): Sure. Mary, it's great to see you again and thank you for this opportunity, Shannon, and the whole Journal, thank you for this opportunity. The FBI is mainly focused on the United States, protecting the United States from a range of threats both domestic and foreign, and on also enforcing the criminal law of the United States. And so, in order to do that, we inevitably have to be international in scope as well. So, to think about it correctly, there are two buckets I would put our work in. One is, our operational folks that people might be familiar with—counterterrorism in particular, but criminal, counterintelligence, the whole nine yards, really everything that we do—is inevitably to some degree international in its scope because of the way that the perpetrators operate, the threats, and the threat vectors. Hopefully we'll also talk about cyber security in detail. So that's the operational way we deal with the international world and I can dive into that in a second.

* This is an edited transcript of a conversation between Professor Mary DeRosa of the Georgetown University Law Center and General Counsel James Baker of the FBI. Their discussion was orchestrated as part of the Georgetown Journal of International Law 2017 Symposium, "International Justice: Where We Stand, Where We Fall, and Where We Need to Be," held in Hart Auditorium, Washington D.C., on February 27 and 28.

Then we also have a dedicated cadre of folks who focus almost exclusively on international operations. It's called the international operations division, helpfully. We have about 400 people and about 300 of them are overseas. About 100 or so, 150 or so are located at headquarters or in the United States. So the folks overseas are referred to as legal attaches, and they are at Embassies. We have, I think, sixty-three legal attaché offices around the world and another twenty-five or so sub-offices in different locations. They have responsibility for covering, in one way or another, about 200 countries. We have folks all over the world dealing with international interactions.

What they do is coordinate and consult with our international partners—with U.S. government folks at Embassies first, and then also with our international partners. They're trying to assist in joint investigations that we might be running with the foreign partner and with coordinating evidence requests back and forth. We might need evidence from a foreign country and they might need evidence from the United States, so we work on that.

A substantial part of what they do is training. They are over there training folks in what we do and how we do it. Folks are very interested in how the FBI goes about its investigations.

MD: So foreign law enforcement?

JB: We are training foreign law enforcement. Sometimes they're very interested in U.S. law, and we'll train on that. But they're also interested in FBI techniques: investigative techniques; investigative methodology; how we go about conducting oversight; management oversight of our activities; how we deal with technology issues and things like that. We do substantial training in-country, if you will. We also then have, at the FBI academy down at Quantico, something we call the "National Academy." It's a rather lengthy course where folks from around the United States, state and local law enforcement, as well as from foreign countries, come to Quantico and spend significant time at the FBI, at the Academy, going through a range of courses covering how we go about our business, how U.S. law enforcement works, how U.S. legal structures work, and so on. This is highly sought after by state and local authorities, as well as our foreign partners. This is a big deal and it is crucial in terms of building the relationships overseas that then help us do our jobs. As you can imagine, really in any line of work, having effective business relationships is critically important to being successful over the long term. So that's what they focus on.

We operate in an international environment on very case-specific things: pursuing the bad guys overseas, trying to get evidence, coordinating to make sure that something bad doesn't happen overseas,

protecting our allies from a threat or protecting a U.S. facility overseas from a threat. Then we've also got this longer term deep international presence. Just for the law students in the room, in terms of dealing with, and thinking about, the international environment you end up focusing on public international law—customary international law, treaties, these kinds of things—and thinking about the legal structure in that way. But that is a somewhat narrow, in terms of the number of person hours spent on that by lawyers and people around the world, small subset of what happens internationally, so to speak. All this other stuff is happening at the FBI and at other government agencies. For those of you who are interested in this kind of thing from a career perspective, you should think more broadly about international law. The State Department is great and the Legal Advisor's Office at the State Department is great, but that's not the only game in town, in terms of thinking about working in international matters. There are a lot of opportunities beyond the State Department.

MD: So, in the U.S. Government, you can think more broadly. For example, the Justice Department also has a lot of presence outside the country.

With that background, you have over your career, spent a lot of time working on cyber issues and it has been a major and increasing focus of the FBI over the last fifteen or twenty years. Now it is a very significant focus and it is, by its nature, very international. Maybe you can talk more about this. Many of the perpetrators of cybercrime in the United States are located overseas, but even if they're located here, the nature of the internet means that investigations would likely be international.

Maybe you could talk about the way the FBI handles cyber investigations: what are the challenges? And in what way does the unusually international quality of cybercrime maybe complicate or challenge the investigations of those issues. You can start wherever you want, but I think the beginning, the number one issue, in an investigation is who did it, and even that in the cyber area is very complicated. Maybe you can start there and talk about that aspect of cyber investigation.

JB: Sure. I'll just start, and then pull me back and guide me in a different direction if I go off on some tangent. There is no doubt that cyber is international. And any person working in that area, regardless of where you are—at the FBI, another part of the government or in the private sector—if you're not thinking about it in terms of its international aspects, you really don't understand it, you don't get it, and you're not going to be able to deal with it. That's the main thing.

Cyber is international and international is cyber. And I'm kind of flipping those around in the sense that in cyber people think about it

perhaps too narrowly in the sense of intrusions and intrusion protections and so on, but it makes sense if you really think more broadly about the role of technology today in society, and how we cannot operate really without engaging with technology in a significant way. And so I think it's important to understand that fact. It's important to understand it both in terms of the threat, then what the threat actors are thinking about, and how they're thinking about us, the potential victims. I read something recently that I thought was quite interesting that—I can't remember who said this, so I apologize to the source of it—the most useful human tool today is the smartphone. It's not a hammer or chisel or anything else that we can think of. It's a smart phone because that's what so many people have and they use it to such a significant degree. Well that presents all kinds of risks, and a lot of those risks are posed by international folks.

But in terms of dealing with this “whodunit” kind of thing, I would say we have to approach how we go about our investigation with an open mind. In the cyber environment, it is not a simple question to answer. Sometimes it's easy but many times it's not.

One of the particular problems that I'm trying to focus on is the attribution question—that is and has been a key problem and we can spend a lot of time talking about here today in the cyber area. And I guess I would say that attribution—it's an art. It's an art as much as a science. And it requires analysis and data and facts. And that you have to understand the technology in order to be able to understand the facts correctly. The facts can lead you to an identification, but you have to think deeply about those facts and understand them, and that requires a careful analysis, so we really try to do that effectively. I would say that we as a government, a federal government, are getting better, increasingly, about attribution, and using the tools available to us. The issue is that the adversaries are also getting better about obscuring the nature and scope of their activities and their location. So, I don't know if that's a chicken and egg problem, or if that's a cat and mouse problem, or just an escalating problem, but, those two things are happening simultaneously, so that presents challenging issues.

MD: So, maybe just, back up a little and talk a little about why attribution is so much more difficult. And when you say the FBI or the government is getting better, is it getting better technically at tracing back, or are there other aspects to understanding and improving attribution?

JB: I would say we're increasingly better technologically. We are increasingly better with our analysis of the technology and what it means. You have to really be knowledgeable about these networks:

understand what is happening, what a particular piece of data means in terms of how a network has routed material, and the forensic footprint of the data. That does require specialization, and we have more people who are better at it, therefore we're getting better at it. That's one way to think about it.

It is both technology and analytical rigor and skill that enables you to better figure out what's happening. And as I say, at the same time the bad guys know this is a problem, they know this is hard for us, and they want to make it even harder. They are doing whatever they can, especially focusing on obscuring the metadata or the data about data (the bread crumbs if you will) that are associated with their communications. They are trying like heck to obscure that, even to a greater degree, than exists inherently within the networks. Inherently, there are challenges with respect to attribution because of how communications are routed for lawful reasons by legitimate companies, and then if you layer on top of that some of the techniques that adversaries use, it's even harder. Then you layer on top of that encryption, and we have a whole other ball of wax. We'll come back to that.

MD: We definitely want to get to encryption. I read something very recently about a number of cyber criminals, cyber actors who are now pretending to be Russian because there is so much attention paid to Russian hackers. You're seeing a lot of—and people have been able to identify—Russian code that looks like it has gone through a translation app, so maybe that's an example—when you say they are trying to mask, hide and trying to misdirect. There are very creative criminals.

JB: It's extremely creative. So, it depends on their purpose, where they are, what they're trying to do, and how they're trying to fake us out. Sometimes they'll pretend to be from particular foreign countries and do things—without getting into too much detail—to make themselves look like they're coming from that particular location in a deeper way than just an IP address that happens to show up from a foreign country. They try to really look like they are coming from that location. But then also, we have the problem of foreign actors trying to look like they are coming from the United States, for a variety of reasons. One reason is because we have good infrastructure here, and they want to piggy back off of that. But secondly, they know a lot about U.S. laws and they know what restrictions are going to apply inside the United States. They want to take advantage of that to slow us down. Even if at the end of the day if we ultimately figure out where they were at the time of their intrusion activities, they might be gone by that point, so if they can just slow us down, knowing that eventually we might catch up to where they were, they think they'll be gone from there by a certain point. It's

both things—they sometimes want to look like they're overseas, they sometimes want to look like they're here.

MD: Interesting. When we talk about different cybercrimes or different aspects of cybercrime, what are the different kinds of international actors engaging in the same sort of techniques maybe, but for different purposes. Can you talk a little about who those actors are, and maybe what some of the differences are? Does who it is make a difference in how you have to deal with them?

JB: Sure. So it's nation-states that are highly technically advanced in many instances. They are very well-resourced both from a technological perspective as well as from a human resource perspective. They have lots of people they can throw at a problem. I can come back to that in a second. Transnational criminal organizations are mostly interested in money. The nation-states are interested in a range of different things, in particular they are interested in information, both about U.S. government officials and U.S. government classified information. The type of thing that you would think of as more classical espionage. But then they are stealing personally identifiable information about Americans and stealing it with a long-term perspective in mind as they monitor who we are, what we do, and where we move. They plot out where they are going to take advantage of that information. And they also steal economic data that is beneficial to them and their companies.

In addition to then embedding themselves in a persistent way in our networks to continue their espionage activities. They are then potentially positioning themselves to actually take something more characteristic of a cyber-attack in the future, should that be necessary. They are very well resourced and robust in terms of the threat that they pose.

Aside from focusing on money, transnational criminal organizations after money are also, in many instances, highly sophisticated, dangerous, and they might cause wreckage inadvertently. So, that's a potential problem. Terrorist organizations are also a threat, both in the physical world as well as in the cyber world. Then you have different types of criminals, in smaller groups, that you might consider organized crime but not on the scale that I was talking about a second ago. Individual hackers that are after something. And then you have other types of organizations that aren't interested in damage, destruction, or in stealing money, but for whatever reason, they want to disrupt the operation of a network or a website, or take command of some type of thing. So they potentially pose threats as well.

Did I answer your question?

MD: You did, yes. I don't know what's gotten the most attention, but there has certainly been a lot of attention on state actor hacks and

“attacks” in a non-legal sense. I’m thinking, for example, of North Korea and the Sony incident, Iran and the U.S. financial sector. With Sony, Iran, and China’s economic espionage, the FBI and the U.S. government have gone public with their attribution assessments. Maybe you can talk about the process there and some of the challenges that present when you are actually dealing with an investigation of a state actor.

JB: Because of the FBI’s role as a national security entity, with both national security authorities as well as law enforcement authorities, we can look at a problem from a 360-degree perspective and try to figure out the right, or best, way to thwart or disrupt the activities of the nefarious actor, as well as bring them to justice. We know that it’s not always the case that you’re going to have something wrapped up in a nice prosecution: you bring somebody to the United States, you put them in a federal court, you try them, convict them, and send them to jail.

That happens, but it doesn’t always happen, and we’ve gotten our minds around that, especially over the last sixteen years with respect to terrorism cases. We know that there are going to be other outcomes aside from just arresting somebody and putting them in jail here in the United States. I think we try to look at these threats from that 360-degree perspective. If the nefarious actor is a nation state, you’re not going to put a nation state in jail. You can put individual actors in jail if you can figure out who those are, and I’ll come back to that if I can. The question is: how do you disrupt these activities and how do you deter future activities like that? One way is to go public with attribution. With respect to that process, at a high level, we want to make sure we were right. We want to make sure that we’ve done rigorous analysis of the facts, that we’re highly confident in the attribution that we are going to make publically. That’s number one.

Number two is that we want to make sure that we have coordinated or de-conflicted with other entities in the U.S. government and perhaps with our foreign partners to make sure that they don’t have some interest that would be damaged by making this information public. You do increase the risk of public disclosures about how you determined that it was country X, and we have to be prepared to deal with that. You’re going to get a million FOIA requests for this kind of information, so you want to make sure that you’ve thought through all the risks and benefits of the attribution. But then, that may be the way to go about doing it. The attribution problem is—and I’m not an international lawyer by training or by trade currently—one of the things that inhibits the development of international legal norms with respect to

cyber activities. It's this idea that countries have that they can basically get away with it, and they don't have to conform to the norm because they can sneak around it. The norm doesn't get developed and doesn't have the effect that legal norms that have developed over the years have internationally because you can see that it's a state actor driving a ship through a particular location.

MD: I'm not aware of the U.S. government having actually identified a state actor as a cyber actor up until a few years ago, and recently there have been quite a few. Is that a movement on the part of the Government, the FBI, and others, to recognize that the other way wasn't working and we need to be more public about it?

JB: I guess I would say I think we've gained more experience dealing with the problem, and the limitations on the tools that are available to us to thwart the activities, and so, again, it's sort of a risk-benefit analysis to try to deal with these countries and not let them get away with it. To try to hold them accountable, knowing that there is a certain amount of risk involved. Then also knowing that there are risks involved in not doing something to protect our people, our facilities, our information.

I think we're gaining more experience and willing to try different things. If we think we can indict a foreign government official because we have the evidence, and we think that would make sense, then we'll do that. If we think attribution is the thing to do, we'll do that. If it turns out that there's some equity out there that the intelligence community has, for example, that militates against making an attribution public, then we'll hold off. I think we're evolving our thinking about the range of options available to us and trying to be very thoughtful, but also aggressive when dealing with what is a very aggressive threat coming at us.

MD: Just to wrap up on the cyber issue and lead us into the encryption issue: the investigation of cybercrime and cyber activities very much involves the private sector, and the private sector is, for the most part, the victim of a lot of these cyber activities. How do you see the FBI interacting with the private sector, and what are some of the challenges there? How do you work with the private sector to try to make sure that it's an effective relationship?

JB: We think of companies that have been victimized as victims, and we approach them on that basis. The FBI is very used to dealing with victims of a whole range of terrible crimes. We have a lot of tools that we can bring to bear to try to deal with what may be a persistent ongoing threat, or to help them understand what happened and to ultimately bring the people who are responsible for this to justice, if possible, or at

least call them out or deter them from further activities. Companies are often weary of dealing with us in the cyber realm, there is no doubt about that. I understand that, having been in the private sector a couple of different times, I get that. You lose a certain amount of control when you start to bring the federal government into it.

I think, however, that we've been effective in developing ways to protect their data. If we have to do some examination of some part of their data or their network in connection with the investigation a) we care a lot about getting it right and b) I think we've come up with ways to actually be effective in protecting the data from exposure either in court, in a proceeding, through FOIA, or through criminal discovery. Obviously if you end up with a defendant, the defendant's rights have to be protected as well. Trying to figure out that balance is critically important to us. But we care a lot about it and we care a lot about getting it right.

I guess, to flip it around a little bit, I think companies also are sometimes hesitant to come to us and expose that they have been victimized. They don't want that to become public for a lot of different reasons. Perhaps for reputational reasons, or because competitors who might take advantage of them. What I would add though is in that there are many great companies out there who offer cyber security services to protect them and to do forensic evaluations, and so on. It's important to remember that in many instances a company is dealing with a nation-state on the other side that is trying to victimize them. That, as I said before, is well-resourced, highly technically advanced and persistent, and can be there for the long term.

The question is: are you, as a corporation, able to fend off a nation-state? Is that really what you're capable of doing? Even though you might hire some great companies collectively, are you really able to do that without assistance in some way from the federal government, from the FBI, from DHS, etc.? I would urge people to think carefully about that and to not be overconfident, frankly, in their ability to do that.

And as an aside, if you are a corporate leader and you are not focused on cyber, you are missing the boat. It is critically important in a whole range of ways to your effective operation as a company, and perhaps your existence as a company. Not only are people stealing things like intellectual property, and have been for a long time, we increasingly see the ransomware threat, where these malicious actors will find some way to tie up your networks, tie up your data so you can't access or use it and you have to pay them a ransom in order to free it up. Even if you pay it, how confident are you that they're not still there doing whatever they want to do.

MD: It's hard to imagine, given everything that's been out there in the last five or so years, that there are corporate leaders that aren't focusing on cyber. Is that something you still see? Has that improved or do you still think there's a challenge there?

JB: I think there's a challenge there. I think it has improved but I still think there is a challenge there. People, such as executives, are too willing to delegate to cybersecurity folks without themselves spending enough time developing a sufficient level of understanding of what's happening to execute their fiduciary responsibilities to the company. I think that's an issue. I think people need to focus on that.

Also, just for lawyers, my two-cents to the law students in the audience is sort of similar: I don't really care what part of the law you are interested in, if you are not focused on understanding technology and cyber to a degree of proficiency, you are going to be left behind. You are not going to be an effective lawyer in today's environment and you are going to increasingly be left behind in your legal career because it infuses so many different parts of the world. You continually bump into it from a legal perspective, whether you are in the government or whether you're in the private sector. You need to understand tech to a significant degree.

MD: I teach a cyber class here and I always have a similar message because I think you are absolutely right. I have definitely seen in my time and practice that there is a tendency with cyber issues or other technology related issues, for senior people to say "oh, that's tech, I don't get that," "that's cyber, I don't get that," and turn it over to experts. And these are lawyers and policymakers, and therefore the law and the policy hasn't developed in as healthy a way as it otherwise could. What I say to my students is, don't be scared by the technology. There is a lot that you can understand about how all of this works. And you can work on these issues without being a computer science PhD. I completely agree that if you aren't comfortable with these issues, a lot of the law is going to leave you behind.

Continuing with technology issues, obviously a lot of attention last year after the San Bernardino attack, and the FBI's attempts to get information from the perpetrator's iPhone, and that brought this issue of the proliferation of strong encryption and its impact on law enforcement and national security investigations to public attention. I'd like to first get your explanation of this issue, for people who've heard about it but are not completely familiar, and then I'd like you to solve it.

JB: OK, so, we've talked about the going dark problem, which many people have derided as a name, but that's what we've called it. Going dark, it is essentially the inability of the FBI—or federal, state, local law

enforcement as well as the intelligence community—to obtain, with appropriate legal process, the evidence or information that the law would otherwise entitle us to obtain because of some technological reason. That’s really what it’s all about—we can’t get the information because of the application of technology. Encryption is one subset of that, so I’ll just talk about encryption. I’ve said it before and I’ll keep saying it: the FBI supports strong encryption. It is a good thing for society; it protects our data across many different vectors, personally identifiable information, our commercial transactions, our financial transactions, our health data, and it protects government information. Strong encryption is a good thing for society.

But, strong encryption also has costs. It has costs in particular with respect to public safety because it impacts our investigations. It impacts our investigations by, in some instances, making evidence or foreign intelligence information simply unavailable. It’s just not there. We cannot, and will never, be able to get it. In addition, it has implications for our ability to conduct effective investigations. So it makes evidence unavailable, but it also slows us down because we have to try to deal with this problem; we have to try to figure out other ways to get at the evidence or to deal with the threat. It costs more money. It imposes risks, it increases risks, with respect to the investigation itself because we have to do riskier things. If we’re trying to keep it quiet and not let the perpetrator know we are investigating, they might figure it out because we’ve done something riskier. It creates risks to our investigators and undercover agents who might have to be in dangerous situations that they otherwise wouldn’t find themselves in because we could get access to the person’s electronic communications. We might have to put human sources in there. We might have to use other techniques that are, perhaps, more fragile, if you will—

MD: I’m going to want to come back to that.

JB: OK, so we might have to use techniques like that. It creates significant risks for the investigation. It is often argued that we should adopt or use substitutes for trying to obtain the content of communications, which is really what I’m talking about. Two that come up most often are legal hacking and metadata analysis. We do both but they are not a panacea; they do not solve all the problems.

MP: So this is the FBI . . . ?

JB: With a warrant, hacking into a particular device, as opposed to going to a provider, with an order, and saying “give me all of Mary DeRosas’ email.” If I can’t do that, if your communications are encrypted end-to-end and that’s not available to me anymore, one way to get around it might be to hack your device and try to see what’s

happening when it's in the clear or when it's not been encrypted. That is possible but those types of solutions are expensive. They are also fragile because anytime the manufacturer or the software developer changes something, it could throw the whole solution off. It's not easy to do at scale if you have a whole network of people. Metadata analysis is great; we do it to understand communications networks and social networks if you will . . .

MD: Can you give me just a sentence or two on what you mean by that?

JB: An old-fashioned metadata analysis is understanding telephone records: who's talking to whom, who else are they talking to, how does that work, and what do those connections mean? Then you start looking at who people are communicating with through a variety of communications platforms, and understanding how that network works. What financial transactions a person engages in, what their movements are if we can understand those. In other words, understanding not the content of the communications, but data about the communications. That's what metadata is.

MD: There are a lot of people who would argue, I think, that there is a tremendous amount you can get out of metadata analysis, and maybe even so much that it makes the content analysis or the content, less important. What would your response to that be or your reaction to that be?

JB: Metadata is highly useful, and we use it, there's no doubt about that. But it is not everything. It can tell us who's talking to whom, but it doesn't tell us about what. So we might have some leads from some other source that says these are two "bad guys," then we see that they talk a lot to each other, but we don't know what they're talking about. This came up in the threat in Garland, Texas that ended up with the perpetrator being shot by local law enforcement. We could see in that instance that the perpetrator was in contact with a terrorist operative overseas—I can't remember the exact number—over a hundred times. But because of the platform that they were using, we couldn't see what they are talking about. We knew they were talking, we didn't know what they were talking about.

For the law enforcement folks at the scene, something tragic might have taken place. So that is kind of what I am talking about. Metadata is good, it is useful, it's not everything. It doesn't tell you about the capabilities, plans, intentions, or activities of the threat actor in the same way.

We, the FBI, are not trying to impose some solution on society. We don't have the solution for this problem and we understand that. We're

not trying to force American companies or the American people to adopt a back door or give us some golden key that undermines cyber security in some significant way—we don't want that.

MD: There's no pushing a particular legislative solution to build a backdoor or anything? Why? I assume it's because you don't think it would be useful—why is that?

JB: So, the concern that we would have about a back door is that it would be threatening and would undermine even further our cyber security. Let's just remember cyber security is not some "perfect" state we are in today and that the FBI is trying to get people to weaken that thing which is perfect. It's not perfect now, so there are risks associated with it. But we don't want to make it any worse, that's for sure. We want to protect people's privacy—we want to protect their personal information. We want to protect their rights of association and free speech. We need to do that. We want American companies to be competitive and innovative, especially in the global marketplace in which they must operate. We want all of those things simultaneously. That is hard to do—and I don't think anybody has figured that out.

There are some interesting ideas that have been put forth. Matthew Tait on Lawfare had put out the "multiple envelope" concept, we can talk about it more if you want. There are certain things that are worth exploring in terms of getting an appropriate balance of all these things. But I think—as President Obama said—you can't be absolutist about these things. We need to find something that is an appropriate balance for American society.

At the end of the day, look, what we're saying is, we, the FBI, work for the American people. You have given us the responsibility to protect you from a range of threats and to enforce the criminal law. So the question is, what tools do you want us to have? What information do you want us to have available to us in order to do the job that you've given us? That's the question. We're trying to tell people that this is a problem and we don't have a solution. But the country has to make some choices. And if it does nothing, that's a choice because technology will continue to evolve, and it changes every day. Encryption is spreading more and more, and in some ways that's good, but it presents more and more challenges for us.