# OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JUNE 13, 2013

**Serial No. 113–32**

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
81–462 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAUL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
JASON T. SMITH, Missouri

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

# CONTENTS

JUNE 13, 2013

# OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

**THURSDAY, JUNE 13, 2013**

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
*Washington, DC.*

The Committee met, pursuant to call, at 10:07 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Sensenbrenner, Coble, Smith of Texas, Chabot, Bachus, Issa, Forbes, King, Franks, Gohmert, Jordan, Poe, Chaffetz, Marino, Gowdy, Amodei, Labrador, Farenthold, Holding, Collins, DeSantis, Smith of Missouri, Conyers, Nadler, Scott, Watt, Lofgren, Jackson Lee, Cohen, Johnson, Pierluisi, DelBene, and Jeffries.

Staff Present: Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Allison Halataei, Parliamentarian & General Counsel; Robert Parmiter, Counsel; Kelsey Deterding, Clerk; Perry Applebaum, (Minority) Minority Staff Director & Chief Counsel; Danielle Brown, Parliamentarian; and Aaron Hiller, Counsel.

Mr. GOODLATTE. The Committee will come to order, and without objection the Chair is authorized to declare recesses of the Committee at any time. We welcome everyone to today's hearing on the oversight of the United States Federal Bureau of Investigation. I recognize myself and the Ranking Member for opening statements.

This hearing on oversight of the Federal Bureau of Investigation will come to order. We welcome Director Mueller to your final appearance before the House Judiciary Committee as FBI Director, and we are happy to have you here with us today.

Before we begin, let me take a moment to commend you for your successful tenure at the FBI. You took office under extremely difficult circumstances. In fact, you were confirmed 1 week before September 11, 2001, and the attacks on New York City and Washington, D.C. During your 12 years as Director, you have led the transformation of the FBI from a domestic law enforcement agency into a complex intelligence-driven national security organization whose primary missions include confronting the most significant security threats facing our Nation today. You have done the American people a great service, and for that you have my sincere gratitude.

We now know that last week's unauthorized disclosure of certain NSA intelligence programs was committed by a 29-year old former defense contractor. I know there is little you will be able to say about these programs in a public hearing, but I and other Members of the Committee believe it is important for you to explain to the extent you are able why you believe these programs are a necessary part of America's counterterrorism operation.

I also believe the recent reports regarding the NSA programs illustrate this Administration's ongoing problem of national security leaks. The Obama administration takes credit for having investigated more national security leaks than any previous Administration. While this may be true, I am not certain whether it is due to a more aggressive investigative approach to national security leaks or the simple fact that there have been a shockingly high number of leaks in the last 4½ years.

These leaks illustrate the delicate balancing act between the need to protect national security information and investigate leaks and the need to preserve the First Amendment right to freedom of the press.

Regardless of how some Members of Congress may feel about the recently revealed NSA programs, the fact remains that the terrorist threat to the United States is ongoing. We were reminded of this nearly 2 months ago when the Boston Marathon, traditionally a day of celebration, was the target of a terrorist attack. Dzhokhar Tsarnaev and his brother, Tamerlan, set off twin explosions that killed three people and injured more than 250. This attack was a grave reminder, as you warned this Committee in 2010, that domestic and lone wolf extremists are now just as serious a threat to our safety as international organizations, like al-Qaeda.

I would like to commend the FBI and its State and local partners, all of whom worked tirelessly to identify and locate the bombers and apprehend Dzhokhar. However, prior to the Boston attack, several Federal agencies, including the FBI, received intelligence information about Tamerlan. I am concerned that inadequate interagency coordination may have prevented robust information sharing in this case. It is imperative that the Administration and Congress examine this matter closely to identify areas in which intelligence information sharing can be improved.

On the subject of counterterrorism, I also look forward to hearing from you about the FBI's efforts to investigate the attacks on the American consulate in Benghazi, Libya. Immediately following the attacks, the Obama administration called them a spontaneous response to a video critical of Islam. As we all now know, the attacks were, in fact, preplanned acts of terror. I am intensely concerned that the Administration's handling of the attacks has hampered the FBI's ability to conduct a thorough investigation. As former Deputy Chief of Mission Gregory Hicks testified, the Administration's mischaracterization of the attacks so angered the Libyan government that they prevented the FBI Evidence Response Team from traveling to Benghazi for 2 weeks.

Finally, Mr. Director, I am very interested in hearing from you about how the Bureau intends to tighten its belt in a responsible manner during this time of fiscal uncertainty. Along with Crime Subcommittee Chairman Sensenbrenner, I sent you a letter in

April asking several questions about the FBI's budget and spending priorities, including the FBI's policy to provide extensive financial benefits, including paying for all laundry and food for the highly paid professionals brought to work at FBI headquarters for 18-month stints.

I appreciated receiving your response last week, but I believe this is an area where the FBI and other Federal law enforcement agencies are not making the best use of taxpayer dollars. I hope to hear what the Bureau intends to do to address this issue. I look forward to hearing your answers on all of these important topics today, as well as on several other issues of significance to the FBI and the country.

And it is now my pleasure to recognize for his opening statement, the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Goodlatte, and I join in welcoming the Director of the Federal Bureau of Investigation. We gather today at a time when the Nation stands at a legal and political crossroad. We are confronted with a seemingly endless war that increasingly must be fought in the digital age. And I say this not only because of the recent disclosures concerning the FBI and the NSA surveillance programs, but because of a range of actions that occurred since the attacks of September the 11th, 2001.

It's not a partisan concern, and it is one that applies both to the present Administration and to the last one as well. Nor is it a concern particularly limited to surveillance programs. It extends to our increasing reliance on drones to conduct foreign policy and the government's use of the so-called state secrets doctrine to avoid legal accountability. And, yes, in no small part because of the actions of the NSA and the Federal Bureau of Investigation, it's my fear that we are on the verge of becoming a surveillance state, collecting billions of electronic records on law-abiding Americans every single day.

A point the recent disclosure confirmed by the Administration that Section 215 of the USA PATRIOT Act is being used to engage in a nationwide dragnet of telecommunications records. I have, along with many of my colleagues, both Democrats and Republicans alike, I've long expressed concern that Section 215 fails to impose a meaningful limit on the government's ability to collect this type of information. If every call is relevant, then the relevance standard we enacted into law has little practical meaning.

Another point is the total secrecy in which surveillance operates under the PATRIOT Act and FISA. This secrecy denies Congress the opportunity to conduct meaningful oversight and prevents the public from holding its government accountable for its actions. I concede that it's a difficult and sensitive issue to resolve, but that's our job. A free society can only be free if it has the informed consent of its citizens. It is critical that the public knows how its government treats the content of its emails and telephone calls even when it collects them by mistake.

It is true that some Members of the Congress have chosen to receive classified briefings about these programs, I among them. These briefings, though, often prohibit attendees from taking even notes or to even discuss such information with anyone else. And

with all due respect to my friends in the Administration, the mere fact that some Members may have been briefed in a classified setting does not indicate our approval or support of these programs.

Indeed, many of us voted against the reauthorization of the PATRIOT Act and the FISA Amendments Act, precisely because of what we learned in those classified sessions. I agree with President Obama about the need to find a way to have a responsible conversation about these issues and how we can engage all Americans in this debate to a maximum extent possible.

But at a time when no major decision of the FISA Court has been declassified, and when the Administration continues to rely on the state secrets doctrine to avoid accountability in the courts, I must say that we are not yet able to have a more public and rational, even if limited conversation. The only way to ensure that this critical debate will actually occur is for this Committee to achieve an appropriate balance between the need for secrecy and the need for informed debate. One way to tell that that balance has been tilted too far in favor of national security is when individuals in public service have legitimate grievances with our government, but feel they have no recourse but to leak classified information to the press.

I don't condone these leaks. I believe that if we fail to adjust the concerns at the heart of these controversial programs that there will be more leaks. And so, Director Mueller, as one who supported the extension of your term as Director, and whose integrity I have always held in highest regard, we in the end are a Nation of laws and not men. Moreover, with all due respect, my considered judgment is that the Federal Bureau of Investigation's actions are inconsistent with the requirements of the PATRIOT Act and violate the fundamental privacy of law-abiding citizens.

And so I finish where I started. The Congress, and in particular this Committee, stands at a crossroad. Every day it seems that a new part of the legal architecture put in place to fight this war on terror is exposed. The prison at Guantanamo Bay is unsustainable. Of the 166 men held there, 86 are already cleared for transfer. More than 100 are engaged in the third month of a hunger strike. Nearly 2,000 personnel are needed to keep the prison functioning.

Thanks in no small part to the efforts of the Chairman, we have begun to explore the legal underpinnings of the Administration's drone programs. There is a growing bipartisan unease with the notion that the executive branch can kill a United States citizen on its own determination that he poses an "imminent threat."

And with respect to the Section 215 collections exposed only last week, it seems clear that the government's activity exceeds the authority this Congress has provided, both in letter and in spirit. With every new disclosure, another piece of the legal architecture put in place after September the 11th crumbles.

And so it is my hope that over the coming weeks the Members of this Judiciary Committee can come together and conduct meaningful oversight of these programs. Where needed, we should pass relevant and credible legislation, just as we did on a unanimous basis after September 11.

Tomorrow morning my colleague Justin Amash and I will introduce a bill that will address the overbreadth and impenetrability

of the surveillance programs. It is not the only proposal to address these problems. It should not be the only response to the broader questions we face. But it is a modest start and I hope that my colleagues will join me. This is a time for Members of both sides of the aisle to come together and help restore our Nation to its proper role as a beacon for civil liberties around the world.

I thank the Chairman for indulging me additional time to make the statement.

Mr. GOODLATTE. The Chair thanks the gentleman.

Mr. GOODLATTE. And without objection, other Members' opening statements will be made a part of the record.

We again thank Director Mueller for joining us today.

And, Director, if you would please rise, I will begin by swearing you in.

[Witness sworn.]

Mr. GOODLATTE. Let the record reflect that Director Mueller responded in the affirmative, and I will now introduce him.

Our only witness today is Federal Bureau of Investigation Director Robert S. Mueller, III, who has led the FBI since September 4, 2001. He was first nominated by President George W. Bush. In 2011 he was asked by President Obama to remain as FBI Director for an additional 2-year term, and that was swiftly approved by the Congress.

Director Mueller has a long and honorable record in public service. After graduating from Princeton and receiving a master's degree from New York University, Director Mueller enlisted as a Marine and served in combat in Vietnam. He received a Bronze Star, two Navy Commendation Medals, a Purple Heart, and the Vietnamese Cross of Gallantry.

After his military service, he earned his law degree in my home State, at the University of Virginia. Early in his legal career, Director Mueller served as a prosecutor in the United States Attorney's Offices in both San Francisco and Boston. After working as a partner in the Boston law firm of Hill & Barlow, Director Mueller returned to the Justice Department in 1989 as an assistant to Attorney General Thornburgh and later as head of the Criminal Division. In 1998, Director Mueller was named United States Attorney in San Francisco, a position he held until 2001, when he was nominated to be Director of the FBI.

Director Mueller, as your tenure is set to expire this year, we welcome you today for one last look and look forward to your statement. Please proceed.

**TESTIMONY OF THE HONORABLE ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION**

Mr. MUELLER. Thank you, and good morning.

Mr. GOODLATTE. You know what, turn on that microphone.

Mr. MUELLER. Good morning, Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee. And I thank you for the opportunity to appear here today and appear on behalf of the men and women of the FBI. And on their behalf let me begin by thanking you for your support of the Bureau over the 11 years that I have been there.

We live in a time of diverse and persistent threats from terrorists, spies, and cyber criminals. And at the same time we face a wide range of criminal threats from white-collar crime to child predators. And just as our national security and criminal threats constantly evolve, so, too, must the FBI counter these threats, even during a time of constrained budgets.

Today I would like to highlight several of the FBI's highest priority national security and criminal threats. As illustrated by the recent attacks in Boston, the terrorist threat against the United States remains our top priority. And as exhibited by many of our arrests over the past year, we face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often distinct, which makes them difficult to identify and difficult to stop.

At the same time, foreign terrorists still seek to strike us at home and abroad. Terrorists today operate in more places and against a wider array of targets than they did a decade ago. And we have seen an increase in cooperation among terrorist groups and an evolution in their tactics and an evolution in their communications. Core al-Qaeda is weaker and more decentralized than it was 11 years ago, but it remains committed to attacks against the West. Al-Qaeda affiliates and surrogates, in particular al-Qaeda in the Arabian Peninsula, pose a persistent threat. And in light of recent attacks in North Africa, we must focus on emerging extremist groups capable of carrying out attacks from that region.

Next, let me turn for a moment to discuss the cyberthreat, which has evolved significantly over the past decade and cuts across all FBI programs. Cyber criminals have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate both state secrets and trade secrets. And we also face persistent threats from hackers for profit, organized criminals, cyber syndicates, and hacktivist groups.

As I have said in the past, I do believe that the cyber threat may well eclipse the terrorist threat in years to come. And in response, we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks. Our Cyber Division is focused on computer intrusions and network attacks. FBI special agents work side by side with Federal, State, and local counterparts on cyber task forces and our 56 field offices. We have increased the size of our National Cyber Investigative Joint Task Force, which brings together 19 law enforcement, military, and intelligence agencies to stop current attacks and prevent future attacks.

And cyber crime requires a global approach. And through the FBI's 64 legal attache offices, we are sharing information and coordinating investigations with our international counterparts.

And at the same time, we recognize that the private sector is the essential partner to protect our critical infrastructure and to share threat information. We have established several noteworthy outreach programs, but we must do more. We need to shift to a model of true collaboration and build structured partnerships within the government, as well as in the private sector.

Turning finally to the FBI's criminal programs, the FBI's responsibilities range from complex white-collar fraud to transnational criminal enterprises and from violent crime to public corruption. Given limited resources, we must focus on those areas where we bring something unique to the table. For example, violent crime and gang activity continue to exact a high toll in our communities, and through Safe Streets and Safe Trails Task Forces we identify and target the most dangerous of these criminal enterprises.

At the same time, the FBI does remain vigilant in its efforts to find and stop child predators. Our mission is threefold. First, to decrease the vulnerability of children to exploitation. Second, to provide a rapid, effective response to crimes against children. And third, to enhance the capabilities of State and local law enforcement through task force operations such as the Innocent Images and Innocence Lost initiatives.

Now let me turn and spend a moment discussing the recent public disclosure of highly classified national security programs. The highest priority of the Intelligence Community is to understand and to combat threats to our national security, but we do so in full compliance with the law. We recognize that the American public expects the FBI and our Intelligence Community partners to protect privacy interests, even as we must conduct our national security mission. The FISA Court has approved both programs, and these programs have been conducted consistent with the Constitution and the laws of the United States. And the programs have been carried out with extensive oversight from courts, independent inspectors general, and Congress.

These programs do remain classified today, so there are significant limits on what we can discuss this morning in open session. But I do understand that there have been classified briefings on these programs for this Committee and for the House at large, and I hope that you have been able to attend it, and if not, will be able to attend such a briefing from the Intelligence Community regarding both the focus, the strictures on, and the legality of these programs.

As to the individual who has admitted making these disclosures, he is the subject of an ongoing criminal investigation. These disclosures have caused significant harm to our Nation and to our safety. We are taking all necessary steps to hold the person responsible for these disclosures. As this matter is actively under investigation, we cannot comment publicly on the details of the investigation.

Now in closing, I would like to turn to sequestration. The impact of sequestration on the FBI's ability to protect the Nation from terrorism and crime will be significant. In 2013 the FBI's budget was cut by more than $550 million due to sequestration, and in 2014 proposed cuts will total more than $700 million. The ongoing hiring freeze will result in 2,200 vacancies at the FBI by the end of this fiscal year, with 1,300 additional vacancies in 2014.

I have long said that our people is the Bureau's greatest asset. Additional operational cuts will impact the FBI's ability to prevent crime and terrorism, which will impact the safety and security of our Nation. We do understand the need for budget reductions, but we would like to work with the Committee to mitigate the most significant impacts of those cuts.

Chairman Goodlatte, Ranking Member Conyers, Members of the Committee, I want to thank you again for your support of the FBI and for its mission. Our transformation over the past decade would not have been possible without your cooperation, and I look forward to any questions you may have. Thank you.

Mr. GOODLATTE. Thank you, Director Mueller.

[The testimony of Mr. Mueller follows:]

# Department of Justice

**STATEMENT**

**OF**

**ROBERT S. MUELLER, III**
**DIRECTOR**
**FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**
**UNITED STATES HOUSE OF REPRESENTATIVES**

**AT A HEARING ENTITLED**

**"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"**

**PRESENTED**

**JUNE 13, 2013**

**Statement for the Record**
**Robert S. Mueller, III**
**Director**
**Federal Bureau of Investigatiou**

**Committee on the Judiciary**
**U.S. House of Representatives**

**"Oversight of the Federal Bureau of Investigation"**
**June 13, 2013**

Good morning, Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

Today's FBI is a threat-driven, intelligence-led organization. We have built a workforce and leadership team that view continuing transformation as the means to keep the FBI focused on key threats to our nation.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and to our communities.

Counterterrorism remains our top priority. As illustrated by the recent attacks in Boston, the terrorist threat against the United States remains very real.

Yet national security is not our sole focus – we remain committed to our criminal programs. In the economic arena, investment fraud, mortgage fraud, and health care fraud have undermined the world's financial systems and victimized investors, homeowners, and taxpayers.

At the same time, gang violence, violent crime, crimes against children, and transnational organized crime pose real threats in communities across the country.

These diverse threats facing our nation and our neighborhoods underscore the complexity and breadth of the FBI's mission. To do this, we in the Bureau are relying on our law enforcement and private sector partners more than ever before.

Yet regardless of the challenges we face, the FBI remains firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the citizens we serve.

I look forward to working with this committee in these final months of my term to ensure that the FBI maintains the capabilities needed to address these diverse threats now and into the future.

**Counterterrorism**

Over the past two months, we have seen an extraordinary effort by law enforcement, intelligence, and public safety agencies to find and hold accountable those responsible for the Boston bombings.

I would like to thank those who have worked tirelessly in the pursuit of safety and justice. These collaborative efforts, along with the public's help, enabled us to identify the individuals who we believe are responsible for this attack. Our thoughts and prayers remain with the bombing victims – those who perished and those who are embarking on a long road to recovery.

As this case illustrates, we face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often distinct, but they are increasingly savvy and willing to act alone, which makes them difficult to identify and to stop.

In the past two years, we have seen homegrown extremists attempt to detonate IEDS or bombs at such high profile targets as the Federal Reserve Bank in New York, commercial establishments in downtown Chicago, the Pentagon, and the U.S. Capitol. Fortunately, these attempts, as well as many others, were thwarted. Yet the threat remains.

Overseas, the terrorist threat is similarly complex and ever-changing. We are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Al Qaeda and its affiliates, especially al Qaeda in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

In December 2011, Somali national Ahmed Abdulkadir Warsame pled guilty to nine counts of providing material support to AQAP and al Shabaab. A Joint Terrorism Task Force investigation found that Warsarme conspired to teach terrorists how to make bombs, provided explosives weapons and training to al Shabaab and arranged for al Shabaab leaders to obtain weapons from members of AQAP. Warsame faces up to life in prison.

**Counterintelligence**

We still confront traditional espionage – spies posing as diplomats or ordinary citizens.

But espionage also has evolved. Spies today are often students, researchers, or businesspeople operating "front companies." And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the federal government, U.S. corporations, and American universities.

They continue to grow more creative and more sophisticated in their methods to steal innovative technology, eroding America's leading edge in business and posing threats to national security. In the past four years, the number of arrests related to economic espionage has doubled, indictments have increased four-fold, and convictions have risen six-fold.

The loss of critical research and development data, intellectual property, and insider information poses a significant threat to national security.

In March, Steve Liu, a Chinese national and former employee of a New Jersey defense contractor, was sentenced to more than five years in prison for stealing thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, and drones. Liu traveled to China and delivered presentations about the technology at several Chinese universities.

These cases illustrate the growing scope of the "insider threat" — when trusted employees and contractors use their legitimate access to information to steal secrets for the benefit of another company or country. This threat has been exacerbated in recent years as businesses become more global and increasingly exposed to foreign intelligence organizations.

We in the FBI are working to combat this threat. The Counterintelligence Division educates academic and business partners about how to protect themselves against economic espionage. We also work with the defense industry, academic institutions, and the general public to address the increased targeting of unclassified trade secrets across all American industries and sectors.

And we are focused on the possible proliferation of weapons of mass destruction. In July 2011, the FBI established the Counterproliferation Center to identify and disrupt proliferation activities. The center combines the operational activities of the Counterintelligence Division, the subject matter expertise of the WMD Directorate, and the analytical capabilities of the Directorate of Intelligence. Since its inception in July 2011, the Counterproliferation Center (CPC) has overseen the arrest of approximately 50 individuals, including several considered by the U.S. Intelligence Community to be major proliferators.

For example, Lu Futain pled guilty on November 18, 2011, to federal charges of selling sensitive microwave amplifiers to the People's Republic of China (PRC). Lu was sentenced to 15 months in prison and three years of supervised release on October 29, 2012. Lu founded Fushine Technology, a corporation based in Cupertino, California, which exported electronic components used in communications and radar equipment. In April 2004, Lu's firm exported a microwave amplifier to co-defendant Everjet Science and Technology Corporation, a PRC-based company also owned by Lu, without having obtained a license from the U.S. Department of Commerce.

Susan Yip, a Taiwanese citizen, was sentenced to two years in prison on October 24, 2012, for helping obtain sensitive military parts for Iran in violation of the Iranian trade embargo. In her guilty plea, Yip admitted to using her Taiwan and Hong Kong-based companies to carry out a fraudulent scheme to violate the Iranian Transaction Regulations, by acting as a

broker and conduit for the purchase of items in the United States for shipment to Iran. From October 2007 to June 2011, Yip and her fellow conspirators obtained, or attempted to obtain, more than 105,000 parts valued at approximately $2.6 million. Yip helped buy the parts without notifying U.S. suppliers that the parts were being shipped to Iran, and without obtaining the required U.S. Government licenses.

Together with our law enforcement and intelligence partners, we must continue to protect our trade secrets and our state secrets, and prevent the loss of sensitive American technology.

**Cyber**

The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas, threatening innovation. And as citizens, we are also increasingly vulnerable to losing our personal information.

That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

We in the FBI have built up a substantial expertise to address cyber threats, both here at home and abroad.

We have cyber squads in each of our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. We have hired additional computer scientists. The FBI also has 63 Legal Attaché offices that cover the globe. Together with our international counterparts, we are sharing information and coordinating investigations. We have Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players in the cyber crime arena.

Here at home, the National Cyber Investigative Joint Task Force comprises 19 law enforcement, military, and intelligence agencies to coordinate cyber threat investigations. We in the FBI work closely with our partners in the NSA and DHS. We have different responsibilities, with different "lanes in the road," but we must all be on the same page in addressing cyber threats.

The leaders of the FBI, DHS, and NSA recently met to clarify the lanes in the road in cyber jurisdiction. Together, we agreed that the DOJ is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. DoD's role is to defend the nation, gather intelligence on foreign cyber threats, and to protect national security systems.

Although our agencies have different roles, we also understand that we must work together on every substantial intrusion, and to share information among the three of us. Notification of an intrusion to one agency will be notification to us all.

In addition, the private sector is a key player in cyber security.

Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to be an integral partner in reducing instances of cyber crime.

In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance – a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the Alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and manufacturing. The members of the Alliance work together with federal and international partners to provide real-time threat intelligence, every day.

Another initiative, the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems – together.

We intend to further strengthen the bridges we have built between the federal government and the private sector in the cyber security realm. We must fuse private-sector information with information from the Intelligence Community and develop channels for sharing information and intelligence quickly and effectively.

Our success in resolving cyber investigations rests on the creative use of investigative techniques we have used throughout the FBI's history – physical surveillance, forensics, cooperating witnesses, sources, and court-ordered wire intercepts.

One example concerns the hacker known as "Sabu" – one of the co-founders of the hacktivist group LulzSec.

The case began when our Los Angeles Division collected numerous IP addresses used to hack into the database of a TV game show. Our New York Office used a combination of investigative techniques, including human sources, search warrants, and surveillance, to identify and locate Sabu.

We went to arrest him, and we gave him a choice: go to jail now, or cooperate.

Sabu agreed to cooperate, and he became a source, continuing to use his online identity. His cooperation helped us to build cases that led to the arrest of six other hackers linked to

groups such as Anonymous and LulzSec. It also allowed us to identify hundreds of security vulnerabilities – which helped us to stop future attacks, and limit harm from prior intrusions.

Defeating today's complex cyber threats requires us to continually evolve and adapt.

Instead of just building better defenses, we must also build better relationships. And we must overcome the obstacles that prevent us from sharing information and, most importantly, collaborating.

U.S. law enforcement and the Intelligence Community, along with our international and private sector partners, are making progress. However, technological advancements and expansion of the Internet continue to provide malicious cyber actors the opportunity to harm U.S. national security and the economy. Given the consequences of such attacks, the FBI must keep pace with this rapidly developing and diverse threat.

**Criminal**

With regard to criminal threats, our responsibilities range from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises, and from violent crime to public corruption. These criminal threats pose a significant threat to the safety and security of our communities.

**Public Corruption**

Public corruption is the FBI's top criminal priority. We have had a number of successful investigations in this area in recent years, including a racketeering indictment handed down in April. Twenty-five individuals, including 13 Maryland correctional officers, allegedly conspired with the Black Guerilla Family gang inside prisons to distribute drugs and launder money. Gang members allegedly bribed correctional officers at several Maryland prison facilities, convincing them to smuggle in drugs, cell phones, and other contraband. The correctional officers alerted imprisoned gang members of upcoming cell searches and several of the officers had long-term sexual relationships with the gang members and were impregnated by them. The defendants face maximum sentences of 20 years in prison.

**Financial Crimes**

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, health care fraud, and securities fraud.

**Mortgage Fraud**

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. As of May, the FBI had nearly 2,000 mortgage fraud investigations nationwide — and nearly three-fourths of these cases included losses of $1 million or more.

With the economy and housing market still recovering in many areas, we have seen an increase in schemes aimed at distressed homeowners, such as loan modification scams and phony foreclosure rescues.

Others seek to defraud lenders by submitting fraudulent loan documents and setting up straw buyers to purchase homes. The homes then go into foreclosure, the banks are left holding the bag, and neighborhoods are left to manage the blight associated with vacant properties.

Last month, the leader of a $66 million mortgage fraud scheme was sentenced to eight years in prison after arranging home sales between straw buyers and distressed homeowners. Gerard Canino, 51, from Long Island, New York, along with his co-conspirators, obtained mortgage loans for sham deals by submitting fraudulent applications to banks and lenders. The lenders sent the mortgage proceeds to the conspirators' attorneys and the attorneys submitted false statements to the lenders about how they were distributing the loan proceeds. They then distributed the loan proceeds among themselves and other members of their conspiracy.

Over the past five years, we have continued to boost the number of Special Agents investigating mortgage fraud. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud.

We also work closely with the Department of Housing and Urban Development, Postal Inspectors, the IRS, the FDIC, and the Secret Service, as well as with state and local law enforcement offices.

**Health Care Fraud**

Health care spending currently makes up about 18 percent of our nation's total economy — and that percentage will continue to rise as our population ages. The federal government projects that by 2021, health care spending will reach 20 percent of the U.S. economy. These large sums present an attractive target for criminals — so much so that we lose tens of billions of dollars each year to health care fraud.

Last month, the Medicare Fraud Strike Force – a partnership between the Department of Justice and the Department of Health and Human Services – arrested 89 individuals, including doctors, nurses, and other licensed medical professionals, for allegedly participating in Medicare fraud schemes costing more than $223 million in false billing.

Since its inception in March 2007, Medicare Fraud Strike Force operations have charged more than 1,500 individuals who collectively have falsely billed the Medicare program for more than $5 billion.

Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, every taxpayer who funds Medicare, is a victim. Schemes can cause actual patient harm, including

subjecting patients to unnecessary treatment, providing sub-standard services and supplies, and passing potentially life-threatening diseases due to the lack of proper precautions.

As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used to care for the sick — not to line the pockets of criminals.

**Corporate and Securities Fraud**

Another area where our investigations have increased substantially in recent years is in corporate and securities fraud. From September 2008 to April 2013, the FBI has seen a 36 percent increase in these cases, to more than 2,750 today.

One of our largest securities fraud cases centered on the Stanford Financial Group – a Houston, Texas, financial company that caused $7 billion in losses and impacted more than 30,000 victims. Using evidence obtained throughout the investigation, the FBI identified key executive management personnel who conspired to commit large-scale securities fraud. In January and February of 2013, the last of these co-conspirators were sentenced to prison. To date, five individuals have been sentenced, ranging from 3 years to 110 years in prison.

As financial crimes become more sophisticated, so must the FBI. In the post-financial crisis period, the FBI devoted an additional 150 Special Agents and more than 175 forensic accountants to combat evolving financial crimes.

In addition to the dedication of more personnel, the FBI continues to use sophisticated techniques, such as undercover operations and Title III intercepts, to address these criminal threats. These techniques have been widely known for their successful use against organized crime, and they remain a vital tool to gain concrete evidence against individuals conducting crimes of this nature on a national level.

Finally, the FBI recognizes the need for increased cooperation with our regulatory counterparts. Currently, we have embedded agents and analysts at the Securities and Exchange Commission and the Commodity Futures Trading Commission, which allows the FBI to work hand-in-hand with U.S. regulators to mitigate the corporate and securities fraud threat. Furthermore, these relationships enable the FBI to identify fraud trends more quickly, and to work with our operational and intelligence counterparts in the field to begin criminal investigations when deemed appropriate.

**Gangs/Violent Crime**

For many cities and towns across the nation, violent crime – including gang activity – continues to pose a real and growing problem.

Gangs continue to become more sophisticated. They commit criminal activity, recruit new members in urban, suburban, and rural regions across the United States, and develop criminal associations that expand their influence over criminal enterprises, particularly street-level drug sales.

Gangs also have expanded their operations to alien smuggling, identity theft, and mortgage fraud. Our Violent Crime, Violent Gang/Safe Streets, and Safe Trails Task Forces target major groups operating as criminal enterprises – high-level groups engaged in patterns of racketeering. This allows us to identify senior leadership and to develop enterprise-based prosecutions.

**Active Shooter Threats**

Communities across America also continue to face active shooter and mass casualty incidents. Since the Sandy Hook tragedy last December, the FBI has been working with the Department of Justice's Bureau of Justice Assistance to provide tactical training to law enforcement agencies upon request.

One hundred FBI agents across the country have attended Advanced Law Enforcement Rapid Response Training (ALERRT) school and are prepared to train other officers in life-saving tactics. The 16-hour Basic Active-Shooter course prepares first responders to isolate any given threat, distract the threat actors, and end the threat. In addition, during the month of April, the FBI conducted two-day conferences and table top exercises with state, local, tribal, and campus law enforcement executives. We have also worked with experts at Texas State University to improve tactical training for officers that respond to active shooter situations and then held two-day conferences on active shooter situations at most of our 56 field offices nationwide. These conferences reached senior command staff from state, local, tribal and campus police agencies. These experiences gave behavioral experts, victim assistance specialists, and other personnel the opportunity to work through best practices and spurred discussions on how to best react to active shooter and mass casualty incidents. We are continuing our efforts with a new table top exercise specifically designed for campus law enforcement. This is an issue that impacts all of us, and the FBI is committed to working with our partners to protect our communities.

**Transnational Organized Crime**

We continue to confront organized crime. Crime syndicates run multi-national, multi-billion-dollar schemes – from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

These sophisticated enterprises come from every corner of the globe. Often they operate both overseas and in the United States, and include Italian, Russian, Asian, Balkan, Middle Eastern, and African syndicates as well as Outlaw Motorcycle Gangs. We work to cripple these national and transnational syndicates with every capability and tool we have: undercover operations; confidential sources; surveillance; intelligence analysis and sharing; forensic accounting; multi-agency investigations; and the power of racketeering statutes that help us take down entire enterprises. We also work closely with our international partners – in some cases, swapping personnel – to build cases and disrupt groups with global ties.

In the spring of 2012, four members of an Armenian organized crime ring were convicted in one of the largest bank fraud and identity theft schemes in California history. Two of those

convicted directed the scheme from behind bars. Using cell phones that were smuggled into a California state prison, they coordinated with others to obtain confidential bank profile information and stole money from high-value bank accounts. The six-year conspiracy cost more than $10 million in losses to victims throughout the Southwest.

**Crimes Against Children**

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Our mission is threefold – first to decrease the vulnerability of children to sexual exploitation through awareness; second, to provide a rapid and effective federal investigative response to crimes against children; and, third, to enhance and assist the capabilities of state and local law enforcement investigators through task force operations.

Through our entire Violent Crimes Against Children program, including the Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, the Office of Victim Assistance, Innocent Images program, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

And as new technology and new tactics are used to lure our young people, we must evolve in our efforts to stop those who would do them harm.

In January, a 31-year-old man from Montgomery, Alabama, was sentenced to 35 years in prison for producing child pornography through a massive online sextortion scheme. Christopher Patrick Gunn reached out to hundreds of young girls, gained their trust and their personal information, and then threatened to reveal that information unless they sent sexually explicit images of themselves. Gunn victimized children in at least a half-dozen states and Ireland.

This case came to light after junior high school aged-victims contacted their local police in a small Alabama town. Authorities soon realized there were strikingly similar cases in Mississippi and Louisiana.

By combining our resources and using our partnerships with state, local, and international law enforcement, we are able to investigate crimes that cross geographical and jurisdictional boundaries.

In April, we apprehended Eric Justin Toth, who had been added to the FBI's Ten Most Wanted Fugitive list in April 2012, and is currently charged with production and possession of child pornography. Toth, who also used the name David Bussone, is a former camp counselor and private-school teacher who taught here in Washington, D.C. He had been on the run since 2008, after an FBI investigation revealed pornographic images on a camera in his possession while at the school where he taught. A recent tip led law enforcement to Nicaragua, where Toth was living under an alias. He was apprehended in Esteli, Nicaragua, and has been returned to the United States to face prosecution.

And in February, the FBI's Hostage Rescue Team, crisis negotiators, and behavioral analysts were instrumental in rescuing a five-year-old boy in Midland City, Alabama. Working with the Dale County Sheriff's Department and the Alabama Department of Public Safety, some 300 officers and agents worked side-by-side to end a six-day siege in which an anti-government gunman named Jimmy Lee Dykes killed Charles Poland, a heroic school bus driver who died protecting the children on his bus. Dykes kidnapped the boy and held him hostage in an underground bunker. For six days, local, state, and federal negotiators spoke with Dykes and attempted to resolve the situation peacefully. When it was clear Dykes was becoming more and more agitated, authorities feared that the boy was in imminent danger. At that point, members of the Hostage Rescue Team entered the bunker in an attempt to rescue the boy. Dykes immediately attempted to detonate one of several bombs he had planted around his property and fired several shots at law enforcement. Dykes died during the confrontation. The boy was rescued safely, and incredibly, no law enforcement officials were injured.

This case represents some of the finest collaboration between local, state, and federal law enforcement agencies in recent time.

**Indian Country**

The FBI continues to maintain primary federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. More than 100 Special Agents from 20 different field offices investigate these cases.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults.

The FBI continues to work with tribes through the Tribal Law and Order Act of 2010 to help tribal governments better address the unique public safety challenges and disproportionately high rates of violence and victimization in many tribal communities. The Act encourages the hiring of additional law enforcement officers for Native American lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

Currently, the FBI has 14 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country. In addition, the FBI continues to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

**Technology**

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which

enables us to process fingerprint transactions much faster and with more accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's next-generation information and case management system was deployed to all employees on July 1, 2012. The system's indexing ability allows users to extract names, dates, vehicles, addresses, and other details, and to more efficiently share data with our law enforcement partners. Sentinel also enhances the FBI's ability to link cases with similar information through expanded search capabilities and to share new case information and intelligence more quickly among Special Agents and analysts.

The FBI shares information electronically with partners throughout the Intelligence Community, across the federal government, as well as with state and local agencies. For example, the FBI works closely with the nationwide Suspicious Activity Reporting (SAR) Initiative to ensure that SARs entered into the Justice Department's Information Sharing Environment's Shared Space system are simultaneously shared with eGuardian, the FBI's system used to collect and share terrorism-related activities among law enforcement, and in turn, delivered to the appropriate policing and Intelligence Community partners.

**Going Dark**

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge for conducting court-approved electronic surveillance of criminals and terrorists.

Court-approved surveillance is a vital tool for Federal, State, and local law enforcement authorities. It is, for example, critical in cyber cases where we are trying to identify those individuals responsible for attacks on networks, denial of service attacks, and attempts to compromise protected information. However, there is a growing gap between law enforcement's legal authority to conduct electronic surveillance, and its ability to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information to which it is lawfully authorized and that it needs to protect public safety, bring criminals to justice, and keep America safe. We must ensure law enforcement capabilities keep pace with new threats and new technology, while at the same time protecting individual privacy rights and civil rights.

It is only by working together – within the law enforcement and intelligence communities, with our private sector partners and with members of Congress – that we will find a long-term solution to this growing problem. In March, the FBI took one step toward improved collaboration and communication with the opening of the National Domestic Communications Assistance Center. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

**Civil Rights / Civil Liberties / Rule of Law**

Technology is one tool we use to stay a step ahead of criminals and terrorists. Yet as we in the FBI continue to evolve to keep pace with today's complex threat environment, our values must never change. The rule of law remains our guiding principle.

Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. For the men and women of the FBI, this is our guiding principle. In my remarks to New Agents upon their graduation from the FBI Academy, I emphasize that it is not enough to catch the criminal; we must do so while upholding his civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights make all of us safer and stronger. In the end, we will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

**Conclusion**

Chairman Goodlatte and Ranking Member Conyers, I thank you for this opportunity to discuss the FBI's priorities. The transformation the FBI has achieved during my term would not have been possible without your support and the support of the American people. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices throughout the United States and abroad, and we thank you for that support.

I look forward to any questions that you may have.

Mr. GOODLATTE. Before we begin the questions portion of the hearing, I want to remind Members of the Committee that although certain classified programs were publicly leaked last week, that does not mean that they have been declassified. Members who may choose to question the Director about these programs should exercise caution in how they phrase their questions in due regard for their classification and appreciate the Director's very limited ability to speak to the programs in an unclassified setting.

We will now proceed under the 5-minute rule, and I will recognize myself for 5 minutes.

Mr. Director, the recent revelation of the NSA data collection programs has led to a great deal of debate both in Congress and in the public. I know there is very little you may be able to say in a public setting, but to the extent you can, please explain to this Committee why you think these programs are important and how they protect the American people from terrorism. Do you share the concerns of many Members of Congress, including myself, and American citizens, that civil liberties need to be protected in the operation of these programs?

Mr. MUELLER. Well, let me start by saying that the challenge in a position such as I have held for the last 11 years is to balance, on the one hand, the security of the Nation, and on the other hand, the civil liberties that we enjoy in this country. And there is not a day that goes by that we don't look at some issue that raises that balance. One of the things we do insist upon and assure, and that is any endeavor we undertake addressing national security is legal.

In this particular case, the programs to which you refer, the legality has been assured by the Department of Justice. The FISA Court has ruled on these two programs, monitors these two programs, and, again, has assured the legality of the efforts undertaken in these two programs.

And lastly, I will say in response to what Ranking Member Conyers said in terms of a debate, Congress has been briefed, as has been pointed out, has been briefed over the years, was briefed prior to the 2009 re-up, was briefed before the 2000 re-up, in an effort by the Administration to make certain that Congress knew and understand the efforts that were being taken under Section 215. And if there were a change to be made by Congress, if the line is to be drawn differently, so be it. We would follow that to the letter of the law. But I repeat that in both of these programs passed by Congress they have been approved and the legality assured by the Department of Justice, by the FISA court, and have been briefed and——

Mr. GOODLATTE. Let me interrupt you because we do need to get a couple more questions in.

Mr. MUELLER. Thank you.

Mr. GOODLATTE. I think you've made your point on that. I'm sure further discussion about it before the day ensues.

As you know, the Committee is investigating the use of the Privacy Protection Act of 1980 to obtain a search warrant for Fox News correspondent James Rosen's emails. In your experience as a Federal prosecutor, as assistant to Attorney General Thornburgh, as Assistant Attorney General of the Criminal Division, and as FBI Director, when you authorize a search warrant for a target of a

criminal investigation, wasn't prosecution of that target the objective?

Mr. MUELLER. I would say no. Quite often in search warrants there are—or affidavits in support of search warrants—there are occasions where a person will be mentioned as having culpability, but there will be no discussion or anticipation of prosecution. That could be for a variety of reasons.

Mr. GOODLATTE. Well, to that point, in the case in particular we have got Mr. Rosen, and perhaps in other cases, where you did not intend to prosecute. Did you characterize the individual as a flight risk, as was done in the matter involving Mr. Rosen? And did you delay notice of the search warrant for 18 months, as was done in the case with regard to Mr. Rosen? And it actually turned out to be 3 years because the judge neglected to release the information until 18 months after his order had required that it be done, but the Justice Department requested 18 months in the first place.

Mr. MUELLER. Yeah, I am not——

Mr. GOODLATTE. Why would that be necessary if there were no intention to prosecute?

Mr. MUELLER. I am not familiar with the full extent of that investigation in particular, all of the facts that were raised either in the affidavit or in the discussion as to how one would proceed to get the data that persons wanted. I can say two things. One, that there was great scrutiny given at the local level, I am sure, to what needed to go into the search warrant and its affidavit, in particular with reference to the judicial requirements for getting those particular records. And secondly, that there is a protocol, longstanding protocol in the Department of Justice that was adhered to in getting approval for that particular action.

I know and you know that the Department of Justice is now looking at this set of circumstances——

Mr. GOODLATTE. Let me interrupt you and get one more question in.

Mr. MUELLER. All I want to say is that to the extent that there are tweaks that need to be done, we are happy to abide by those tweaks.

Mr. GOODLATTE. Following the apprehension of Dzhokhar Tsarnaev, some criticized the timing of the criminal complaint against him and his initial appearance. We know the timing of these acts is set forth by the Constitution and the rules of criminal procedure. Do you believe these criminal rules are well suited to intelligence gathering from a domestic terrorism suspect, and should the Congress consider amending these rules when we are faced with a domestic terrorism situation, whereas in this case the questioning of this individual by the FBI prior to him being given Miranda warnings short circuited your opportunity to question him about imminent dangers, like other potential sites, other suspected co-conspirators, and other bombs that may have been in existence at the time, and therefore very important that the defendant—the prospective defendant be questioned?

Mr. MUELLER. Any investigator would tell you or interrogator would tell you, the longer you have, the more information that you get. And particularly in this day and age, where if you have access to the information on computers or thumb drives or what have you,

you will have a much better opportunity to get appropriate questioning accomplished. On the other hand, you have the dictates of the Constitution and the applicable statutes.

In a very narrow sliver of cases, where it is terrorism, where the threat is substantial, I would say that one could look at opportunities for giving those questioners additional time to extract information that may protect the public.

Mr. GOODLATTE. Thank you.

My time has expired. The gentleman from Michigan, Mr. Conyers, is recognized for 5 minutes.

Mr. CONYERS. Thank you. We appreciate your presence here today.

In the past week, many in the Administration have implied that because they have briefed the Congress and this Committee, that we are all complicit in the use of these surveillance tactics. Can you acknowledge here this morning that your briefing me and my staff does not constitute our assent or agreement to these programs?

Mr. MUELLER. The briefings that have been, continue to be provided to Congress is to inform Congress of how these programs are being applied, to what end they're being used, and in order to establish a dialogue as to what, if any changes need to be done to these programs, but also in furtherance of the Congress' role as the oversight body. And consequently, I don't think we look at the briefings as a form of agreement in any way, shape, or form, but look at the briefings as our obligation to inform Congress as to what is happening so if Congress wishes to take steps to change the particular statute and the applicability of a particular statute, then Congress takes the steps to do that.

Mr. CONYERS. The public's understanding of this program is that the government collects these records. Let's take the Verizon system. And they collect the records of every person in the United States and retains them for some period of time, and then queries a massive database when it has a specific concern about one of us, any one of us. Is that understanding accurate?

Mr. MUELLER. Within broad parameters, yes. But let me make two points, if I could. First, that the particular databases of metadata has no content whatsoever. We have no authority to get content. What the statute, we believe, and the FISA Court has allowed is the accumulation of metadata; that is the fact of a telephone call, the numbers called, and the time and length of those calls, and there are cases that where that has been instrumental in identifying individuals who sought to harm our country.

Mr. CONYERS. Yes, I know that, that the content isn't kept. But to have that information of who called whom, the length of time, probably where the parties were, do we need—does that serve any real purpose? I mean, is that—this puts everybody in the United States of America subject to this kind of content. We have a feeling, at least some of us, that it's not necessary, nor does it serve a legitimate legal protective purpose.

Mr. MUELLER. Would you indulge me, because I want to go back to what occurred 9/11, and which has some bearing on this. Before 9/11, there was an individual by the name of Khalid al-Mihdhar, who came to be one of the principal hijackers. He was being

tracked by the intelligence agencies in the Far East. They lost track of him. At the same time, the intelligence agencies had identified an al-Qaeda safehouse in Yemen. They understood that that al-Qaeda safehouse had a telephone number, but they could not know who was calling into that particular safehouse.

We came to find out afterwards that the person who had called into that safehouse was al-Mihdhar, who was in the United States in San Diego. If we had had this program in place at the time, we would have been able to identify that particular telephone number in San Diego.

Mr. CONYERS. Yes. I'm almost out of time.

Mr. MUELLER. I understand, but I ask indulgence just to finish because it's a critical point as to why we have this program and how important it is.

Mr. CONYERS. All right.

Mr. MUELLER. If we had the telephone number from Yemen, we would have matched it up to that telephone number in San Diego, got further legal process, identified al-Mihdhar.

One last point. The 9/11 Commission, itself, indicated that investigations or interrogations of al-Mihdhar, once he was identified, could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity was not there. If we had had this program that opportunity would have been there.

Mr. CONYERS. Mr. Chairman, let me just finish.

I am not persuaded that that makes it okay to collect every call. Look, the Verizon system, how can the government collect information on all of the Verizon system if the statute limits the government to those records that are relevant? If they are relevant, relevant under your interpretation means that anything and everything goes, and that's what you did in the example that you just gave me.

Mr. GOODLATTE. Let me say, the gentleman's time has expired. We are going to try to be very close to the 5-minute rule. And it is an excellent question. We will have to wait for the answer. We will submit the questions in writing to the Director and ask him to respond in writing to those that we don't have time to ask today.

The Chair now recognizes the gentleman from Wisconsin, Mr. Sensenbrenner, for 5 minutes.

Mr. SENSENBRENNER. Thank you very much, Mr. Chairman.

To begin, Director Mueller, let me commend you for your 12 years of very dedicated service in an agency that obviously had to change its targeting and its mission as a result of 9/11. And you and I got our jobs as leaders, me as Chairman, about the same time. You're about ready to retire. I was retired as Chairman in 2007, but I'm not about ready to retire from Congress or asking questions. So I'll begin.

Let me start out with two quotes from then Senator Barack Obama. First is, "President Bush has put forward a false choice between the liberties we cherish and the security we provide. I will provide our intelligence and the law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom."

The second quote, which comes from the same speech in Washington of August 1st, 2007, "The Bush administration acts like violating civil liberties is the way to enhance our security. It is not. There are no shortcuts to protecting America." Unquote.

Now, Director Mueller, you have served both under President Bush and through the transition to President Obama. What new privacy protections did the FBI implement under President Obama, and were those in place when the FBI applied for the FISA application that was leaked to the Guardian?

Mr. MUELLER. Well, we have internally a privacy officer. The Department of Justice has a privacy officer. I do not know specifically, but in programs such as this or other areas where we initiate collection of information, it goes through our privacy shops.

Mr. SENSENBRENNER. That's not my question, with all due respect. Were there new privacy protections that were implemented by the new President, Barack Obama, after January 20th, 2009, when he took office?

Mr. MUELLER. Are you asking were there?

Mr. SENSENBRENNER. Yes.

Mr. MUELLER. I'm not certain of the timing of additional, whatever additional privacy protections were instituted, if there were.

Mr. SENSENBRENNER. Okay. So there might not have been.

Well, I am very interested in your comment about the al-Mihdhar case, which was somebody who got on the radar screen before 9/11 and before the PATRIOT Act. Section 215 of the PATRIOT Act, which I had a hand in drafting, requires that the business records FISA warrants, or orders, be directed solely at foreigners who are the targets of an authorized terrorism investigation and not on United States citizens unless they are contacted or involved with foreigners.

Now, I don't think that Section 215 would have put a crimp on identifying al-Mihdhar if that was in place before September 11th. But my question is, with respect to the FISA order that was leaked to the Guardian, is with the narrowness that Section 215 is, and as I have described it. How can Section 215 be utilized to scoop up the phone records of American citizens who are not in communication with a foreigner who is an object of an authorized terrorism investigation?

Mr. MUELLER. To a certain extent I have to defer to the Justice Department on the legal theory and the FISA Court. I can tell you generally that there is the belief that the body of telephone toll data has in that information that is relevant, may be relevant in the future, has been relevant in the past, and that its collection in this matter thereby satisfies the requirement for relevance according to the court.

Mr. SENSENBRENNER. Well, you know, the question of relevance is the same type of question that could be issued either with a grand jury subpoena or with a national security letter without involving the PATRIOT Act. I hear you involved the PATRIOT Act in something that is done in secret, and there are no due process protections in place because the recipient of the FISA warrant can't tell what records he's turned over. And that's not the case with either national security letters or grand jury subpoenas.

Now, I guess what my concern is, is that there really isn't any way for anybody whose records are turned over to approach the FISA Court or any other court, because they don't know about it, to try to get the order quashed. And an FBI agent was the one that signed the affidavit to get that order.

And my time is up.

Mr. MUELLER. Well, let me, if I may just follow up with one observation. And that is, as we all know, these particular records are not covered by the Fourth Amendment. The Supreme Court has held that to be the case. And secondly, the determination as to the legality and that standard has been addressed by the FISA Court in the affirmative to support this particular program.

Mr. GOODLATTE. The Chair recognizes the gentleman from New York, Mr. Nadler, for 5 minutes.

Mr. NADLER. Thank you.

Let me just suggest, by the way, that that 1979 decision of the Supreme Court that a phone bill is not protected by the Fourth Amendment might not apply to a lot of the stuff today given how pervasive and privacy invading this metadata has become, compared to what could be done in 1979. So I wouldn't—I don't know that I would totally rely on that precedent to do everything that is being done.

But let me ask you the following. Under Section 215—and I also would like to associate myself with the remarks that a dragnet subpoena for every telephone—every telephone record, et cetera, every email record—although I know they don't do that anymore, but they could again tomorrow, and they did do it—certainly makes a mockery of the relevance standard in Section 215.

If everything in the world is relevant, then there is no meaning to that word. Now, some of us offered amendments to narrow that several years ago, and in retrospect maybe we should have adopted those amendments. But that's no excuse for a misinterpretation of relevance to the point that there is no such meaning to the word.

Now, secondly, under Section 215, if you've gotten information from metadata and you as a result of that think that, gee, this phone number, 873, whatever, looks suspicious and we ought to actually get the contents of that phone do you need a new specific warrant?

Mr. MUELLER. You need at least a national security letter. All you have is a telephone number. You do not have subscriber information, so you need the subscriber information. You would have to get probably a national security letter to get that subscriber information. And then if you wanted to do more——

Mr. NADLER. If you wanted to listen to the phone?

Mr. MUELLER. Then you have to get a particularized order from the FISA Court directed at that particular phone and that particular individual.

Mr. NADLER. Now, is the answer you just gave me classified?

Mr. MUELLER. Is what?

Mr. NADLER. The answer you just gave me classified in any way?

Mr. MUELLER. I don't think so.

Mr. NADLER. Okay. Then I can say the following. We heard precisely the opposite at the briefing the other day. We heard precisely that you could get the specific information from that telephone sim-

ply based on an analyst deciding that and you didn't need a new warrant. In other words, that what you just said is incorrect. So there's a conflict——

Mr. MUELLER. I'm not certain it's the same—answer to the same question. I'm sorry, I didn't mean to——

Mr. NADLER. Well, I asked the question both times and I think it's at same question. So maybe you'd better go back and check because someone was incorrect.

Mr. MUELLER. I will do that. That is my understanding of the process.

Mr. NADLER. Okay. I don't question it's your understanding. It was always my understanding. And I was rather startled the other day. And I wanted to take this opportunity to——

Mr. MUELLER. I would be happy to clarify it.

Mr. NADLER. Thank you.

Second, we have heard from Director—DNI Clapper of the terrible, horrible damage to national security done by, what's his name, Snowden, by releasing this information. I'd like to you comment on that. I don't understand how national security was breached.

We knew publicly, from 2006 at least, from the reporting in the USA Today on May 11th, 2006, about the—basically the existence of a massive NSA database of metadata from domestic phone calls. That was reported back then. We debated it in this Committee and on the floor of the House in connection with the reauthorization, I believe in 2012 and in 2008. At least several times. So that was known publicly.

The only thing that was not known as far as I can tell that was revealed was the specifics of that court order, which tell us nothing other than what was already public. Plus you could have it for whatever length of time it was. And even the stuff about Section 702, we debated that at length in the FISA Amendments Act debate a couple years ago, so that was pretty known. The only thing that may not have been known is the exact technical capabilities.

But my assumption—and tell me why you think this is not correct—is that any terrorist or would-be terrorist with half a brain in his head would assume that all electronic communications are vulnerable and may be subject to interception. And how does what what's his name just released add to that assumption or change that assumption?

Mr. MUELLER. And let me address the last point, because I often hear that any terrorist who has a brain would figure it out. The fact of the matter is there are terrorists and there are terrorists. And I can speak generally, but I cannot going into some of the more details as to specific harm to national security. But I can tell you every time that we have a leak like this, if you follow it up and you look at the intelligence afterwards, there are persons who are out there who follow this very, very, very, very closely and they are looking for ways around it.

One of the great vulnerabilities that terrorists understand is their communications, and they are consistently looking for ways to have secure communications. Any tidbit of information that comes out in terms of our capabilities and our programs and the like they are immediately finding ways around it.

And if we lose, as we—one of my problems is that we are going to lose because we've got chat, VoIP, a number of other things, lose our ability to get their communications, we are going to be exceptionally vulnerable. I ask you to get the more—the classified briefing as to more specifics. But nobody be misled in this: This hurts national security.

Now, the issue is, how do you balance that against privacy? I understand that. And you may come down differently than others, than the FISA Court, than me, perhaps. But all I can say is that there is a cost to be paid.

Mr. GOODLATTE. The time of the gentleman has expired.

The Chair recognizes the gentleman from North Carolina, Mr. Coble, for 5 minutes.

Mr. COBLE. I thank the Chairman.

Mr. Director, again, thank you for your years of service.

I want to revisit Benghazi, Mr. Director. Some recent weeks ago the former Secretary of State, Hillary Clinton, appeared before a Senate hearing and she was asked about certain facts that surrounded the Libyan tragedy, and she responded, what difference does it make? Well, I'll take umbrage with that response. Which I felt was insensitive and condescending. It may make a great deal of difference.

Having said that, we have all seen, are familiar with reports that the FBI's Evidence Response Team, the ERT, waited in Tripoli for more than 2 weeks for access to Benghazi. Some have said that this was due to bureaucratic entanglements. Do you agree with that?

Mr. MUELLER. I do not. We monitored the situation very closely after that occurrence. We had persons ready to go. Quite obviously we were in touch immediately with the State Department requesting the opportunity to go. There were a number of factors that made this as unique a situation overseas as we have seen. This isn't the first bombing that we've had of our embassies. East Africa, we had a number of years ago. But we got our people in. In this case there were a combination of factors that were the delay.

In Benghazi there is no law enforcement. Was not then. Is not now. There is nobody that you can deal with in terms of assuring your security.

Mr. COBLE. Let me ask one more question.

Mr. MUELLER. Secondly—pardon?

Mr. COBLE. Go ahead.

Mr. MUELLER. Secondly, the Libyan government. It is dependent upon getting visas from the Libyan government and the Libyan government then and today is still unstable and it's very difficult to get any decisions made from a person who is a decision maker in that arena. But I would say the bottom line is to assure the security of our people when we went in. When we could assure the security of our persons, we did go in and do our onsite review.

Mr. COBLE. Did you speak to anyone in the Libyan government about the delay?

Mr. MUELLER. We were talking through our Ambassador. I think it was the Ambassador there at the time pushing hard. I know the State Department was pushing hard. We were pushing hard. But the two concerns, the safety and the reluctance of the government

to move quickly on this, inhibited our ability to do what we wanted to do.

Mr. COBLE. Mr. Mueller, as a former prosecutor I know you are familiar with the importance of preserving a crime scene in order to assure that you can collect the maximum amount of evidence. Having said that, once the ERT arrived in Benghazi, how quickly were they able to secure that scene and begin collecting evidence?

Mr. MUELLER. Well, the ERT team went in with a military component with support from air assets and others. And I think we did it within a 24-hour period.

Mr. COBLE. Would it be fair to say that the 2-week delay in the FBI's ability to secure the scene of the attacks led to the corruption of the scene?

Mr. MUELLER. I would say that—I'm not certain I would say corruption of the scene. I would say that you always want to get to the scene as soon after the occurrence. Certainly, the scene had been entered by any number of people and it was not as pristine as we would like. Absolutely.

Mr. COBLE. Mr. Mueller, would it also be fair to say that the corrupted scene led to less evidence collection since we cannot establish the chain of custody? That is to say that the same evidence at the scene was the same when you all began as was 2 weeks prior?

Mr. MUELLER. Oh, I think yes, I would say yes. The delay adversely impacted the ability to gather evidence in a variety of ways and adversely impacted the investigation.

Mr. COBLE. Has this put a damper on our ability to pursue leads?

Mr. MUELLER. I'm sorry?

Mr. COBLE. Has this put a damper on our ability to pursue leads and/or suspects?

Mr. MUELLER. Well, you don't know what you don't know, what you may have missed. I can tell you that the investigation is ongoing. We've had some success that I can't get into today. But it is a very difficult operating environment, not just at the scene itself, but obtaining the cooperation of witnesses and others who may have information relating to the——

Mr. COBLE. My time is about up. Mr. Mueller, this Benghazi tragedy still hangs in my craw. I'm not directing this at you, but I'm directing it at somebody. We still don't know all the facts. I don't suggest there is a cover-up but it has the trappings of a cover-up. And I repeat it hangs in the craw. As my late granddaddy used to say: It makes my coffee taste bad in the morning. But we will see what happens. Thank you for being with us.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Virginia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Director Mueller, thank you for your very distinguished service.

As you know, people acquiring firearms can, with the gun show loophole and a lot of other exceptions, easily obtain a firearm without a criminal background check. What difference would a universal or virtually universal background check make?

Mr. MUELLER. Well, at the outset it would mean fewer persons who have the characteristics, ability and characteristics, would be in possession of guns.

Mr. SCOTT. On the issue of these telephone records, you've indicated how the acquisition of all telephone records helps to protect us from terrorism. Is it true that this data can be used for things other than terrorism?

Mr. MUELLER. No.

Mr. SCOTT. You can't use it for a criminal investigation?

Mr. MUELLER. No.

Mr. SCOTT. You can't use it if the purpose of the Section 104 wiretap is a significant purpose, that terrorism is a significant purpose, there may be some other purpose?

Mr. MUELLER. I'm sorry, I missed the question, sir.

Mr. SCOTT. Under Section 104 you can get the warrant, you have to show that a significant purpose of the surveillance is to obtain foreign intelligence information. "Significant purpose" was the change in the law from "the purpose," which suggests that it's the primary purpose. If it's just a significant purpose, that would leave open the idea that there is another purpose for getting the information. When I asked Attorney General Gonzales that question, what other purpose you could be using these warrants for, he blurted out criminal investigations, of course without the normal probable cause and everything else.

Is the acquisition of this information, this metadata, solely for protection against terrorism or can it be used for something else?

Mr. MUELLER. Terrorism.

Mr. SCOTT. Now, if you tripped over some other things, like you noticed a crime, could you use it in a criminal prosecution?

Mr. MUELLER. No. Not that I'm aware of. The strictures are that you cannot. Now, there may be a way to go to the court if there was an egregious crime that you get some permission of the court, but the court would have to authorize it.

Mr. SCOTT. Well, the exclusionary rule works because you don't illegally obtain evidence because if you got it you can't use it. There is a suspicion that some of us have that you're getting this information and you can use it, if you've got one of these task forces and one of the guys can get a FISA warrant, other guy can't, will you go get the FISA warrant, we'll track down, because you've got one of the guys in the place is an agent of a foreign government, so we can go listen in and see if we can't trip over a crime, then use the evidence. You're saying you can't use it for anything other than terrorism?

Mr. MUELLER. You cannot under the statute. If you are talking about 215, it says reasonable, articulable suspicion that a particular telephone number was associated with al-Qaeda or a foreign power. It's very simple.

Mr. SCOTT. Yeah, significant purpose. Not primary purpose.

Mr. MUELLER. I'm uncertain on—I'd have to go back——

Mr. SCOTT. We changed it from primary purpose to significant purpose which just opened up the idea that you could have some ulterior motive.

Mr. MUELLER. Well, on that particular language and language change, if you allow me to get back to you, I'd like to give some thought to that.

Mr. SCOTT. And so that this information that we're getting can only be used for terrorism? That's what we're hearing——

Mr. MUELLER. Yes, under 215, yes.

Mr. SCOTT. In the IRS situation there is some question as to whether some progressive groups were also targeted for scrutiny under Section 501(c)(4) abuse. But if it can be shown that only groups targeted were targeted because of political views, would that violate criminal law?

Mr. MUELLER. I'd have to—that's speculative. Excuse me just 1 second if I could.

I just wanted to check whether I was right on—I wanted to check my answers on my previous—on your previous questions. Thank you.

Mr. SCOTT. Okay. On the Boston bombing, obviously there was information out there that you could have used. Do your limited resources limit your ability to track down each and every lead that you're given and compromise your ability to protect us against terrorism?

Mr. MUELLER. We get thousands upon thousands of terrorism leads each year. The Boston office is up in that range of those number, a thousand a year. In this particular case, though, I do believe that when we got the lead on Tamerlan from the Russians, that the agent did an excellent job in investigating, utilizing the tools that are available to him in that kind of investigation. As I think you're aware, he did all the records checks. He went out to the—interviewed persons at the college where Tamerlan was there for a period of time. Ultimately, interviewed the parents. Interviewed Tamerlan himself. Sent the information back to Russia. And on three separate occasions we asked the Russians for additional information that might give us indications or evidence that he was a terrorist.

So I think we did a thorough job in following that lead. And at that point in time, I do not know that there was much else that could be done within the statutes, within the Constitution to further investigate him.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair recognizes the gentleman from Ohio, Mr. Chabot, for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman.

Mr. Director, as Mr. Sensenbrenner did, I want to thank you for your service over the years to our country. I also want to disclose that I happen to represent Cincinnati, Ohio, where some of the allegations of apparently rogue employees who were allegedly acting on their own have—were originated.

But my questions, let me begin with this. The IRS, of course, is privy to some of our citizens' most sensitive information and it's tasked with applying the law in a fair and impartial way. You would agree with that?

Mr. MUELLER. Yes.

Mr. CHABOT. Okay. However, the members of a tea party group in my district received a letter asking some pretty invasive questions, I believe. Providing all their Facebook and Twitter information, for example. Any of their advertising. They specifically mentioned a gentleman by the name of Justin Binik-Thomas—although it says Bink, B-I-N-K, it's actually B-I-N-I-K, I believe—who's just an ordinary citizen who didn't have any connection with that par-

ticular organization that received this inquiry from the IRS. And he also got no notification in that matter at all.

They also got questions about providing a list of all the issues that were important to that organization. And they wanted to know what their position was regarding each issue. And I am very concerned about the IRS' admitting to targeting conservative groups and this overly invasive line of questioning and request for information. It's really, I believe, more like harassment rather than an appropriate inquiry under 501(c)(4) status inquiries.

Now, the Attorney General announced back on May 14th that he had ordered an investigation by the FBI. Has the FBI begun that investigation now?

Mr. MUELLER. Yes.

Mr. CHABOT. Okay. And I assume that you can't go into the details of that because it's an ongoing investigation. Am I correct on that?

Mr. MUELLER. Correct.

Mr. CHABOT. Okay. Now, the IRS Commissioner, Steven Miller, initially blamed these actions, as I said, on two rogue employees way out there in the Cincinnati office, so how could we possibly know anything about that here in Washington, basically. And he acted like nobody here in this city knew anything it or was connected in any way with it.

That's become pretty clear at that point that the IRS in Washington was involved in this. And I'd like to read a couple of things here relative to Elizabeth Hofacre, who was one of the Cincinnati employees, and some of the things that she has indicated on the record. She said that the tea party cases, the patriot cases, those types of organizations that were questioned by the IRS, that they were basically in a holding pattern, their applications. She indicated that they were basically in a black hole. She had been working for 11 years at the IRS and she said the way the IRS handled the tea party cases was unprecedented.

So unprecedented, which I think is pretty significant. She said it was micromanaged to death by an IRS lawyer who worked in Washington. Again, no Washington connection, of course, but that's where this IRS lawyer was, here in Washington, D.C. And back in July 2010 the IRS developed what was called a BOLO list. Do you know what a BOLO list is?

Mr. MUELLER. No, sir.

Mr. CHABOT. Okay. Well, it stands for Be on the Look Out. BOLO, Be on the Look Out. And it instructed——

Mr. MUELLER. Well, I knew BOLO in the law enforcement context. I didn't know whether you were using it in that context.

Mr. CHABOT. Yeah, it was used in that context to send Hofacre applications from organizations involved with the tea party movement. And she told congressional investigators that she understood the purpose of the list was to target conservative and Republican groups. Other political groups did not get handled the same way, according to her. A USA Today review of tax exemptions granted at the time showed dozens of liberal groups got exemptions while tea party groups were on hold.

And subsequently there was another BOLO criteria that came down from D.C. talking about including groups whose issues in-

clude government spending, government debt and taxes, and if you're critical of the country or the direction that it's going or the way it's being run. And, again, a lot of these things sat in limbo for 27 months.

Will all these matters be investigated by the FBI no matter how high up they go?

Mr. MUELLER. I can specifically assert that all will. To the extent that there is any indication of criminal misconduct, we will follow the leads and the evidence wherever it takes us.

Mr. CHABOT. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from North Carolina, Mr. Watt, for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman.

And thank you, Director Mueller, for your service over the years. I think you have raised the standard very high and I appreciate that.

I want to follow up on—in a response that you made to a question Mr. Conyers gave you used the phrase that you thought the American people were concerned about to what end they, the programs, these two programs, are being used.

And I think that is absolutely the case. I think that was the case when we were debating the PATRIOT Act and the reauthorization of it. And the concerns that a number of us were raising at that time was to what end would these programs be used.

Congressman Scott has questioned you about some of those ends. And what I want to do is frame this based on the four things that you mentioned in your opening statement. You talked about terrorism. You talked about national security. You talked about cybersecurity. And you talked about criminal activity in your description of cybersecurity, and you said that that required public-private interaction. And all of these things have become more global, I take it, all four of those categories have become more global.

So the question I'm raising is, is there a distinction between terrorism, the purposes for which information can be used in these programs for terrorism purposes—that's why the statutes were put in place—is there a distinction between terrorism and national security?

Mr. MUELLER. I think terrorism as defined is a threat to national security, in and of itself.

Mr. WATT. Okay, but does national security include some things outside terrorism?

Mr. MUELLER. Include the what?

Mr. WATT. Some things that are outside the category of terrorism?

Mr. MUELLER. Terrorism is a separate category, but you have cyber terrorists, you have individuals, and one of the concerns we have, quite obviously in the future——

Mr. WATT. What about trade, trade as a matter of——

Mr. MUELLER. Trade——

Mr. WATT [continuing]. National security, I take it——

Mr. MUELLER. I can tell you if—I mean, one of the hypotheticals is a terrorist attack, cyber terrorist attack on Wall Street. That is trade. To the extent that you would disrupt that, then absolutely, that is a matter of national security.

Mr. WATT. So I think what—you were right that the public's concern here is what is the overlap between these four categories and to what extent can this information that is being gathered be used for things that—in the gray areas here.

I was uncomfortable that we got so preoccupied with terrorism that we compromised, I thought, personal liberties, but assume that we got comfortable with that after 9/11. What if you found something in this information that's gathered under these two programs that related more to criminal activity, serious criminal activity, the question is can that be used, anything you find in these phone dragnets, can it be used in a criminal investigation if you decide that it's not terrorist related necessarily, but could be national security related or cybersecurity related? What is the dividing line between the use of these things other than an individual agent's discretion or whatever an individual agent represents in an affidavit to the court?

Mr. MUELLER. Let me start by the use of the word dragnet. I do not believe——

Mr. WATT. I'm sorry. And I didn't intend to use it either. I really apologize. It's data gathering.

Mr. MUELLER. It's data gathering; it is not content. The statute is fairly specific that it's attributable to terrorism, and the traditional what one would understand to be terrorism, al-Qaeda and its like, and other terrorist groups that are specifically mentioned.

As I tried to point out before, the program is set up for a very limited purpose, in a limited objective, and that is to identify individuals in the United States who are using a telephone for terrorist activities and to draw that network.

Mr. WATT. Is cyber terrorism?

Mr. MUELLER. If there was——

Mr. WATT. Is cyber terrorism?

Mr. MUELLER. Sniper?

Mr. WATT. Cyber?

Mr. MUELLER. Cyber? It can be, it can be. But not as distinguished—I'd have to look at that, but I don't believe it would be covered in this particular statute. I tried to leave out the possibility that if there were a piece of evidence that was applicable to a homicide or substantial, the only way for that piece to be utilized was go back to the court and get the approval of the court to utilize this information in a way that was not covered in the original order.

Mr. GOODLATTE. The time of the gentleman has expired.

The Chair recognizes the gentleman from Alabama, Mr. Bachus, for 5 minutes.

Mr. BACHUS. Director Mueller, I also want to commend you on your service to our country.

Mr. MUELLER. Thank you.

Mr. BACHUS. And let me ask you, I have been reading about James Rosen case, the reports on it, and I find a great deal of confusion over what the Justice Department and the FBI have done and what they haven't done. You're familiar with the search warrant and the affidavit?

Mr. MUELLER. In that particular case?

Mr. BACHUS. Yes.

Mr. MUELLER. No, I'm not that familiar with it.

Mr. BACHUS. All right. Are you familiar—I mean, at the time the search warrant was issued, Stephen Kim had already been identified as the leaker of the information. Are you aware of that?

Mr. MUELLER. I am not aware of the timing, I know this was 3 years ago.

Mr. BACHUS. Yeah. No, actually in 2010, yeah, yeah, that's right, he had already been identified, I'll just tell you, if you read the affidavit, clearly he had been identified as the leaker. And I know that Attorney General Holder said he didn't know of a prosecution, you know, or wasn't a party to a prosecution of the press. But if you read the search warrant, I know that it talks about Mr. Rosen as being perhaps an aider or abetter or co-conspirator. But if you read the affidavit, he clearly was encouraging Stephen Kim to leak classified information. I mean, there is quite a bit of that. In fact he was concealing his identity and telling Kim to conceal his identity.

Now, also according to this affidavit—and I take this as being true, I know of nothing in this affidavit that has been disproved—this disclosure threatened our national security, clearly, and it probably or could have cost the life of our intelligence source in North Korea, because I'm not even sure if the person is still alive.

Now, just assuming that what I say—that assuming the affidavit is correct and that James Rosen was doing all of this information, daily contact with Kim, I know that there has been accusations that the Privacy Protection Act was violated. But, you know, it says that protects journalists from being compelled to turn over to law enforcement any work product or documentary materials, including sources, before the information contained in these materials is disseminated.

Now, it was disseminated a year before. So that I don't think is valid. It also prevents investigators from searching newsrooms to uncover information or sources that a news organization has assembled. I don't think that applies in this case. I know of no search of any newsroom or any work product.

But it says there is no protection if there is probable cause to believe the person possessing the materials has committed or is committing a crime to which the materials relate to, including receipt, possession, or communication of classified material.

Now, this affidavit contains 35 pages of very active recruiting of the State Department employee, advising him, the reporter, to use a fake email. And the search warrant was to Google. So, you know, it's has been said that they should take—the government should take reasonable steps to obtain the information through alternative sources or means than the reporter. Well, I would think Google would be an alternative source.

And there is a clear presumption—well, there isn't now, but there is a presumption I think again seizing a reporter's work product. But I would ask you to read that affidavit. And my point is simply, from reading the affidavit, I would think it's clearly within the right of the government to prosecute this reporter.

Mr. MUELLER. I can tell you two things. One, I did briefly review the affidavit when it—when the issue arose, so I am somewhat familiar with it. I can tell you that the focus of our investigations are on the person within the government has leaked the information.

Mr. BACHUS. Sure.

Mr. MUELLER. That is the focus of our investigations. And thirdly, I would say that given the issues that have been raised, that it is appropriate to go back and look at the statute that was applied to that search warrant and to the protocols that have been established in our exercise of our investigative ability when it comes to this tension between the First Amendment, on the one hand, and stopping leaks on the other hand.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. BACHUS. Let me just—Mr. Chairman—there was no prosecution——

Mr. GOODLATTE. The time of the gentleman has expired. The Chair recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

And thanks to you, Mr. Director, for your years of service to our country. I remember so well seeing you right after 9/11. You had been on the job just a handful of days. And you have certainly served our country well and honorably, and I thank you for that.

I do have, following up Congressman Bachus' questions, I do have concerns about our posture relative to the press. And I wanted to talk about the issue of the phone numbers for the Associated Press or Associated Press reporters.

The Department of Justice recently let AP know that it had subpoenaed the records for 20 phone numbers as part of a leak investigation. And the AP has said that approximately 100 of its reporters use these phones on a regular basis.

Now, one of the phones was the AP's primary number in the House of Representatives press gallery and used by many reporters, not just the AP. And this raises concerns not only about the First Amendment, but also about separation of powers. Certainly it is likely that many of the calls made by these phones were with congressional staff or Members of Congress and likely irrelevant to the leak case, but certainly do raise issues of speech and debate.

I am wondering, in the Department of Justice, the Attorney General has to personally sign off on subpoenas for reporters. In this case, since the Attorney General recused himself, the Deputy Attorney General apparently signed off. Who at the FBI needs to sign off on a subpoena request like this before it goes over to the Justice Department? Is that you?

Mr. MUELLER. No. It is at the Assistant Director level, if I'm not mistaken. I'd have to get back do you specifically.

But I believe, depending on the context and what is ordered, it would be the Assistant Director in charge of the particular division that is doing that. Generally it is the Assistant Director that handles the leak investigations.

Ms. LOFGREN. In a case like this would there be at that level consideration of the implications for chilling First Amendment rights, and would there also be an analysis of the speech and debate implications and the separation of power implications?

Mr. MUELLER. I think the flag would be raised on both of—certainly it's a leak investigation. Any leak investigation you know that you're in an environment where there are competing tensions. Any time you come across anything that implicates the legislature and Congress in some way, then that sends up a red flag and re-

quires additional scrutiny and decision as to who to—or how the investigation goes. And then you absolutely want to be with Assistant United States Attorney handling the case and deciding what steps to be taken.

Ms. LOFGREN. We would assume then in this case that the Department of Justice and the FBI decided it was okay if Members of Congress in the legislative branch were the subject of your inquiry because of the location of this phone call in the House gallery?

Mr. MUELLER. I'm not certain that that in and of itself, the fact that there is this one telephone number that is a main number would be sufficient to raise a flag of, okay, we're going to get congressional conversations across this line. And it's not across this line. It's not that at all. Because remember it's the toll records, it's a request for toll records, not conversations themselves.

Ms. LOFGREN. In terms of investigating leaks of classified information, certainly that's a worrisome issue. But why did you think it was necessary to seek records for so many telephones used by so many reporters in the AP case? Obviously many of the records under this subpoena wouldn't have relevance to the leak investigation. Did the FBI have a process for minimizing the collection of irrelevant records from the subpoena or did all the data get uploaded into FBI databases regardless of relevance?

Mr. MUELLER. Well, we are adapting, let me just say adapting special procedures to assure that the records are protected. In terms of the numbers, I'd have to leave that to the Department of Justice and it's an investigative—it's in the midst of investigation still. I will tell you that I do believe that there was a substantial effort made to minimize the request.

Ms. LOFGREN. Let me just close with this. In order to get a subpoena for the records of the reporters, they would have to be implicated in this leak investigation. Is it the FBI——

Mr. MUELLER. Did you say they would have to be implicated?

Ms. LOFGREN. The reporters. Is it the FBI practice to consider reporters, editors, and publishers who print stories about classified government matters as criminals? And how many times since you've been the FBI Director has the FBI sought reporters' work materials or communications with search warrants alleging that they are criminals?

Mr. GOODLATTE. The time of the gentlewoman has expired, but the Director may answer the questions.

Mr. MUELLER. Well, we quite obviously don't consider that category that you listed criminals in any way, shape, or form. Our focus is on identifying that individual who has those secrets and to whom that person has given the secrets. Part of that investigation goes to show the contacts between the person who is leaking the materials and the person publishing the materials. If you go to court on this you have to show that this particular set of materials that were leaked went to a particular person for publication. But the focus is on the person who is doing the leaking.

And the last part, I can't recall.

Ms. LOFGREN. Could you get back to us on that?

Mr. MUELLER. Yes, ma'am.

Ms. Lofgren. Thank you.

Mr. GOODLATTE. The gentleman from California, Mr. Issa, is recognized for 5 minutes.

Mr. ISSA. Thank you. And I would yield 10 seconds to the gentleman from Alabama.

Mr. BACHUS. Let me say I think the AP—what happened with the AP is outrageous. What I was simply saying is there is a totally different dynamic with Rosen.

Mr. ISSA. Director, you used a term just now for the gentlelady from California, you said we are in the process of. Actually, no, you said we are, and you said it in the present tense. It's fair to characterize that what you are really saying is we are now in the process of protecting that which has not been previously protected. In other words, since you used the present tense, I'm assuming that before this became very public, protections that will be in effect in the future were not in effect?

Mr. MUELLER. Well, we have protection of all of our investigations. Some investigations are protected more than others.

Mr. ISSA. But, Director, I just want to hold you to the explicitness of your word, if I may. You said it in the present tense. So is it fair—yes or no—is it fair for me to assume that there are additional efforts now underway that will be implemented?

Mr. MUELLER. Yes, yes.

Mr. ISSA. Thank you. At some time in the past was James Rosen a subject of an investigation as to criminal activity?

Mr. MUELLER. Not to my knowledge.

Mr. ISSA. Is he now a suspect in a criminal investigation?

Mr. MUELLER. Not to my knowledge.

Mr. ISSA. Thank you. So a warrant or any other document naming him as a suspect of a criminal investigation would be false?

Mr. MUELLER. Well, I don't think there is such a warrant out there.

Mr. ISSA. Okay. So any kind of documentation that alleged that he was involved in that would be a false statement? I just want to follow up on what Mr. Bachus said that, you know——

Mr. MUELLER. I know—I think I know where you're going.

Mr. ISSA. Will you get me there?

Mr. MUELLER. We're not all the way there. The colloquy and questions that you ask I am comfortable with. When you go and say conduct described in a particular entity which could or could not be subject to ultimately a prosecution.

Mr. ISSA. Okay. But it's fair to say he wasn't a suspect.

Mr. MUELLER. No.

Mr. ISSA. And we'll let the words of some documents speak for itself.

Today are you using all necessary and available resources to apprehend those people responsible for the murders in Benghazi.

Mr. MUELLER. Yes.

Mr. ISSA. To your knowledge, are the CIA, NSA, and other appropriate overseas assets being used to try to find those responsible and bring them to justice?

Mr. MUELLER. Yes.

Mr. ISSA. Is there a reason, can you explain to us—this is a little longer than the usual answer I'm sure—how it could be that we've got videos of them, we've got knowledge of who many of these peo-

ple are, in some cases by name, and yet we haven't found one of them in Libya or some other country? Isn't that unusual, to have such a cold record as far as we know today?

Mr. MUELLER. Let me explain in a couple of ways. Yes, it is unusual to have such a cold record. As I articulated before, this is a unique situation. We have had embassy attacks before. We have had our colleagues in law enforcement and the government helping us. There is no government to help us in Libya. We don't have colleagues we can go to. And so it is unique. But——

Mr. ISSA. But you have had access to the site and to people there and you do have the ability to get into Benghazi, if absolutely necessary, either you or agents on our behalf.

Mr. MUELLER. If absolutely necessary. But it is a very hostile territory, as you can understand. Nonetheless, we have video. We something there to work with, and I can tell you that we have been working with it. And that quite obviously individuals who may have participated against whom we may have evidence, whether it be video or otherwise, we are pursuing.

Mr. ISSA. Okay. Just two more quick questions. In your lifetime of law enforcement, is it a practice that you believe is appropriate to, when you have information and transcripts and other collected data, to selectively make some of it available in order to facilitate both public and witness cooperation? In other words, do you put out certain information, and, conversely, do you retain certain information? In other words, you don't put out an entire transcript or deposition, you don't put out all the evidence you have, but you do put some of it out as a matter of course in investigations in order to get people pointed. For example, you put out a picture of somebody in the case of Benghazi and yet you're retaining, I'm sure, some information that only you know.

Mr. MUELLER. We are making use of newer media, on Facebook and the like, and in the course of our investigation in Benghazi you can go on our Web site and find stills from the videos.

Mr. ISSA. Selectively picked while others were retained.

Mr. MUELLER. Picked because we want people to come forward. We did the same thing in Boston. The way we were able to identify the two responsible there was to focus in on the—identify them leaving the—at the scene and identifying them afterwards and publicizing their pictures.

Mr. ISSA. Lastly, the people responsible for Benghazi to our knowledge are not U.S. persons. Therefore, if you knew the location of them, wouldn't they be eligible for a presidential-ordered drone strike, no matter what country they were in?

Chairman GOODLATTE. The time of the gentleman has expired. The Director will be allowed to answer the question.

Mr. MUELLER. That could perhaps be answered by others than I who are more familiar with the ins and outs of the regime for undertaking such activity.

Mr. ISSA. But to your knowledge, it would be consistent with other drone strikes ordered by the President?

Mr. MUELLER. Again, I'm not that familiar with other drone strikes and I'd have to try to defer from answering that particular question on lack of knowledge and probably legal ability as well.

Mr. ISSA. Okay. Well, with the Chairman's indulgence for 10 seconds, Director, I want to thank you for your long years of service and for all that you've done for America. This is always a tough place to come, but you're always welcome.

Mr. MUELLER. Thank you, sir.

Mr. GOODLATTE. The Chair thanks the gentleman.

The gentlewoman from Texas, Ms. Jackson Lee, is recognized for 5 minutes.

Ms. JACKSON LEE. Let me start by saying, Director, we have interacted with each other for the past 11 years, and I want to thank you for your service. You are particularly one that I admire. Having graduated from the University of Virginia School of Law, you are obviously a very wise man. So, fellow alum, let me thank you and know that we will show no bias this morning, but I do want to thank you for your service.

One of the points that seemingly has not penetrated into this Committee is the enormous hit that the FBI is going to take on sequestration. You mentioned $550 million, $700 million in 2014, the other was 2013. A loss of 2,200, I think you said, 1,400.

That is going to be somewhat somewhat devastating, is that correct?

Mr. MUELLER. Yes.

Ms. JACKSON LEE. And the FBI has had a vigorous influence on the civil rights investigations of America. Yesterday was the 50th anniversary of the death of Medgar Evers. Would that impact a variety of responsibilities that the FBI has, including civil rights enforcement?

Mr. MUELLER. I can't go that far because let me tell you that when we get faced with cuts we prioritize. We would not cut counterterrorism, we would not cut counterintelligence, we would not cut cyber. The two principal criminal programs are public corruption and civil rights. They will be——

Ms. JACKSON LEE. So you would be tight, you would be tight, but you would try to do it, but you would be tight in other areas.

Mr. MUELLER. We would be tight. And as we go down that list of priorities we will be cutting and the support that you get in those investigations would be cut——

Ms. JACKSON LEE. And that's very important.

Let me just ask you about gun legislation. You are a lawyer and a strong advocate, I know, of the Constitution, the Bill of Rights. Would a gun storage bill, a universal background check—when I say that, requiring people to store their guns, universal background checks—would that seemingly infringe on the Second Amendment, just on its face?

Mr. MUELLER. The one thing I am not is a constitutional lawyer. And I understand the thrust of the question. And I understand——

Ms. JACKSON LEE. Would good laws help make us safer possibly?

Mr. MUELLER. We can always do more.

Ms. JACKSON LEE. Thank you very much.

Let me move to this question of the emails and the various public discussion, which I think is good. Do you think that we could have a significant release or significant construction interpretation of Section 501 decisions that could be declassified in a manner consistent with the protection of national security intelligence sources,

methods, and properly classified and sensitive information, meaning that the decisions of the FISA Court be declassified, keeping in mind under the restraints of national security, classified intelligence sources, et cetera? Could that occur?

Mr. MUELLER. I have to defer to the Department of Justice on that because that relates to the protocols that are set up not just by the Department of Justice, but by the FISA Court as well.

Ms. JACKSON LEE. And so opinions of the FISA Court, you think, disclosing them, you as an investigator, if it was protecting other classified, would not be open to the public and be reasonable?

Mr. MUELLER. Well, I would think that, no, there are absolutely in those opinions are matters that absolutely should remain classified.

Ms. JACKSON LEE. But some could—if they would keep that classified, others could be released?

Mr. MUELLER. I don't know that for a fact.

Ms. JACKSON LEE. With respect to Section 501, it speaks to tangible things that are part of this investigation. Do you think Section 501, that is the issue of application for order of investigation, could be narrowed somewhat?

Mr. MUELLER. I'm just not familiar with what you are talking about, ma'am. Section 501?

Ms. JACKSON LEE. It's 215, codified 501, Section 215.

Mr. MUELLER. Oh, 215. I'm sorry.

Ms. JACKSON LEE. Whether or not that would be codified, narrowed a little bit from its broadness, which is how we have gotten to where we are today.

Mr. MUELLER. I think there can be a discussion as to the scope of 215, understanding that the purpose of it, but also the impact on privacy——

Ms. JACKSON LEE. Well, let me ask these two quick questions.

Do you think what we have done over the past—what we have been disclosed is so broad that we undermine what we need to do by not narrowly focusing? And then lastly, with respect to the Boston Marathon case, I want to quickly get to that. Have you in your investigation determined why the dots were not connected as they looked at the two perpetrators' travel overseas, coming back, have you found the smoking gun on that issue? Can you go first to the question of narrowing this broad trolling, it seems to be, and still get where you needed to go.

Mr. MUELLER. Well, I wouldn't call it broad trolling, needless to say. I see it appropriate to the goal that you have. And to the extent that you narrow it, you narrow the dots that are available. You will narrow the dots that are available that may be that dot that prevents the next Boston.

On the Boston case, I think we did a very thorough job when he came to our attention. I do think there could have been better exchange of information, particularly by the Russians earlier on. That may have helped. And there were other things in terms of alerting the travel that we are fixing. But even if we fix that, even if that had been fixed prior to the Boston bombing, I do not think it would have stopped it.

But I go back to the point, yes, you can narrow, yes, you can draw a balance, but you are going to minimize the dots.

Ms. JACKSON LEE. Let me thank the gentleman again for his service. Thank you.

Mr. GOODLATTE. The time of the gentlewoman has expired.

Ms. JACKSON LEE. Thank you. I yield back. Thank you again for your service.

Mr. GOODLATTE. The gentleman from Virginia, Mr. Forbes, is recognized for 5 minutes.

Mr. FORBES. Mr. Director, I want to join the chorus of those complimenting you for your service. The unfortunate thing is so many Americans will never thank you because they don't know the harm that you kept from befalling them because of your efforts. But we thank you for that.

You have heard a lot of Members who asked you about an application for a search warrant. I gave a copy of that application to your staff before this hearing, and I think they have it to present to you now. But for the record, it's case 1:10-MJ-00291-AK document 20. With the Chairman's permission I'd ask that that be made a part of the record of this hearing.

Mr. GOODLATTE. Without objection, so ordered.

[The information referred to follows:]

AO 106 (Rev. 04/10) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

E-mail Account [redacted]@gmail.com on Computer Servers Operated by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California

Case No. 10-291-M-01

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
E-mail account [redacted]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California,

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data and more fully described in ATTACHMENT A to this application.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 793 | Gathering, transmitting or losing defense information |

The application is based on these facts:
See attached affidavit herein incorporated by reference as if fully restated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Reginald B. Reyes, Special Agent, FBI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: MAY 28 2010

*Judge's signature*

City and state: Washington, D.C.

ALAN KAY
U.S. MAGISTRATE JUDGE
*Printed name and title*

**THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **APPLICATION FOR SEARCH WARRANT** | ) | MAG. |
| **FOR E-MAIL ACCOUNT** | ) | **MISC. NO.:** 10-291-M-01 |
| **[redacted]@GMAIL.COM** | ) | |
| **MAINTAINED ON COMPUTER SERVERS** | ) | |
| **OPERATED BY GOOGLE, INC.,** | ) | **UNDER SEAL** |
| **HEADQUARTERED AT** | ) | |
| **1600 AMPHITHEATRE PARKWAY,** | ) | |
| **MOUNTAIN VIEW, CA** | ) | |

**AFFIDAVIT IN SUPPORT OF**
**APPLICATION FOR SEARCH WARRANT**

I, Reginald B. Reyes, being first duly sworn, hereby depose and state as follows:

## I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, and have been employed by the FBI for over five years. I am assigned to a squad responsible for counterespionage matters and matters involving the unauthorized disclosure of classified information, and have worked in this field since October 2005. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure of classified information, I am familiar with the tactics, methods, and techniques of particular United States persons who possess, or have possessed a United States government security clearance and may choose to harm the United States by misusing their access to classified information. Before working for the FBI, I was a Special Agent with the Drug Enforcement Administration for two years.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

The statements in this affidavit are based in part on information provided by the investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning the investigation at issue is known to me as a result of my own involvement in that investigation or has been provided to me by other law enforcement professionals. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa to compel Google, Incorporated, which functions as an electronic communication service and remote computing service, and is a provider of electronic communication and remote computing services (hereinafter "Google" or the "PROVIDER"), located at 1600 Amphitheatre Parkway, Mountain View, California, to provide subscriber information, records, and the contents of limited wire and electronic communications pertaining to the account identified as [redacted]@gmail.com, herein referred to as the SUBJECT ACCOUNT. I have been informed by the United States Attorney's Office that because this Court has jurisdiction over the offense under investigation, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. § 2703(a).[1]

4. The SUBJECT ACCOUNT is an e-mail account. As discussed below, investigation into the SUBJECT ACCOUNT indicates it is an e-mail account used by a national news reporter (hereinafter "the Reporter").

[1] See 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation . . . .").

5. For the reasons set forth below, I believe there is probable cause to conclude that the contents of the wire and electronic communications pertaining to the SUBJECT ACCOUNT, are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), and that there is probable cause to believe that the Reporter has committed or is committing a violation of section 793(d), as an aider and abettor and/or co-conspirator, to which the materials relate.

6. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that Title 18, United States Code, Section 793(d) makes punishable, by up to ten years imprisonment, the willful communication, delivery or transmission of documents and information related to the national defense to someone not entitled to receive them by one with lawful access or possession of the same. Specifically, section 793(d) states:

> (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(d). Further, section 793(g) makes a conspiracy to violate section 793(d) a violation of 793 and punishable by up to ten years imprisonment. See 18 U.S.C. § 793(g).

7. Based on my training and experience, and discussion with the United States

Attorney's Office, I have learned that "classified" information is defined by Executive Order 12958, as amended by Executive Order 13292, and their predecessor orders, Executive Orders 12356 and 12065, as information in any form that: (1) is owned by, produced by or for, or under control of the United States government; (2) falls within one or more of the categories set forth in the Order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such damage could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "TOP SECRET." Access to classified information at any level may be further restricted through compartmentalization "SENSITIVE COMPARTMENTED INFORMATION" (SCI) categories, which further restricts the dissemination and handling of the information.

8. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that the Privacy Protection Act (the "PPA"), codified at 42 U.S.C. § 2000aa et seq., defines when a search warrant impacting media-related work product and documentary materials may be executed. Section 2000aa(a) of the PPA states, in pertinent part:

**(a) Work product materials**

> Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any *work product materials*[2] possessed by a person reasonably

[1] Section 2000aa-7(b) defines the terms "documentary materials" as follows:

> (b) "Work product materials", as used in this chapter, means materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as a means of committing a criminal offense, and --

believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section *793*, 794, 797, or 798 of *title 18*, or [other enumerated statutes]) ....

**(b) Other documents**

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize *documentary materials, other than work product materials,*[3] possessed

---

(1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person;

(2) are possessed for the purposes of communicating such materials to the public; and

(3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored or created such material.

42 U.S.C. § 2000aa-7(b).

[3] Section 2000aa-7(a) defines the terms "documentary materials" as follows:

(a) "Documentary materials", as used in this chapter, means materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or

> by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—
>
> (1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section *793*, 794, 797, or 798 of *title 18*, or [other enumerated statutes]) ...

42 U.S.C. § 2000aa(a) (emphasis added). Thus, section 2000aa(a) specifically exempts from its prohibitions cases in which there is probable cause to believe that the possessor of media related work product or documentary materials has committed a violation of section 793. I have been further informed that the legislative history of the statute indicates:

> The purpose of the statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

S. Rep. No. 96-874 at 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950. I also have been informed that violations of the PPA do not result in suppression of the evidence, see 42 U.S.C. §

---

which is or has been used as, the means of committing a criminal offense.

42 U.S.C. § 2000aa-7(a).

2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees executed the search in violation of section 2000aa(a). See 42 U.S.C. § 2000aa-6(a).

## II. FACTS SUPPORTING PROBABLE CAUSE

9. In or about June 2009, classified United States national defense information was published in an article on a national news organization's website (hereinafter the "June 2009 article"). The June 2009 article was written by the Reporter who frequently physically worked out of a booth located at the main Department of State (DoS) building located at 2201 C Street, N.W., Washington, D.C.

10. The Intelligence Community owner of the classified information at issue (the "Owner") has informed the FBI that the June 2009 article disclosed national defense information that was classified TOP SECRET/SPECIAL COMPARTMENTED INFORMATION (TS/SCI). It has also informed the FBI that the information was not declassified prior to its disclosure in the June 2009 article, that the information's public disclosure has never been lawfully authorized, and that the information remains classified at the TS/SCI level to this day.

11. Following the disclosure of the classified national defense information in the June 2009 article, an FBI investigation was initiated to determine the source(s) of the unauthorized disclosure. That investigation has revealed that the Owner's TS/SCI information disclosed in the June 2009 article was first made available to a limited number of Intelligence Community members in an intelligence report (the "Intelligence Report") that was electronically disseminated to the Intelligence Community outside of the Owner on the morning of the date of

publication of the June 2009 article. The Intelligence Report was accessible on a classified information database that warned all Intelligence Community users seeking access to information in the database, through a "click through" banner, of the following:

> Due to recent unauthorized disclosures of sensitive intelligence, you are reminded of your responsibility to protect the extremely sensitive, compartmented intelligence contained in this system. Use of this computer system constitutes consent to monitoring of your actions. None of the intelligence contained in this system may be discussed or shared with individuals who are not authorized to receive it. Unauthorized use . . . is prohibited and violations may result in disciplinary action or criminal prosecution.

12. The Intelligence Report was clearly marked TS/SCI. The security markings further instructed the reader that every portion of the information contained in the Intelligence Report was classified TS/SCI and was not authorized for disclosure without permission of the Owner.

13. The investigation has revealed that one individual who accessed the Intelligence Report through the classified database on the date of the June 2009 article (prior to the publication of the article) was Stephen Jin-Woo Kim.[4] Review of government records has revealed that Mr. Kim was born on [redacted] and was naturalized as a United States

[4] So far, the FBI's investigation has revealed in excess of 95 individuals, in addition to Mr. Kim, who accessed the Intelligence Report on the date of the June 2009 article and prior to its publication. To date, however, the FBI's investigation has not revealed any other individual, other than Mr. Kim, who *both* accessed the Intelligence Report *and* who also had contact with the Reporter on the date of publication of the June 2009 article. Thus far, the FBI's investigation has revealed four other individuals who have admitted to limited contacts with either the Reporter's news organization or the Reporter anywhere from six weeks, to six months, or to nine years prior to publication of the June 2009 article. The FBI's investigation of these contacts is on-going. All these individuals have denied being the source of the June 2009 article and the FBI has not discovered any information to date that would tend to discredit their statements.

citizen in 1988.[5] Mr. Kim is a Lawrence Livermore National Laboratory employee who was on detail to the DoS's Bureau of Verification, Compliance, and Implementation (VCI) at the time of the publication of the June 2009 article. VCI is responsible for ensuring that appropriate verification requirements are fully considered and properly integrated into arms control, nonproliferation, and disarmament agreements and to monitor other countries' compliance with such agreements. On his detail to VCI, Mr. Kim worked as a Senior Advisor for Intelligence to the Assistant Secretary of State for VCI.

14. Like the Reporter's booth at DoS on the date of publication of the June 2009 article, Mr. Kim's VCI office was located at the DoS headquarters building at 2201 C Street, N.W., Washington, D.C.

15. Based on my training and experience, I have learned that classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access to classified information, that is, the individual has received a security clearance, has signed an approved non-disclosure agreement and possesses a "need to know" the information in question. If a person is not eligible to receive classified information, classified information may not be disclosed to that person.

16. Government records demonstrate that, at all times relevant to this investigation, Mr. Kim possessed a TS/SCI security clearance. As a government employee with a security clearance, and prior to the disclosures at issue, Mr. Kim executed multiple SF 312 Classified Information Non-Disclosure Agreements (NDAs) with the Government. NDAs are legally

[5] In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, the date of Mr. Kim's naturalization was erroneously reported as 1999 rather than 1988.

binding agreements between an individual being granted, or already in possession of, a security clearance, and the United States Government wherein the parties agree that the individual never disclose classified information without the authorization of the Government. The NDAs further notified Mr. Kim that the unauthorized disclosure of classified information can lead to criminal prosecution, including for violations of 18 U.S.C. § 793.

17. The Reporter did not possess a security clearance and was not entitled to receive the information published in the June 2009 article. Nor was Mr. Kim authorized, directly or indirectly, by the United States Government to deliver, communicate, or transmit the TS/SCI information in the article to the Reporter or any other member of the press.

18. Government electronic records revealed that between the hours the Intelligence Report was made available to the Intelligence Community on the morning of the publication of the June 2009 article, and the publication of the June 2009 article, the unique electronic user profile and password associated with Mr. Kim ***accessed at least three times*** the Intelligence Report that contained the TS/SCI information which later that day was disclosed in the June 2009 article.[6] Specifically, the Intelligence Report was accessed by Mr. Kim's user profile at or

[6] Mr. Kim accessed the classified database in question through his DoS work computer provided to him to process and access TOP SECRET/SCI information. The "click through" banner on Mr. Kim's DoS classified computer permits the government's review of the data contained therein. It read:

NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF STATE (DoS) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DoS COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED

around 11:27 a.m., 11:37 a.m., and 11:48 a.m. on the date the article was published. DoS security badge access records suggest that, at those times, Mr. Kim was in his VCI office suite where his DoS TS/SCI computer was located on which he would have accessed the Intelligence Report.

19. Telephone call records demonstrate that earlier on that same day, multiple telephone communications occurred between phone numbers associated with Mr. Kim and with the Reporter. Specifically:

- at or around10:15 a.m., an approximate 34-second call was made from the Reporter's DoS desk telephone to Mr. Kim's DoS desk telephone;
- two minutes later, at or around 10:17 a.m., an approximate 11 minute 35 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone;

---

ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DoS ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Further, Mr. Kim had to "click through" *an additional* banner on the classified database where he accessed the Intelligence Report, as detailed in Paragraph 11 above, which stated that "use of this computer system constitutes consent to monitoring of your actions."

Moreover, DoS policy specifically prescribes that "personal use [of DoS classified computers] is strictly prohibited; therefore, users do not have a reasonable expectation of privacy." 12 FAM 632.1.5; 5 FAM 723(2). In addition, the DoS's Foreign Affairs Manual states that DoS office spaces are subject to security inspections to insure that classified information is properly protected. Indeed, Mr. Kim's office was located in a secured facility within the main DoS building that was subject to daily inspections by rotating duty officers (sometimes including Mr. Kim himself) who were responsible for making sure that classified information in each of the offices within the facility was properly secured.

- one hour later, at or around 11:18 a.m., an approximate 3 minute 58 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone; and
- at or around 11:24 a.m., an approximate 18 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone.

20. Thereafter, telephone call records for Mr. Kim's office phone reveal that ***at or around the same time that Mr. Kim's user profile was viewing the TS/SCI Intelligence Report two telephone calls were placed from his desk phone to the Reporter.*** Specifically, a call was made at or around 11:37 a.m (at or around the same time that Mr. Kim's user profile was viewing the Intelligence Report) from Mr. Kim's desk phone to the Reporter's desk phone located within the DoS. That call lasted approximately 20 seconds. Immediately thereafter, a call was placed by Mr. Kim's desk phone to the Reporter's cell phone. This second call lasted approximately 1 minute and 8 seconds.

21. In the hour following those calls, the FBI's investigation has revealed evidence suggesting that Mr. Kim met face-to-face with the Reporter outside of the DoS. Specifically, DoS security badge access records demonstrate that Mr. Kim and the Reporter departed the DoS building at 2201 C Street, N.W., at nearly the same time, they were absent from the building for nearly 25 minutes, and then they returned to the DoS building at nearly the same time. Specifically, the security badge access records indicate:

- Mr. Kim departed DoS at or around 12:02 p.m. followed shortly thereafter by The Reporter at or around 12:03 p.m.; and
- Mr. Kim returned to DoS at or around 12:26 p.m. followed shortly thereafter by The Reporter at or around 12:30 p.m.

22. Within a few hours after those nearly simultaneous exits and entries at DoS, the

June 2009 article was published on the Internet. Following the publication of the article, yet another call was placed from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone number. This call lasted approximately 22 seconds.

23. In the evening of August 31, 2009, DoS Diplomatic Security entered Mr. Kim's DoS office space, without his knowledge, pursuant to DoS internal regulations, procedures, and computer banner authority for purposes of imaging his computer hard drives. Lying in plain view on Mr. Kim's desk next to his DoS computer was a photocopy of the June 2009 article as well as two other articles published in June 2009. All three articles were stapled together. These three articles were also observed on Mr. Kim's desk during entries made in his DoS office space on September 21 and 22, 2009.

24. On September 24, 2009, the FBI conducted a non-custodial interview of Mr. Kim concerning the leak of classified information in the June 2009 article, among other leaks of classified information. During that interview, Mr. Kim denied being a source of the classified information in the June 2009 article. Mr. Kim also claimed to have no recollection of one of the other two articles which were seen in plain view on his desk on August 31, 2009. Mr. Kim admitted to meeting the Reporter in approximately March 2009 but denied having any contact with the Reporter since that time. Mr. Kim acknowledged that DoS protocol required that he would have to go through the DoS press office before he could speak with the press. Mr. Kim stated, "I wouldn't pick-up a phone and call [the Reporter] or [the news organization that the Reporter works for]."

25. An analysis of call records for Mr. Kim's DoS ***desk phone*** reveals that between May 26, 2009 and July 14, 2009, ***36 calls*** were placed to or received from telephone numbers

associated with the Reporter, including the 7 aforementioned calls on the date of the publication of the June 2009 article. Further, there were *3 calls* during this timeframe between his desk phone and a number associated with the Reporter's news organization.

26. During the September 24, 2009 non-custodial interview, when asked by the FBI for a cell phone number to reach him in the future, Mr. Kim stated that his cell phone was "no longer active" as of the day of the interview. Mr. Kim indicated to the FBI that he would be purchasing a new cell phone with a different number.

27. An analysis of call records for Mr. Kim's ***cellular phone*** reveals that between May 26, 2009 and June 30, 2009, *16 calls* were placed to or received from telephone numbers associated with the Reporter and *10 calls*[7] were placed to or received from telephone numbers associated with the Reporter's news organization.

28. It is apparent from the foregoing both that Mr. Kim was in contact with the Reporter on multiple occasions prior to and after the publication of the June 2009 article, and that Mr. Kim did not want the FBI, who he knew was investigating the leak of classified information in that article, to know about those contacts. The FBI has also learned that, following its interview with Mr. Kim, he provided the Department of Energy (DoE) – for which Mr. Kim's permanent employer, LLNL, is a sub-contractor – with "pre-paid" cell phone number

[7] In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, it was reported that there were 11 calls between Mr. Kim's cellular phone and telephone numbers associated with the Reporter's news organization. Mr. Kim's toll records for his cellular phone do, in fact, list 11 such calls. Further review of those records suggested, however, that one of the calls may have been double counted by Mr. Kim's cellular telephone service provider. Discovering this discrepancy, the service provider was contacted and indicated that what appears to be two calls on the toll records was, in fact, only a single call. Accordingly, in this affidavit, I have corrected the total of the calls between Mr. Kim's cellular telephone and telephone numbers associated with the Reporter's news organization to reflect that there were only 10 such calls.

(sometimes referred to as a "throw away" phone) that he instructed DoE representatives to use in the future to contact him about future employment opportunities.

29. Similarly, during the same September 24, 2009 non-custodial interview, Mr. Kim told the FBI that the best e-mail address through which to contact him was [redacted]@yahoo.com. One day later, Mr. Kim e-mailed the FBI and stated that "[m]y yahoo account that I gave you is full and am [sic] going to get rid of it. I can be reached at [redacted]@gmail.com." It is apparent from the foregoing that, like his cell phone number, Mr. Kim was concerned about the FBI focusing on his [redacted]@yahoo.com e-mail account.

30. Following the FBI's interview of Mr. Kim on September 24, 2009, FBI and DoS/Diplomatic Security entered Mr. Kim's office on the evening of September 26, 2009. The stapled photocopies of the three articles containing classified information (including the June 2009 article) seen next to Mr. Kim's computer on August 31, 2009, September 21 and 22, 2009, were no longer present in Mr. Kim's office on September 26th – two days after his interview with the FBI wherein he was questioned about the unauthorized disclosures of classified information in the June 2009 article.

31. A forensic analysis of the hard drive imaged from Mr. Kim's DoS unclassified DoS computer,[8] has revealed an e-mail communication, dated July 11, 2009, from the Reporter's

[8] The "click through" banner on Mr. Kim's DoS unclassified computer permits the government's review of the data contained therein. It reads as follows:

> You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to the network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary actions, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

Nothing herein consents to the search and seizure of a privately-owned computer or other privately owned communications device, or the contents thereof, that is in the system user's home.

Further, when he first started at the DoS in June 2008, Mr. Kim signed an "Internet Briefing Acknowledgement" and "Security Briefing for OpenNet+ Account" forms, both of which stated that he understood that his use of Government provided Internet and of his OpenNet+ account "may be monitored at any time." He also signed a "Waiver Statement Form," wherein he acknowledged that he understood that

- he did "not have a reasonable expectation of privacy concerning the data on [his] computer;"
- "All data contained on [his] computer may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. For example supervisors, system personnel or security personnel may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on [his] computer."
- "Law enforcement may be authorized to access and collect evidence from [his] computer."
- "Authorized personnel will be routinely monitoring [his] computer for authorized purposes."
- "Consequently, any use of [his] computer by any user, authorized or unauthorized, constitutes DIRECT CONSENT to monitoring of [his] computer."

Similarly, while DoS policy permits limited personal use of the Internet and personal e-mail through an Internet connection, that policy also states:

Employees have no expectation of privacy while using any U.S. Government-provided access to

e-mail account to an e-mail account entitled [redacted]@yahoo.com. The e-mail from the Reporter forwarded another e-mail from other news reporters which included in its body a news article (not written by the Reporter) that would appear in the Washington Times (not the Reporter's news organization) the following day, July 12, 2009. This e-mail was found in the unallocated space located on Mr. Kim's DoS unclassified hard drive. I have been informed that when a computer file is deleted, the deleted file is flagged by the operating system as no longer needed, but remains on the hard disk drive in unallocated space unless the date is later overwritten.

32. Electronic evidence retrieved from Mr. Kim's DoS unclassified workstation also revealed that on September 24, 2009, following his interview with the FBI, Mr. Kim's user profile logged into the [redacted]@yahoo.com account through an DoS Internet connection accessed through his DoS unclassified workstation. DoS security badge access records suggest that Mr. Kim was in his VCI office suite where his DoS unclassified workstation was located when the [redacted]@yahoo.com account was accessed on September 24, 2009. While accessing that account on his DoS computer, Mr. Kim's user profile observed e-mails in that account from an e-mail account entitled [redacted]@gmail.com (which is the subject matter of the Government's request for a warrant here). Mr. Kim's profile also observed e-mails between the Reporter's work e-mail and [redacted]@yahoo.com, the e-mail account

---

the Internet. The Department considers electronic mail messages on U.S. Government computers, using the Internet or other networks, to be government materials and it may have access to those messages whenever it has a legitimate purpose for doing so. Such messages are subject to regulations and laws covering government records, and may be subject to Freedom of Information Act (FOIA) request or legal discovery orders."

5 FAM 723 (4).

identified by Mr. Kim as his own during his September 24, 2009 interview with the FBI, but which, one day later, he told the FBI was "full" and that he was "going to get rid of it."

33. During the Internet session described above on September 24, 2009, Mr. Kim attempted to clear his "Temporary Internet Files." I have been informed that deletion of Temporary Internet Files created by a web browser software application moves the cached content of internet sites visited to unallocated space, which, again, is space on the hard drive flagged by the operating system as being available for overwriting.

34. On November 9, 2009, search warrants were executed on both the [redacted]@yahoo.com and [redacted]@yahoo.com e-mail accounts. Those searches revealed multiple e-mails between Mr. Kim and the Reporter dating between May 11, 2009 and August 15, 2009. Review of those e-mails demonstrates that [redacted]@yahoo.com and [redacted]@yahoo.com are e-mail accounts used by Mr. Kim and [redacted]@gmail.com is an account used by the Reporter[9] to receive e-mails from Mr. Kim and perhaps other sources. Further, in their e-mail communication, Mr. Kim and the Reporter appear to have employed aliases (i.e., Mr. Kim is "Leo" and the Reporter is "Alex"). The content of the e-mail communications also demonstrate that Mr. Kim was a source for the Reporter concerning the foreign country that was the subject matter of the June 2009 article (the "Foreign Country") and that the Reporter solicited the disclosure of intelligence information from Mr. Kim concerning that country. A chronological listing and description of the most

[9] "[redacted]" is not the name of the Reporter. Rather, this e-mail account was apparently named after a former Deputy Assistant to President Richard Nixon who is best known as the individual responsible for the secret taping system installed in the Nixon White House, and who exposed the existence of that taping system when he testified before Congress during the Watergate hearings.

pertinent e-mails is as follows:

(a). A May 11, 2009 e-mail from [redacted]@yahoo.com to [redacted]@gmail.com reads:

> I am back from my trip. Here is my personal information.
>
> Please send me your personal cell number. I believe you have mine. It was great meeting you.
>
> Thanks,
>
> Stephen

(Mr. Kim attached to this e-mail his resume and a biographical description, both of which noted his access to classified information and his expertise concerning the Foreign Country).

(b). A May 20, 2009 e-mail from [redacted]@gmail.com to [redacted]@yahoo.com responding to the above May 11, 2009 e-mail outlines a clandestine communications plan between Mr. Kim and the Reporter. In the e-mail, the Reporter solicits Mr. Kim as a source of sensitive and/or internal government documents (italicized below). It reads:

> Your credentials have never been doubted – but I am nonetheless grateful to have the benefit of a chronological listing of your postings and accomplishments. I only have one cell phone number, on my Blackberry, which I gave you 202-[phone number for the Reporter]. Unfortunately, when I am seated in my booth at the State Department, which is much of every day, it does not get reception. thus [sic] I instruct individuals who wish to contact me simply to send me an e-mail to this address [[redacted]@gmail.com]. *One asterisk means to contact them, or that previously suggested plans for communication are to proceed as agreed; two asterisks means the opposite.* With all this established, and presuming you have read/seen enough about me to know that I am trustworthy . . . let's get about our work! What do you want to accomplish together? As I told you when we met, I can always go on television and say: *"Sources tell [name of the Reporter's national news organization]" But I am in a much better position to advance the interests of all concerned if I can say: "[Name of the Reporter's national news organization] has obtained . . ."*
>
> Warmest regards, [first name of Reporter].

[Emphasis added]

(c). Another May 20, 2009 e-mail from [redacted]@gmail.com to [redacted]@yahoo.com, the body of which states:

> Please forgive my delay in replying to you. I was on vacation out of town . . . .
>
> Yours faithfully, [first name of Reporter]

(d). A May 22, 2009 e-mail from [redacted]@gmail.com to [redacted]@yahoo.com in which the Reporter explicitly seeks from Mr. Kim the disclosure of intelligence information about the Foreign Country. It reads:

> Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors. I want to report authoritatively, and ahead of my competitors, on new initiatives or shifts in U.S. policy, events on the ground in [the Foreign Country], *what intelligence is picking up*, etc. As possible examples: I'd love to report that the *IC*[10] *sees activity inside* [the Foreign Country] suggesting [description of national defense information that is the subject of the intelligence disclosed in the June 2009 article]. I'd love to report on what the hell [a named U.S. diplomat with responsibilities for the Foreign Country] is doing, maybe on the *basis of internal memos* detailing how the U.S. plans to [take a certain action related to the Foreign Country] (if that is really our goal). I'd love to see some *internal State Department analyses* about the state of [a particular program within the Foreign Country that was the subject matter of the June 2009 article], about [the leader of the Foreign Country]. . . . In short: Let's break some news, and expose muddle-headed policy when we see it – or force the administration's hand to go in the right direction, if possible. The only way to do this is to EXPOSE the policy, or *what the [Foreign Country] is up to*, and the only way to do that authoritatively is *with EVIDENCE*.
>
> Yours faithfully, Alex.

[Emphasis added]

(e). Mr. Kim forwarded an e-mail containing the above May 22, 2009 [redacted]@gmail.com e-mail to his [redacted]@yahoo.com at 10:57

[10] "IC" is a common acronym denoting "Intelligence Community."

a.m. on the date of the June 2009 article. At the time of this e-mail, DoS badge records indicate that Mr. Kim and the Reporter were outside the DoS building, having left the building at approximately the same time. The content of the forwarded e-mail is blank, but the subject line is "Fw: Re: here."

(f). In an e-mail dated in June 2009, following the publication of the June 2009 article, the Reporter forwarded from the Reporter's work e-mail account (which spells out the Reporter's name) to the [redacted]@yahoo.com account the following e-mail from another reporter associated with the Reporter's national news organization. It reads:

> Hi [first name of Reporter] – wondering if you would like to check with your sources on something we are hearing but can't get totally nailed down over here.
>
> It seems that the [U.S. Government is concerned about something related to the Foreign Country] and is watching it very closely . . . We can't get many more details than that right now – but our source said if we could find [a specific detail] elsewhere he would give us more. Though you might be able to squeeze out a few details and we could double team this one . . . .
>
> Many thanks, dear friend . . . .,
>
> [Name of second reporter associated with Reporter's national news organization]

The Reporter then forwarded the above e-mail asking for the Reporter to "squeeze out a few details" about the Foreign Country from the Reporter's "sources" to Mr. Kim at his [redacted]@yahoo.com account and included the following introductory note:

> Leo: From the [Reporter's national news organization] Pentagon correspondent. I am at 202-[Reporter's office number at the Reporter's news organization] today.
>
> Hugs and kisses, Alex[11]

[11] One day after this e-mail was sent, toll records indicate that Mr. Kim placed a six-and-a-half minute phone call to the Reporter's office number at the Reporter's news organization (as requested in the above-referenced e-mail).

(g). An e-mail dated in June 2009 from the Reporter's work e-mail to [redacted]@yahoo.com containing a subject referencing the Foreign Country. The content of the e-mail included only the Reporter's phone number next to an asterisk (*) which, according to the May 20, 2009 e-mail described above, was the Reporter's signal that Mr. Kim should call him.[12]

(h). A July 11, 2009 e-mail from the Reporter's work e-mail to [redacted]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the intelligence community.

(i). A July 12, 2009 e-mail from the Reporter's work e-mail to [redacted]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the Foreign Country.

(j). An August 15, 2009 e-mail from the [redacted]@yahoo.com account to the Reporter's work e-mail account, which states:

> Hope you are alright but I sense that they are not.

(k). An August 15, 2009 e-mail from the Reporter's work e-mail responding to the above e-mail, and stating:

> Leo,
>
> You are most perceptive and I appreciate your inquiry. Call me at work on Monday [at the Reporter's work phone number] and I will tell you about my reassignment. In the meantime, enjoy your weekend!
>
> Alex

(The electronic signature to this e-mail following the word "Alex" identifies the Reporter by the Reporter's full name, phone number, e-mail address, and media organization).

35. The FBI conducted a second non-custodial interview of Mr. Kim on March 29,

[12] On the date of this e-mail, Mr. Kim was traveling outside of the United States. Mr. Kim's toll records do not indicate that Mr. Kim called the Reporter after this e-mail was sent. They do indicate, however, that three minutes after this e-mail was sent, a 53 second call was placed from a number associated with the Reporter's news organization to Mr. Kim's cell phone.

2010. During the interview Mr. Kim made a number of admissions, including:

- confirming that the Owner's information disclosed in the June 2009 article was national defense information and most of it, in Mr. Kim's mind, was properly classified at the TOP SECRET/SCI level;
- confirming that the same disclosures in the June 2009 article were, in Mr. Kim's mind, "egregious," "bad" and harmful to the national security in a number of respects which he described in detail;
- acknowledging that, while he could not recall the specifics of the Intelligence Report, he was "fairly certain" he had reviewed it and agreed that if electronic records indicated that he had accessed the Report then he did so;
- agreeing that the Owner's information disclosed in the June 2009 article appeared to be derived from the Intelligence Report with only one difference that he described as a "subtle nuance;"
- acknowledging that he had received extensive training on the handling of classified information, and had executed multiple classified information non-disclosure agreements with the Government;
- confirming that he understood the TS/SCI classification markings that were prominently displayed on the Intelligence Report;
- admitting that the Owner's information disclosed in the June 2009 article, to his knowledge, did not "match" information in the public domain, but advising that "bits and pieces" of the article were possibly derived from open source information;
- acknowledging that he understood the security banner on the classified computer database and that his actions were subject to monitoring;
- re-stating his false statement from his interview with the FBI on September 24, 2009, that he had no contact with the Reporter after they first met in March 2009;
- after being confronted with the evidence of his extensive contacts with the Reporter in the months after they first met, (i) first stating that his calls with the Reporter had been facilitated by an unidentified "friend" and that he did not inform the FBI of his telephone contacts with the Reporter because he did not consider then "direct contacts;" but then later (ii) openly admitting during the interview that he had "lied" to the FBI about the extent of his relationship with the Reporter because he was "scared" that the FBI might investigate him for the leak;

- while denying that he had met face-to-face with the Reporter on the date of the June 2009 article, admitting that he had met with the Reporter outside of the DoS building at other times including once following the FBI's September 24, 2009 interview;
- admitting that the emails seized during the FBI's investigation were, in fact, emails between himself and the Reporter;
- admitting, after being asked the question a number of times, that "Leo Grace" was an alias used in the e-mails for himself and that "Alex" was an alias used by the Reporter, and
- while asserting that the [redacted]@yahoo.com account pre-dated his relationship with the Reporter, stating that it was the Reporter's idea to use covert e-mail communications as a means of compartmentalizing the information and a way for Mr. Kim to "feel comfortable talking with [the Reporter]."

36. According to the FBI agents who conducted the interview, during the interview, Mr. Kim never provided a coherent explanation for the evidence of his extensive contacts with the Reporter including on the date of the leak in question. At one point, he indicated that he was communicating with the Report hoping that the Reporter "could help put him in a think tank." Mr. Kim's reaction to the evidence was mostly stunned silence, although at one point he admitted that some of the evidence was "very disturbing." Nevertheless, Mr. Kim denied that he was a source for the Reporter or had knowingly provided the Reporter with classified documents or information. Mr. Kim claimed to have specifically informed the Reporter that the Reporter "won't get stuff out of me," to which the Reporter allegedly replied, "I don't want anything." Mr. Kim did admit, however, that he may have "inadvertently" confirmed information that he believed the Reporter had already received from other individuals. Mr. Kim made further

statements which could fairly be characterized as either a confession or a near confession[13]:

- "I did not purposely discuss the [Intelligence Report], but might have discussed [some of the topics discussed in the Report]."
- "Maybe I inadvertently confirmed something . . . too stubborn to not . . . . [I] just don't know . . . someone values my views, listens up,. . . maybe I felt flattered. [The Reporter] is a very affable, very convincing, persistent person. [The Reporter] would tell me I was brilliant and it is possible I succumbed to flattery without knowing it. Maybe it was my vanity. [The Reporter] considers me an expert and would tell me . . . could use my insight. . . . The IC is a big macho game but I would never say I'm read in to this and you are not. I would never pass [the Reporter] classified."
- "[The Reporter] exploited my vanity."
- "[M]y personal and professional training told me not to meet people like [the Reporter]. I felt like while on the phone I was only confirming what he already knew. I was exploited like a rag doll. [The Reporter] asked me a lot of questions and got me to talk to him and have phone conversations with him. [The Reporter] asked me a lot, not just specific countries. [The Reporter] asked me how nuclear weapons worked."
- "It's apparent I did it. I didn't say 'did you see this?' I think I did it. I can't deny it. I didn't give [the Reporter] the [specific intelligence information in the article]. I didn't provide him with the stuff."
- "I don't think I confirmed . . . maybe I inadvertently confirmed in the context of other conversations [with the Reporter]. It wasn't far-fetched that the information was out there. I would not talk over an open line about intelligence. I did not leak classified."
- Finally, Mr. Kim opined that "someone either gave [the Reporter] the [the Intelligence Report] or it was read to [the Reporter] over the telephone."

37. During his interview, Mr. Kim also consented to a physical search of his condominium in McLean, Virginia. No hard-copy classified documents or other hard-copy materials directly related to the leak at issue were found during the search of Mr. Kim's

[13] The FBI interview was not audio or video taped. What follows are excerpts from an FBI report memorializing the interview.

condominium. During the search the FBI recovered three computers that are presently being analyzed. Thus far, no information relevant to this investigation has been identified on those computers.

38. The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence information the disclosure of which could be harmful to the United States.

39. I conclude from the foregoing that there is probable cause to believe that:

(a). From the beginning of their relationship, the Reporter asked, solicited and encouraged Mr. Kim to disclose sensitive United States internal documents and intelligence information about the Foreign County. Indeed, in the May 20, 2009 e-mail, the Reporter solicits from Mr. Kim some of the national defense intelligence information that was later the subject matter of the June 2009 article;

(b). The Reporter did so by employing flattery and playing to Mr. Kim's vanity and ego;

(c). Much like an intelligence officer would run an clandestine intelligence source, the Reporter instructed Mr. Kim on a covert communications plan that involved the e-mail of either one or two asterisks to what appears to be a e-mail account set up by the Reporter, [redacted]@gmail.com, to facilitate communication with Mr. Kim and perhaps other sources of information;

(d). To conceal further their communications, the Reporter and Mr. Kim employed aliases in their e-mail communication to each other (i.e., Mr. Kim is "Leo" and the Reporter is "Alex");

(e). The Reporter was in repeated telephone contact with Mr. Kim prior to, and on the day of, the leak of the classified information in question;

(f). On the day of the leak, Mr. Kim was on the telephone with the Reporter at or around the same time that Mr. Kim was viewing the Intelligence Report containing TOP SECRET/SCI national defense information about the Foreign Country;

(g) The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence

information the disclosure of which could be harmful to the United States;

(h). Nevertheless, the Reporter published an article on the Internet containing the TOP SECRET/SCI national defense information about the Foreign Country that was in the Intelligence Report;

(i). Thereafter, it appears the Reporter (i) returned the favor by providing Mr. Kim with news articles *in advance of their publication* concerning intelligence matters and the Foreign Country and (ii) continued to contact Mr. Kim as a source when the Reporter's colleagues needed sensitive government information about the Foreign Country.

40. Based on the foregoing, there is probable cause to believe that the Reporter has committed a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), at the very least, either as an aider, abettor and/or co-conspirator of Mr. Kim.

## III. ITEMS TO BE SEIZED

41. Further, based on the foregoing, there is probable cause to believe that evidence material to this investigation will be found in the [redacted]@gmail.com account. While the searches of Mr. Kim's e-mail accounts have revealed a number of e-mails between Mr. Kim and the Reporter, certain of those e-mails indicate that there are additional e-mail communications that have not been recovered by the FBI and that, if they still exist, would likely be found in the [redacted]@gmail.com account. Specifically, the searches of Mr. Kim's [redacted]@yahoo.com e-mail account did not reveal his responses to the May 20, 2009 or May 22, 2009 e-mails from the Reporter soliciting sensitive, internal and/or intelligence information about the Foreign Country. The May 22, 2009 e-mail from the Reporter, for example, begins "Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors." Thus, the May 22nd e-mail is a response from the Reporter to an earlier e-mail from Mr. Kim apparently inquiring as to what kind of information the Reporter

was interested in receiving. Further, the subject line of the e-mail is "Re: here," indicating that there was a prior e-mail from Mr. Kim to the Reporter with the subject line "here." That e-mail – sent from Mr. Kim to the Reporter just following the Reporter's May 20, 2009 solicitation of information from Mr. Kim – was not found in the searches of Mr. Kim's e-mail accounts. It is reasonable to believe that this and other e-mails *sent from* Mr. Kim to the Reporter would exist in the "in-box" of the [redacted]@gmail.com account. Mr. Kim's missing responses to the Reporter's e-mails would materially assist the FBI's investigation as they could be expected to establish further the fact of the disclosures, their content, and Mr. Kim's and the Reporter's intent in making them, and could be expected to constitute direct evidence of their guilt or innocence.

42. The June 2009 article was published on June 11, 2009. The Owner's information published in that article was first disseminated to representatives of the United States on June 10, 2009.

43. Further, it would materially assist the FBI's investigation to review all e-mails in the Reporter's [redacted]@gmail.com account on these two days to potentially establish by direct evidence the fact of the disclosures. Further, because we know that Mr. Kim was in contact with the Reporter through this account, it is reasonable to believe that any other sources the Reporter may have had with regard to the Foreign Country, if any, would similarly use the [redacted]@gmail.com account to communicate with the Reporter, particularly given the statement in the May 20, 2009 e-mail that the Reporter "instructs individuals who want to reach" the Reporter to send an e-mail to that account.

44. Accordingly, the FBI submits that Google should be ordered to produce in

response to this warrant:

(i) all communications, on whatever date, between [redacted]@gmail.com and Mr. Kim's known e-mail accounts, i.e., [redacted]@yahoo.com, [redacted]@yahoo.com, and [redacted]@gmail.com;[14] and

(ii) all communications "to" or "from" the [redacted]@gmail.com on June 10th and 11th, 2009.

45. While it is not required for a warrant to issue under section 2000aa, the FBI has exhausted all reasonable non-media alternatives for collecting the evidence it seeks. We seek e-mails between the Reporter and Mr. Kim that we have probable cause to believe existed. To gather that evidence, we have the option of searching either the Reporter's or Mr. Kim's e-mail accounts. Our searched of Mr. Kim's e-mail accounts have not yielded all the e-mails between him and the Reporter that our evidence to date demonstrates exist. Other than asking the Reporter for a voluntary production of the e-mails from the [redacted]@gmail.com account, there is no other way to get the evidence we rightfully seek. Because of the Reporter's own potential criminal liability in this matter, we believe that requesting the voluntary production of the materials from Reporter would be futile and would pose a substantial threat to the integrity of the investigation and of the evidence we seek to obtain by the warrant.

46. Based on the above, there is probable cause to believe that the Reporter (along with Mr. Kim) has committed a violation of 18 U.S.C. § 793(d) either as Mr. Kim's co-conspirator and/or aider and abettor, and that evidence of that crime is likely contained within the [redacted]@gmail.com account. Accordingly, the FBI's request to search the contents of

[14] A Google representative has indicated that, if ordered by a court as part of a search warrant, Google can produce e-mail communications between certain e-mail accounts.

that account falls squarely within section 2000aa(a)'s exception permitting searches of media-related work product materials, even when possessed by a national news reporter because there is "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate." 42 U.S.C. § 2000aa(a).

47. On October 2, 2009, the FBI submitted a preservation letter to Google, pursuant to 18 U.S.C. § 2703(f), requesting that the contents of [redacted]@gmail.com be preserved. On January 15, 2010, a second preservation letter for the account was sent to Google. This second preservation letter was 15 days over the 90-day limit for preservation prescribed by 18 U.S.C. § 2703(f). Thus, there remains the possibility that relevant content in the account has been deleted.[15] Nevertheless, we consider that possibility remote because, to the FBI's knowledge, in January 2010, neither Mr. Kim nor the Reporter knew that Mr. Kim was a target of this investigation nor that the existence of the [redacted]@gmail.com account was known to the FBI. On April 9, 2010, another 90-day extension of the preservation order was permitted by Google, Inc. for the account.

## IV. COMPUTERS, THE INTERNET, AND E-MAIL

48. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

(a). The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term "computer", as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or

[15] On January 21, 2010, Google refused to confirm to an FBI agent whether there is any content in the account without service of formal process.

other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider (ISP).

(b). E-mail, or electronic mail, is a popular method of sending messages and files between computer users. When a computer user sends an e-mail, it is created on the sender's computer, transmitted to the mail server of the sender's e-mail service providers, then transmitted to the mail server of the recipient's e-mail service provider, and eventually transmitted to the recipient's computer. A server is a computer attached to a dedicated network that serves many users. Copies of e-mails are usually maintained on the recipient's e-mail server, and in some cases are maintained on the sender's e-mail server.

49. Based on my training and experience, and information provided to me by other law enforcement agents, I know the following: First, searches of e-mail accounts usually provide information that helps identify the user(s) of the e-mail accounts. Second, individuals who use e-mail in connection with criminal activity, or activity of questionable legality, often set up an e-mail account to be used solely for that purpose. This is often part of an effort to maintain anonymity and to separate personal communication from communication and information that is related to the criminal activity. Third, when the criminal violation involves a conspiracy, a search of an e-mail account often allows the identification of any co-conspirators.

## V. BACKGROUND REGARDING GOOGLE

50. Based on my training and experience, I have learned the following about Google:

(a). Google is an internet services company that, among other things, provides e-mail services (known as gmail). Subscribers obtain an account by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided.

(b). Google is located at 1600 Amphitheatre Parkway, Mountain View, California. Google maintains electronic records pertaining to the subscribers of its e-mail

services. These records include account access information, e-mail transaction information, and account application information.

(c ). Subscribers to Google may access their Google accounts using the Internet.

(d). E-mail messages and files sent to a gmail account are stored in the account's "inbox" as long as they are not identified as "SPAM," the account has not exceeded the maximum storage limit, and the account has not been set to forward messages or download to an e-mail client with the option "delete gmail's copy." If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and filed sent from a gmail account will remain on the server indefinitely unless they are deleted by the subscriber.

(e). Google provides POP3 access for gmail accounts. POP3 is a protocol by which e-mail client software such as Microsoft Outlook or Netscape Mail can access the servers of an e-mail service provider and download the received messages to a local computer. If POP3 access is enabled, the account user can select to keep a copy of the downloaded messages on the server or to have the messages deleted from the server. The default setting for gmail accounts is to keep a copy of the messages on the server when POP3 access is enabled. Gmail subscribers can also access their accounts through an e-mail client such as Microsoft Outlook by using the IMAP protocol. When gmail subscribers access their accounts through IMAP, a copy of the received messages remains on the server unless explicitly deleted.

(f). A Google subscriber can store files, including e-mails, text files, and image files, in the subscriber's account on the servers maintained and/or owned by Google.

(g). E-mails and other files stored by a Google subscriber in a Google account are not necessarily also located on the computer used by the subscriber to access the Google account. The subscriber may store e-mails and other files in their Google account server exclusively. A search of the files in the subscriber's computer will not necessarily uncover the files that the subscriber has stored on the Google server. In addition, communications sent to the Google subscriber by another, but not yet retrieved by the subscriber, will be located on the Google server in the subscriber's account, but not on the computer used by the subscriber.

(h). Computers located at Google contain information and other stored electronic communications belonging to unrelated third parties. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. I also know that the manner in which the data is preserved and analyzed may be critical to the

successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Google employees are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

## VI. STORED WIRE AND ELECTRONIC COMMUNICATIONS

51. 18 U.S.C. §§ 2701–2711 is called the "Electronic Communications Privacy Act."

(a). 18 U.S.C. § 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b). 18 U.S.C. § 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> > (A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or . . . .
>
> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service –
>
> > (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission

> from), a subscriber or customer of such remote computing service; and
>
> (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c). The Government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

(d). 18 U.S.C. § 2711 provides, in part:

> As used in this chapter – (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

(e). 18 U.S.C. § 2510 provides, in part:

> (8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;...(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (15) "electronic...communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;... (17) "electronic storage" means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

(f). 18 U.S.C. § 2703(g) provides, in part:

> Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

VII. REQUEST FOR NON-DISCLOSURE BY PROVIDER

52. Pursuant to 18 U.S.C. § 2705(b), this Court can enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant because there is reason to believe that notification of the existence of the warrant will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardize the investigation. The involvement of the SUBJECT ACCOUNT as set forth above is not public and I know, based on my training and experience, that subjects of criminal investigations will often destroy digital evidence if the subject learns of an investigation. Additionally, if the PROVIDER or other persons notify anyone that a warrant has been issued on the SUBJECT ACCOUNT, the targets of this investigation and other persons may further mask their identity and activity, flee, or otherwise obstruct this investigation. Accordingly, I request that this Court enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant.

VIII. REQUEST FOR SEALING

53. Because this investigation is continuing and disclosure of some of the details of this affidavit may compromise subsequent investigative measures to be taken in this case, may

cause subjects to flee, may cause individuals to destroy evidence and/or may otherwise jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

## IX. CONCLUSION

54. Based on the foregoing, there is probable cause to believe that the Reporter has committed or is committing a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), as an aider, abettor and/or co-conspirator, and that on the computer systems owned, maintained, and/or operated by Google, Inc., there exists in, and related to, the SUBJECT ACCOUNT, evidence, fruits, and instrumentalities of that violation of section § 793. By this affidavit and application, I request that the Court issue a search warrant directed to Google, Inc., allowing agents to seize the content of the SUBJECT ACCOUNT and other related information stored on the Google servers as further described and delimited in Attachment A hereto.

Reginald B. Reyes
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this MAY 2 8 2010 day of

United States Judge
ALAN KAY
U.S. MAGISTRATE JUDGE

**ATTACHMENT A: ITEMS TO BE SEIZED**

Pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa(a), it is hereby ordered as follows:

I. **SERVICE OF WARRANT AND SEARCH PROCEDURE**

a. Google, Incorporated, a provider of electronic communication and remote computing services, located at 1600 Amphitheatre Parkway, Mountain View, California, (the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. The PROVIDER shall not notify any other person, including the subscriber(s) of [redacted]@gmail.com of the existence of the warrant.

c. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

d. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the account and files described in Section II below and all information stored in that account and files to the following FBI special agent:

Reginald B. Reyes
FBI-WFO
601 4th Street, NW
Washington, D.C. 20535
Fax: 202-278-2864
Desk: 202-278-4868

The PROVIDER shall send the information to the agent via facsimile and overnight mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

e. The FBI will make an exact duplicate of the original production from the PROVIDER. The original production from the PROVIDER will be sealed by the FBI and preserved for authenticity and chain of custody purposes.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES

a. Any and all communications, on whatever date, between [redacted]@gmail.com ("SUBJECT ACCOUNT") and any of the following accounts:

(1) [redacted]@yahoo.com,

(2) [redacted]@yahoo.com, and

(3) [redacted]@gmail.com.

"Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages (whether "to," "cc'd," or "bcc'd" to the three above-listed accounts), deleted messages, and messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" between the SUBJECT ACCOUNT and any of the three above-listed accounts, whether or not those prior emails were in fact sent between the SUBJECT ACCOUNT and the above-listed accounts;

b. Any and all communications "to" or "from" the SUBJECT ACCOUNT on June 10 and/or June 11, 2009. "Any and all communications" includes, without limitation, received messages (whether "to", "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages, deleted messages, messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files

sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" sent "to" or "from" the SUBJECT ACCOUNT on June 10 or June 11, 2009, whether or not those prior emails in the "chain" were in fact sent or received on June 10 or June 11, 2009;

c. All existing printouts from original storage of all of the electronic mail described above in Section II (a) and II(b);

d. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a) and II(b), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol (IP) address and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a) and II(b), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, methods of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

f. All records indicating the account preferences and services available to subscribers of the SUBJECT ACCOUNT described above in Section II(a) and II(b).

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT as described and limited by Section II(a) and II(b) above,

including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a) and II(b), that pertain to:

1. records or information related to violations of 18 U.S.C. § 793;
2. any and all communications between Stephen Kim and the author of the article (the "Author") that is the subject matter of the FBI investigation that is the basis for this warrant (the "Article") and any record or information that reflects such communications;
3. records or information relating to Stephen Kim's communications and/or activities on the date of publication of the Article;
4. records or information relating to the Author's communication with any other source or potential source of the information disclosed in the Article;
5. records or information related to Stephen Kim's or the Author's knowledge of laws, regulations, rules and/or procedures prohibiting the unauthorized disclosure of national defense or classified information;
6. records or information related to Stephen Kim's or the Author's knowledge of government rules and/or procedures regarding communications with members of the media;
7. records or information related to any disclosure or prospective disclosure of classified and/or intelligence information;
8. any classified document, image, record or information, and any

communications concerning such documents, images, records, or information;

9. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information;

10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified, intelligence and/or national defense information;

11. records or information related to the subject matter of the Article; and

12. records or information related to the user(s) of the SUBJECT ACCOUNT.

b. All of the records and information described above in Sections II(d), II(e), and II(f) including:

1. Account information for the SUBJECT ACCOUNT including:

(a) Names and associated email addresses;

(b) Physical address and location information;

(c) Records of session times and durations;

(d) Length of service (including start date) and types of service utilized;

(e) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;

(f) The means and source of payment for such service (including any credit card or bank account number); and

(g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:

(a) Connection time and date;

(b) Disconnect time and date;

(c) Method of connection to system (e.g., SLIP, PPP, Shell);

(d) Data transfer volume (e.g., bytes);

(e) The IP address that was used when the user connected to the service,

(f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:

(1) Connection destination;

(2) Connection time and date;

(3) Disconnect time and date;

(4) Method of connection to system (e.g., telnet, ftp, http);

(5) Data transfer volume (e.g., bytes);

(6) Any other relevant routing information.

AO 93 (Rev. 12/09) Search and Seizure Warrant

# UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

E-mail Account [redacted]@gmail.com on Computer Servers Operated by Google, Inc.,1600 Amphitheatre Parkway, Mountain View, California

Case No. 10-291-M-01

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
*(identify the person or describe the property to be searched and give its location)*:
E-mail account [redacted]@gmail.com, maintained on computer servers operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
Certain property, the disclosure of which is governed by Title 42, U.S.C. Section 2000aa, and Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data, more fully described in ATTACHMENT A to this application.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before JUN 11 2010
*(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

_____
*(name)*

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying the later specific date of _____.

Date and time issued: MAY 26 2010

_____
*Judge's signature*

City and state: District of Columbia

ALAN KAY
U.S. MAGISTRATE JUDGE
*Printed name and title*

Mr. FORBES. And, Mr. Director, is it not true that the standard for arresting an individual for committing a crime and the standard for charging and individual for committing a crime are both probable cause?

Mr. MUELLER. Yes.

Mr. FORBES. If indeed that is the standard for arresting an individual and charging them with a crime, in this application for a search warrant that we presented to you and you have been questioned about several times today your special agent, Reginald B. Reyes, certifies in this application that there is probable cause to believe that the individual involved in here, which was James Rosen, had committed or is committing a crime. And yet your testimony, as I understand it, today is that there was no potential for prosecution.

My question to you today is, if you have an individual that you know has reached the standard for arrest, the standard for charging with a crime and one of your agents has attested to that, how can you say, what standards does the Department has that says that there is no potential that that individual will be prosecuted?

Mr. MUELLER. There are any number of occasions where we may have probable cause, or facts that would purport to establish probable cause to charge somebody with something, and we do not.

Mr. FORBES. No, no, I understand that. I understand that. But how do you say before you even get the evidence, that you have reached that standard to charge someone to prosecution, how do you say that there is no potential that you will prosecute this individual when you haven't even obtained the evidence to know the extent of that crime?

Mr. MUELLER. Because a lot of the time we include search warrants and we have got cooperators who are——

Mr. FORBES. But in this case of Mr. Rosen's can you tell us if he was cooperating, or if there is any guidelines with the Department?

Mr. MUELLER. That was not my response was to your question before——

Mr. FORBES. Okay.

Mr. MUELLER [continuing]. That there are many occasions——

Mr. FORBES. In this occasion with Mr. Rosen.

Mr. MUELLER. Let me finish, sir. There are many occasions where you have probable cause to believe a person has committed a crime and you have no intention whatsoever to prosecute.

Mr. FORBES. Absolutely, I know that. But in this case can you tell us what guidelines would allow the Department, allow you to testify today under oath that there was no potential to prosecute Mr. Rosen if your agent had said that you had probable cause to charge him and to arrest him and you had not even gotten the results from the search warrant yet?

Mr. MUELLER. I'm not certain I understand the question.

Mr. FORBES. Then let me rephrase it and be very specific. You have stated that there was no potential for prosecution for Mr. Rosen. A search warrant was issued. At the time this search warrant was issued, your agent attested to the fact that that there was probable cause, the standard to both arrest him and charge him. Yet your statement is that there was no potential for prosecution at that time for Mr. Rosen. And my question is, what guideline, or

on what basis do you say that there wasn't even the potential for prosecution?

Mr. MUELLER. I'd have to go back and look at my answer, but I am not certain I stated it in that way.

Mr. FORBES. So then would you say there was at least a potential for prosecution when the search warrant——

Mr. MUELLER. I am not going to say that because I am not the prosecutor on the case. I did not have the case. And those decisions are being made by——

Mr. FORBES. I know they're ultimately being made, but you can't state today that there was no potential for prosecution, can you?

Mr. MUELLER. I'm not going to state it one way or the other.

Mr. FORBES. Okay, let me ask you this question then. I'll shift totally because you don't want to answer that question.

Since the President has been in office, we have had a 40 percent increase in gang membership in the country. We know that 48 percent of violent crimes are committed by gangs in most jurisdictions; 90 percent in some States, including the President's home State of Illinois. Can you tell us what has been the cause of the uptick in gang activity of almost 40 percent since the President has been in office?

Mr. MUELLER. Well, at the same time you talk about the uptick in the gang activity, and it has grown over a period of time, and I don't think there is any person who can say there is any one cause of increase of gang activity. It goes to a number of factors.

But by the same token, there has been a substantial, large reduction in violent crime throughout the country. New York, Chicago, there is an article, as you are familiar with, I am sure, the reduction of homicides in Chicago this fiscal year, or this year, not the fiscal year. And consequently, on the one hand you will have certain communities who have an uptick in gang violence, but you also have a number of communities who have effectively addressed that gang violence with new ways of community policing.

Mr. FORBES. Thank you, Mr. Director, but the increase has been 40 percent.

And with that, Mr. Chairman, I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman.

The gentleman from Tennessee, Mr. Cohen, is recognized for 5 minutes.

Mr. COHEN. Thank you, Mr. Chairman.

Director Mueller, I had the opportunity to go to Russia with a CODEL a couple of weeks ago, and the FSB deputy director met with us and the head of counterintelligence. They said that they had sent a memo to you, or I believe it was to the FBI, and I presume you got it, in 2011 about the Tsarnaevs, that they had been radicalized and they were fearful that they may be some threat either to us or to Russia if they returned and wanted some information about when they would return. They thought there were some laws that maybe impeded your ability to do a complete study or carry your study for a longer period of time.

I'd like to ask you this. First, did you get that paper from the FSB, or from the counterintelligence about the Tsarnaevs, number one? Number two, why could you not follow up on it further than you did and is there legislation needed to be passed to allow you

to do that, that would be keeping within the rights of American citizens? And three, are the relations between the FBI and the FSB improved to where we can share intelligence to work against the threat of radical Islam and terrorism in both of our countries?

Mr. MUELLER. In response to number one, yes, we did get what we call a tear line through our legat in Moscow in March of 2011, an agent was assigned to it and an agent did a thorough investigation; ran through all of the records checks; went to Bunker Hill Community College where he had spent time; did neighborhood research before he then interviewed the parents; and finally interviewed Tamerlan himself.

After all of those efforts, we did not find any indication that he was involved with terrorism, nor did we find predication for further investigative efforts such as wiretap or what have you.

We then reported the extent of that investigation back to the Russians and asked for any additional material they had that would assist us in furthering up additional investigation. And we got after two—actually three requests—we got no response from them.

We did, I think, all of the investigation that could have been done. Any additional information at that time I do not believe would have turned up more evidence of his ultimate radicalization.

And finally, in terms of the FSB, yes, we had a chilly period with the FSB. I, as you I think know, met with General Bortnikov several weeks before you did after Boston. They have been helpful to our investigation. We hope that we can continue to exchange information to prevent further terrorist attacks, particularly in the United States.

Mr. COHEN. Why was there not an ability to let them know that he returned to Dagestan, which was their request to know that?

Mr. MUELLER. Because we did not pick that up. When he got on the plane, there had been—and there were several reasons. And that is one of the——

Mr. COHEN. What are the reasons? The impression that I got, and this is a big leap, but they said that if they would have known, if you would have followed up and they would have known he was coming back to Dagestan, that possibly the Boston Marathon bombing would not have occurred. I presume that means they would have offed him, which would have been great.

Mr. MUELLER. Perhaps. In this particular case, the warning went to the task force and—not the warning, I should say the fact of his having left went to the task force, and for a variety of reasons, not the least of which is the case had been closed some time ago, that particular indication that he was on his way back to Russia did not get acted upon.

Mr. COHEN. Is there something that needs to be corrected? Has it been corrected? Is there a law that needs to be changed?

Mr. MUELLER. Yes, yes. No, it does not need a law. It requires a correction to our procedures, which we have done, to assure that every such notice has a recorded record. It cannot be done informally, somebody talking across the table.

Mr. COHEN. Satisfied, thank you, sir.

Let me ask you this other man, Todashev, who was killed in Florida, apparently was one of the guys that killed the three mari-

juana—you know, to get marijuana in here somewhere—those three marijuana guys up in Massachusetts.

Mr. MUELLER. I'm not certain what you're talking about.

Mr. COHEN. There was another fellow that was a friend of Tamerlan's who was in Florida and being investigated by FBI agents and they killed him. You remember that, don't you?

Mr. MUELLER. I would say that there was a response to a threat that resulted in——

Mr. COHEN. What was the threat? Because at first the reports were there was a knife or something, and then later they said there was no weapon.

Mr. MUELLER. That's still under investigation.

Mr. COHEN. How did you get knowledge of Todashev and his involvement in this crime? Was it through the FSB or was it your own investigation?

Mr. MUELLER. Actually, it was a number of ways, including one of the programs that is under scrutiny today.

Mr. COHEN. What do you mean, 215 and 702?

Mr. GOODLATTE. The time of the gentleman has expired. The Director can answer that question.

Mr. COHEN. Yeah, is it 215 and 702, is that what you mean?

Mr. MUELLER. There was effort done in terms of that particular program as well, but I will tell you that we came upon him in a variety of ways.

Mr. COHEN. Thank you, sir.

Thank you, Mr. Chairman.

Mr. GOODLATTE. The gentleman from Iowa, Mr. King, is recognized for 5 minutes.

Mr. KING. Thanks, Mr. Chairman.

Thanks, Director, for your testimony and your services.

Following up on the question, it wasn't clear to me, was the initial information on the gentleman referred to, Ibragim Todashev, was that original information from the Russians?

Mr. MUELLER. You're saying——

Mr. KING. I think I heard you say there was a variety of sources that brought you to him.

Mr. MUELLER. You're talking about the individual from Florida?

Mr. KING. Yes, who was murdered—or killed, excuse me. I don't want to imply that murder is an FBI activity.

Mr. MUELLER. It came from several leads that we were following here domestically.

Mr. KING. And was there an initial lead that perhaps came from the Russians?

Mr. MUELLER. I don't recall. There may have been, but I can't recall that there was, that he had been identified by the Russians.

Mr. KING. Are you aware of a letter from the FSB dated March 4, 2011?

Mr. MUELLER. Yes.

Mr. KING. And was that letter initiated by the Russians, by the FSB?

Mr. MUELLER. Yes.

Mr. KING. And that letter sat in a file for a while, and your response to that was how soon after that?

Mr. MUELLER. It did not sit in the file for a while. It was acted on very quickly afterwards.

Mr. KING. Did you have domestic information on Tamerlan prior to that, prior to that date of——

Mr. MUELLER. Did we have information on him prior to that date?

Mr. KING. Yes.

Mr. MUELLER. I don't believe so. Now, wait, let me just say, his name had come up——

Mr. KING. Okay.

Mr. MUELLER [continuing]. In two other cases. Those two other cases, the individuals had their cases closed. So he was one or two person away.

Mr. KING. So it is reasonable that the letter of March 4, 2011, refocused the FBI on Tamerlan?

Mr. MUELLER. Absolutely.

Mr. KING. And then are you aware of a letter also from the FSB dated April 22nd of 2013?

Mr. MUELLER. Yes.

Mr. KING. And those two letters, are they classified?

Mr. MUELLER. I am not certain what their classification level is.

Mr. KING. I would ask you to take a look at both of those letters and consider, if they are classified, to release them. The subject matter of that and the information within it, I think that Mr. Cohen and I would agree, is something that would be useful for the American people to be aware of.

And for me, I was struck by the amount of domestic information that the Russians had on activity inside the United States on Tamerlan Tsarnaev, and that seemed to be the first information that flowed forth. Is it also, to the public is my reference, is it also possible to reconstruct, going backward through the timeline, a place or places where there might have been an intervention that could have prevented the Boston bombing, knowing what we knew at the time?

Mr. MUELLER. You know, every time we have an incident like this we go back and scrub it hard. I indicated one area, and that is notification of the subject traveling should have been documented. Whatever action was taken as a result of that notification from borders and customs should have been documented. But in looking back at it, I do believe that his radicalization went forward substantially during probably the time he went to—was in Russia, but I do not believe that he was on the radar screen of the Russian authorities when he was back there.

Mr. KING. It's also my understanding. But as far as the radicalization that took place, do you see that as a long process that perhaps started when he was younger and was a product of his home country, the United States and back to his home country, or how do you view the radicalization?

Mr. MUELLER. I think the best you can say is maybe in fits and starts.

Mr. KING. Okay. And I think that's fair. The security, though, when we have people coming in from, let's say, the North Caucasus region, who are persons that come from, let's say, a profile that would fit persons of interest from Nations of interest, do we do in-

quiries with the Russians or any other country to do background checks on those individuals that might be seeking asylum here in the United States that come from those areas?

Mr. MUELLER. You'd really have to turn to DHS in terms of what they consider, in terms of evaluating the asylum. Well, I think really DHS——

Mr. KING. But don't they subcontract that out to you? Doesn't USCIS ask FBI to do the background checks?

Mr. MUELLER. I don't think they contracted us.

Mr. KING. Shorthand.

Mr. MUELLER. I think they run records checks through us to see what derogatory material we may have on somebody who's seeking asylum.

Mr. KING. But are you aware of any inquiries that might ask the Russians to give us some advice on who they might be watching that's coming into the United States under asylum, which is how Tamerlan got here?

Mr. MUELLER. I don't know, because I can't speak to what the FSB does in all of its cases, but if they have a person they believe to be a terrorist, I would say often they give us that information and ask for assistance from us to address that particular person.

Mr. KING. Let me suggest that in a direct question of Mr. Beseda's, who's second in command at FSB, he said that those kind of inquiries, he couldn't say it never happened, but as he looked at the other people on the panel, they seemed to think there was one inquiry perhaps 10 years ago. His specific response was those inquiries are nil.

So I'm going to suggest to this panel that we need to take a good look at how we do background checks on people that are coming from Nations of interest, who likely are persons of interest, to tighten up our security. And I think that was a window, and there might be hundreds and perhaps more than hundreds that come through a window like that.

I thank you for your service, and I yield back the balance of my time.

Mr. GOODLATTE. The time of the gentleman has expired.

The Chair recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Director Mueller, thank you for your many years of exemplary service to the Nation. This will probably our last time seeing you before this particular Committee. And I wanted to do that. I wanted to give you that.

And I will also agree with you that as terrorism, both foreign and domestic, changes and adapts, our law enforcement capabilities have to do the same. And so if data collection will help us remain secure in our personal liberties, then that's a discussion that we should have. And if we don't have security, then our civil liberties are definitely threatened. And I know that everyone can agree with that.

And this is an issue, unlike those that some of my colleagues on the other side of the aisle are looking for out in the backyard—Benghazi, IRS, the Rosen subpoena—we can deal with those things, but there are some issues right at the front door knocking

loudly. And I think the loudest knock is coming from data collection and secrecy in government. And so my questions would be regarding that.

Why is it necessary for data collection, internal domestic data collection, to be a secret? Why is it that that program has to be a secret? I disagree with the notion that public knowledge of those programs can undermine our ability to respond to terroristic or terrorist threats.

And I also want to applaud the work of companies like Google that work very hard to make government legal requests as transparent as possible. This week Google requested permission from you and the Attorney General to publish aggregate numbers of national security requests, including FISA disclosures, as part of its transparency report.

Wouldn't the aggregate publication of national security requests, kind of like metadata, wouldn't that better serve the conversation on civil liberties and national security than keeping Americans in the dark? Because as we keep Americans in the dark, it tends to break down the trust that Americans have for government. I'm really concerned that we have too much classified information, and I'm disturbed or perplexed, actually, about who actually decides what should be classified and how do we go about unclassifying things?

So I know that's a couple of questions. I want to give you a chance to respond.

Mr. MUELLER. I do think that there is quite obviously a tension between the secrecy attendant, classification attendant to certain programs and documents, and I am not going to say that there aren't occasions where there are things that are overclassified. When it comes to identifying the way we handle communications and all their iterations, particularly in this day and age when you have any number of ways to communicate, whether it be email, chat, and a variety of alternate ways of communicating, to the extent that those were associated with terrorist groups, or actually those associated with the Chinese, the Russians, the Iranians, and the others, to the extent that that they have information as to how we operate in terms of how we identifying——

Mr. JOHNSON. Well, how we may use those programs, but the programs themselves, why is it that just a broad disclosure that, yes, Americans, we are collecting metadata from your phone records and this is why we are doing that, and then you explain the intricacies of what you're doing, what you're not doing. You're not talking about any specific programs or operations—excuse me, no specific operations or operatives, those kinds of things, but just the existence of the program. Americans need to know what is being done and why.

Mr. MUELLER. All I would say is, there is a balance to take. I would urge you to, in the classified briefings, to ask that question and see what——

Mr. JOHNSON. Well, I have, and I've never gotten a satisfactory answer.

Mr. MUELLER. Well, I can tell you because whenever there are disclosures like this, we see, through other programs we have and

intercepted communications, we see exactly what those individuals are doing, the terrorists, to change their communications.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. JOHNSON. There will always be that adaptation to what we're doing.

Mr. GOODLATTE. The Chair recognizes the gentleman from Texas, Mr. Gohmert, for 5 minutes.

Mr. GOHMERT. Thank you, Mr. Chairman.

And thank you, Director. I'm not going to comment about your being the last time here. I did that a few years ago, and didn't turn out right. But anyway, I want to follow up on what my friend Mr. Johnson was talking about, the overclassification issue, because it does seem to be a problem and certainly an issue.

There is an article today entitled "Obama's Snooping Excludes Mosques, Missed Boston Bombers." I wasn't aware of the—and I went to the FBI Web site—I wasn't aware of the Sensitive Operations Review Committee, so I wanted to find out what it was. Well, apparently, if something involves things like news media, religious or domestic, political organization, things like that, then it has to go before the Sensitive Operations Review Committee in order to be approved. And here is the information on the data about if it's a political organization, like a Tea Party, a religious organization, like evangelical Christians, which the Department of Homeland Security is so afraid of, or a mosque, apparently, it has to get approval here, and we already knew and we have gone through with—and it seemed ridiculous to me and Michele Bachmann and Lynn Westmoreland that the material we were reviewing that was purged by subject matter experts was classified.

It would seem that if you're trying to make the Islamists feel better about training materials, you'd want them to see what they were removed. And I'm just curious, why are the subject matter experts that the FBI had go through all their training material and purge anything that might be offensive to an Islamist, why was that needed to be classified? I would think they'd be heroes in the Islamic world for getting that stuff out. Why was that classified?

Mr. MUELLER. Well, we went through a thorough review. I think you have been fully briefed on it. In those materials are examples of cases——

Mr. GOHMERT. Well, I need you, I have just a short time, I need you to answer questions, and my question is, why were the subject matter experts' identity classified?

Mr. MUELLER. Because the process in whole had within its parameters all information that we have in the Bureau, and if I am not mistaken, we gave you the names of the individuals.

Mr. GOHMERT. In a classified setting. And so I'd get prosecuted if I revealed them. And I don't know why you can't make those public, so the people would know. But obviously, you feel——

Mr. MUELLER. I will look at that and——

Mr. GOHMERT. Well, and also I want to go back to Boston. You said things like, and out of the example what you said, the FBI did an excellent job, did a thorough job, don't know what else we could have done. And according to the Russians, there was a great deal more that could have been done. And when we find out about this Sensitive Operations Review Committee, and as this article points

out, if it's true, it says that we don't know who the chairman and members are of the Sensitive Operations Review Committee, who the staff, that's kept secret. The FBI never canvassed Boston mosques until 4 days after the April 15 attacks.

If the Russians tell you that someone has been radicalized and you go check and see the mosque that they went to, then you get the articles of incorporation, as I have, for the group that created the Boston mosque where these Tsarnaevs attended, and you find out the name Al-Amoudi, which you will remember, because while you were FBI Director this man who was so helpful to the Clinton administration with so many big things, he gets arrested at Dulles Airport by the FBI and he is now doing over 20 years for supporting terrorism.

This is the guy that started the mosque where your Tsarnaevs were attending, and you didn't even bother to go check about the mosque? And then when you have the pictures, why did no one go to the mosque and say, who are these guys? They may attend here. Why was that not done since such a thorough job was done?

Mr. MUELLER. Your facts are not altogether——

Mr. GOHMERT. I point out specifically.

Mr. MUELLER. May I finish my——

Mr. GOHMERT. Point out specifically. Sir, if you're going to call me a liar, you need to point out specifically where any facts are wrong.

Mr. MUELLER. We went to the mosque prior to Boston.

Mr. GOHMERT. Prior to Boston?

Mr. MUELLER. Prior to Boston happening, we were in that mosque talking to the imam several months beforehand as part of our outreach efforts.

Mr. GOHMERT. Were you aware that those mosques were started by Al-Amoudi?

Mr. MUELLER. I've answered the question, sir.

Mr. GOHMERT. You didn't answer the question. Were you aware that they were started by Al-Amoudi?

Mr. MUELLER. No.

Mr. GOHMERT. You were not. Okay. Thank you.

Mr. GOODLATTE. The time of the gentleman has expired.

The Chair recognizes the gentleman from Puerto Rico, Mr. Pierluisi, for 5 minutes.

Mr. PIERLUISI. Thank you, Mr. Chairman.

Director Mueller, I want to join my colleagues in thanking you for your service to our Nation. You will leave a lasting legacy and large shoes to fill.

As you have recognized, the FBI's role since 9/11 has evolved and expanded. Prior to the attack, the agency's primary responsibility was to fight domestic crime, including violent crime. Now the Bureau also stands at the forefront of the government's efforts to prevent and respond to terrorism. And as the tragic events in Boston illustrate, the stakes could not be higher. Conducting both law enforcement and counterterrorism operations is a large and complex portfolio, and I know you are constantly reviewing the allocation of personnel and resources to ensure that both missions receive the attention they deserve.

The example of Puerto Rico, though, a U.S. territory, home to 3.7 million American citizens, underscores why it is important for the FBI, notwithstanding its transformation in the wake of 9/11, to continue to place great emphasis on its traditional role as a crime-fighting agency. As Chairman Michael McCaul noted at a hearing last year in the Homeland Security Committee, the people of Puerto Rico are under siege. Like all American citizens, my constituents are targets for al-Qaeda and its affiliated organizations. They, too, worry about terrorism when they board a plane, visit a tourist site with their children, or travel abroad. Indeed, in 1972, 16 American citizens from Puerto Rico were killed and many more were wounded at an airport in Israel, the victims of one of the first incidents of international terrorism.

But the fact is, my constituents are dying violent deaths every day and they are not being killed in terrorist attacks. Rather, they are dying in huge numbers because of the toxic mix of drugs, guns, local gangs, and transnational criminal organizations.

I know you are familiar with the statistics, but they bear repetition. In the 10-year period between 2003 and 2012, there were 8,600 homicide victims in Puerto Rico. The year 2011 was the most violent in the territory's history with 1,164 murders. That is the equivalent of over three homicides a day, every day. It is about the same number of homicide deaths as Texas, which has a population that is seven times that of Puerto Rico.

Although the number of murders in Puerto Rico decreased in 2012, the island's per capita murder rate was still about three times higher than any State and about six times higher than the U.S. national average.

As you know, I have urged the Federal Government to surge resources to Puerto Rico to alleviate this crisis. Earlier this year, following a visit by Secretary Napolitano to Puerto Rico, DHS decided to substantially increase its presence on the island. Next week, I am meeting with a senior advisor to the Secretary to receive an update on the steps that DHS component agencies are taking and the results that we can expect to see.

Yesterday, the Appropriations Committee approved the Defense Appropriations Act for Fiscal Year 2014, and that bill directs the Secretary of Defense to provide a report on the counterdrug activities that DOD is undertaking or intends to undertake to support law enforcement operations in and around Puerto Rico.

In March, I wrote a detailed letter to Attorney General Holder, copying you, reiterating my request that DOJ surge resources to Puerto Rico. It is clear that the FBI, along with DEA and ATF, needs to do more, much more to reduce the level of violence in Puerto Rico and to reassure my constituents that their national government cares about them and is working every day to protect them and their families.

Director Mueller, can you please tell me what concrete steps the FBI is taking or will take to reduce the exceptionally high level of violence in Puerto Rico? The threat has evolved in terms of both its nature and its severity, and it is critical that the FBI's response evolve as well. The time for business as usual, is over, Director.

Mr. MUELLER. Well, as we have discussed previously, Congressman, I am tremendously sympathetic to what is happening in

Puerto Rico as we go along. We have made advances. We have added hybrid squads to cover any kind of crimes. We have got four violent gang Safe Street Task Forces. That is more than I think any office in the country. We have an allocation of 313 full-time agents; they are fully staffed. We're about five down.

But I can tell you, under this term of sequestration, the possibility of allocating additional resources to Puerto Rico is very, very difficult. I, having been a homicide prosecutor, I think I have some understanding of the devastation to communities that are beset by violent crime. I wish we could do more. I wish we had the resources to surge. I know we're working closely with ATF, DEA, and ourselves to combine our resources along with the Puerto Rican National Police, and we're having some success. All I can tell you is that I wish I could do more at this point, but given the budget constraints, it would be very difficult.

Mr. GOODLATTE. The time of the gentleman has expired.

The Chair recognizes the gentleman from Ohio, Mr. Jordan, for 5 minutes.

Mr. JORDAN. Thank you, Mr. Chairman.

Director, this past Sunday, Mr. Cummings, Ranking Member on the Oversight Committee, said based on everything he's seen regarding the IRS case, based on everything he's seen, the case is solved. Is Mr. Cummings accurate in his assessment.

Mr. MUELLER. Could you repeat that, if you would?

Mr. JORDAN. Based on everything I have seen, according to Mr. Cummings, the case is solved. This is regarding the IRS scandal.

Mr. MUELLER. Which case?

Mr. JORDAN. The IRS case.

Mr. MUELLER. The IRS case?

Mr. JORDAN. Yes.

Mr. MUELLER. The IRS case is currently under investigation, and basically it's just started.

Mr. JORDAN. Yeah. What can you tell us? I mean, you started a month ago. What can you tell us about this? Have you found any—have you found the now infamous two rogue agents? Have you discovered who those people are?

Mr. MUELLER. Needless to say, because it's under investigation, I can't give out any of the details.

Mr. JORDAN. Can you tell me some basics? Can you tell me how many agents, investigators you have assigned to the case?

Mr. MUELLER. I may be able to do that, but I'd have to get back to you.

Mr. JORDAN. Can you tell me who the lead investigator is?

Mr. MUELLER. Off the top of my head, no.

Mr. JORDAN. This is the most important issue in front of the country the last 6 weeks, you don't know who's heading up the case, who the lead investigator is?

Mr. MUELLER. At this juncture no, I do not know who they are.

Mr. JORDAN. Can you get that information to us? We would like to know. We would like to know how many people you have assigned to look into this situation.

Mr. MUELLER. I have not had a recent briefing on it. I had a briefing on it when we first initiated it, but I have not had a recent briefing as to where we are.

Mr. JORDAN. So you don't know who is leading the case?

Mr. MUELLER. I do not know who is the lead agent.

Mr. JORDAN. Do you know if you have talked to any of the victims? Have you talked to any of the groups who were targeted by their government? Have you met with any of the tea party folks since May 14, 2013?

Mr. MUELLER. I don't know what the status of the interviews are by the team that's on it.

Mr. JORDAN. Would you expect that that's been done?

Mr. MUELLER. Certainly at some point in time in the course of the investigation it will be done, but generally at the outset of the investigation you get the documents so that you can have a——

Mr. JORDAN. But don't you normally talk to the victims?

Mr. MUELLER. I do not know specifically——

Mr. JORDAN. In your extensive record and history in investigative work, don't you typically talk to the victim? It is a criminal investigation. Don't you typically talk to the victims pretty soon?

Mr. MUELLER. Absolutely. I'm sure it will happen.

Mr. JORDAN. So did the FBI contact any of these same victims, were they contacted by the FBI prior to the investigation? When these same groups were applying for tax-exempt status, did the FBI pay some of these individuals a visit?

Mr. MUELLER. I do not know.

Mr. JORDAN. Pardon?

Mr. MUELLER. I do not know.

Mr. JORDAN. You don't know?

Mr. MUELLER. I do not know.

Mr. JORDAN. Some of them testified that they were paid a visit by the FBI. Specifically, Catherine Engelbrecht in Texas said she was visited by the FBI. She was head of True the Vote. Is that true or not?

Mr. MUELLER. Do not know.

Mr. JORDAN. You do not know, okay. If the FBI did contact people involved in the IRS scandal, victims groups, prior to the investigation when they were applying for tax-exempt status, why was that the case? Why would you be looking into it? And was there possibly coordination with the IRS——

Mr. MUELLER. You are asking me details about the investigation. I would be happy to get back to you.

Mr. JORDAN. I'm not asking you details about the investigation. I'm saying, why were people targeted before the investigation started? Why were they contacted by the FBI, people who are now part of tea party groups who were targeted by the IRS?

Mr. MUELLER. You're asking questions about details of the investigation. I would be happy to take the questions.

Mr. JORDAN. That is not a detail about the investigation. That took place prior to the investigation starting.

Mr. MUELLER. May I finish? May I please finish? You are asking detailed questions about the investigation. I'd be happy to get back to you and answer those questions that I can, understanding ongoing——

Mr. JORDAN. I'm asking basic questions about the investigation, like who's heading it up, and you can't tell me that. Can you get back to me on any group who was targeted by the IRS, who the

FBI visited with prior to the investigation starting while they were applying for tax. That would be important information for this Committee to have. Can you get that to me?

Mr. MUELLER. We'll look at the questions and try to respond.

Mr. JORDAN. Have you reviewed the Inspector General's report regarding the IRS scandal?

Mr. MUELLER. I have been through it, yes.

Mr. JORDAN. Do you have any concerns about the way the Inspector General did the report and collected information?

Mr. MUELLER. I did not focus on that at all. I was looking——

Mr. JORDAN. Well, let me ask you a couple things. Is it typically important for the investigator to have one of the central players in this, Ms. Holly Paz, who was Director of—one of the key players at the Tax Exempt Division, sit in on all the interviews, almost all the interviews with employees in that division? Is that typically how an investigation is done?

Mr. MUELLER. I am not familiar with those circumstances. I understand what you are saying about those circumstances, so not being familiar with it, I can't——

Mr. JORDAN. In your time as an investigator is that how you would do interviews, with the boss sitting next to the person you are trying to get information from?

Mr. MUELLER. Well, again, I'm——

Mr. JORDAN. Is it appropriate for Holly—the Inspector General came out in a transcribed interview that our staff has done, the Oversight Committee staff has done, is it appropriate to have her collect the data and give it to the Inspector General?

Mr. MUELLER. I am not familiar with the——

Mr. JORDAN. If that happened, is that appropriate?

Mr. MUELLER. I'm not going to speculate.

Mr. JORDAN. Let me ask one last thing, because this did happen. Mr. Chairman, the last question.

So is it appropriate when the Inspector General is doing his investigation, doing his audit, to give information to the very people he is investigating in the course of the investigation and not share that same information with the Oversight Committee? Specifically, May 30 of last year, the Inspector General told Doug Shulman that the terms tea party, patriot, 9/12 were used to identify groups and put them on a list. He told them that was going on at the IRS. He told them that a year ago. Four days later he told the general counsel at Treasury, Chris Meade, the same information, but did not share that with the Committee who asked for the investigation, the Committee who has oversight over the Inspector Generals in all Federal agencies, did not share that information with us. Is that typically how an investigation is supposed to work?

Mr. MUELLER. Again, you are talking about circumstances with which I am not familiar. Each investigation is a little bit different, and I really can't comment on what was appropriate in that particular investigation without knowing and sitting down and going through the facts.

Mr. JORDAN. But that's—if I could, Mr. Chairman, then I will stop—that's the point. You've had a month now to investigate. This has been the biggest story in the country and you can't even tell me who the lead investigator is. You can't tell me that actions the

Inspector General took, which are not typically how investigations are done, you can't tell me if that's appropriate or not? This is not speculating. This is what happened and you can't tell me how many agents are assigned to the most important news story, maybe the most important——

Mr. GOODLATTE. The time of the gentleman has expired. The Director will be allowed to answer the question. And if he can't answer it today, we would definitely expect that he answer it in writing to us as promptly as possible.

Mr. MUELLER. Yeah, I would be happy to take your questions in writing, sir.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from Washington, Ms. DelBene, for 5 minutes.

Ms. DELBENE. Thank you, Mr. Chair.

And thank you, Mr. Director, for your service and for being with us here today.

I happen to agree with those who believe that greater transparency and better data about the requests that government entities are making to Internet companies and providers will help inform the discussion that we're having about how to balance legitimate national security needs with privacy rights.

I understand it was referred to a little bit earlier that Google sent a letter to you and Attorney General Holder earlier this week. I'm requesting that it be permitted to provide the reports of the number of FISA national security requests it receives as well as their scope. And I wondered if you could share with us what your response is to that request.

Mr. MUELLER. I think that's being looked at by Justice at this point.

Ms. DELBENE. Okay. Then earlier this year, Google did work with the Department of Justice and the FBI to disclose in broad strokes the number of national security letters that Google receives. And did Google's disclosures of these numbers harm national security in any way?

Mr. MUELLER. Well, let me just hypothesize without answering particularly. If you had such figures out there, would not somebody who wanted to have secure communications maybe make some decisions as a result of that information as to what, you know, as to what communications capability they use?

Basically, there are issues that need to be discussed in the course of deciding what needs to be declassified. I think most of us in the government would love to be able to disclose more because it would be more understandable to persons, but you have the conflicting values of trying to protect the country and trying to protect that information that enables us to continuously identify and to intercept the communications of terrorists in an effort to thwart attacks. That's the conflict.

Ms. DELBENE. Thank you. The Committee is currently also considering reform of the Electronic Communications Privacy Act. And as you may know, the Senate Judiciary Committee recently reported reform legislation out of Committee. Members on both sides of the aisle seem to agree that we've failed to modernize our law to align with reasonable expectations of privacy, especially in the digital age.

For routine criminal investigations, I believe law enforcement should use the same standard to search your inbox that they do to search files and letters in your home, but our current outdated law allows police to provide only a subpoena, issued without a judge's approval, to force service providers to turn over emails that have been opened or are more than 6 months old.

The Committee is currently considering legislation that would require government entities to obtain a warrant before having access to stored content. And I'm pleased that the Department of Justice and Attorney General Holder recently acknowledged that reform to the Electronic Communications Privacy Act has failed to keep up with the development of technology. And I wanted to know if you agree that it's time to reform these laws to include a warrant standard for stored content?

Mr. MUELLER. Well, I would agree that it's time to relook at these laws given the communications in terms of what the impact on—it would have on particular requirements in particular situations. I would wait to see what kind of legislation is proposed.

Ms. DELBENE. Do you have a proposal, what kind? Right now if I, you know, have a physical letter, a piece of paper in my home, you need a warrant. If I have an online piece of communication it doesn't necessarily have the same standard.

Mr. MUELLER. We'd be pleased to get back to you either by regular letter or by email.

Ms. DELBENE. And in terms of broader reform, in terms of keeping up, do you have recommendations on other reforms you think that we need to look at because the way that folks communicate now is very different than in the past? You talked about chat and other forms. Clearly, our laws have not kept up with the changes in technology, and do you have an opinion or ideas of how you would like to see legislation formed there?

Mr. MUELLER. We will get back to you on that with whatever ideas we have.

I do think there needs to be reform. There is always impetus to increase the standards to get particular documents, but it should be done, in my mind, dependent on the attributes of privacy that are necessary for a particular means of communication or a particular piece of data relating to communications. If you raise a standard too high, we then do not get the basic information that can identify terrorists to the point where then we could take the additional investigative steps, identify the subscriber. Once we have identified the subscriber, identify others in that network.

If we, as a result of that predicated level of investigation find that they are involved in terrorism, then getting a wiretap. We tend to confuse that which is covered by the Fourth Amendment, that which is not covered by the Fourth Amendment. And so as one drafts the legislation, my belief is that ought to be kept in mind.

Ms. DELBENE. Thank you.

And thank you, Mr. Chair. I yield back.

Mr. GOODLATTE. The Chair thanks the gentlewoman, and recognizes the gentleman from Utah, Mr. Chaffetz, for 5 minutes.

Mr. CHAFFETZ. Thank you, Mr. Chairman.

And to the Director, thank you. You have made yourself regularly available to this Committee, and as a Member it's very helpful, and we appreciate it and appreciate your service.

I want to talk a little bit about geolocation metadata, and specifically the Jones case, which is a Supreme Court ruling where they ruled 9 to nothing that a GPS device placed on a vehicle for an extended period of time was an unreasonable search. Geolocation is broadly defined as using a GPS device or triangulation so that you can tell the specific whereabouts of where a particular phone is.

Could you help me define what metadata is? Because what we have seen in the news is that the metadata category is the simple telephone number, where they're calling, and how long they're calling. Can you help me define what else is in the so-called metadata category?

Mr. MUELLER. Well, in the case of emails, it would probably be header information. I think people would consider the adressing information——

Mr. CHAFFETZ. What about—

Mr. MUELLER [continuing]. But not the subject line, for instance. That would not be metadata. In terms of the telephone, it would be that which you articulated, principally.

Mr. CHAFFETZ. Would it include geolocation information?

Mr. MUELLER. That's a question I'd have to get back to you on. I have not thought about that.

Mr. CHAFFETZ. We had submitted in advance our questions that we were going to ask here today in part so I could have a candid dialogue with you. We were very good at providing the questions that I was going to ask. With all due respect, sir, you're the Director of the FBI. You've been there for 12 years. You had to of think post-Jones what are the implications of the Jones case, what is geolocation, and how does it apply?

Mr. MUELLER. Absolutely. I mean, we have been—after the Jones case, we have taken—the Jones case can be applied to a number of ways that we utilize geolocation. In each of these different ways, we have taken the most conservative approach because you don't know what is going to be the progeny of Jones.

On the particular question of whether or not geolocation is metadata off the top—well, I shouldn't do it off the top of my head. I have to make certain that I look at that one.

Mr. CHAFFETZ. Is there a database of geolocation information that is warehoused by our Federal Government?

Mr. MUELLER. Not that I am aware of.

Mr. CHAFFETZ. Post-Jones there has been guidance given by the Department of Justice to the FBI. I would love to see that information and share that. I have seen two unclassified documents that were through a Freedom of Information Act. Is that something that you can share with this Committee?

Mr. MUELLER. I'd have to look at that. But if it's unclassified, internal, then I'd have to look at that.

Mr. CHAFFETZ. All right. I guess what I have a problem is, this phone right here, the Federal Government has no problem following this phone, who I call. If I call my 12-year old daughter, the telephone number I called her on, how long I had. But the geolocation is something that we—I have a bill that I have spon-

sored that really basically categorizes geolocation as content as opposed to metadata.

So if you're going to follow what this telephone number is, where it is, is that or is that not content?

Mr. MUELLER. I'll tell you, I think it's a very difficult question, and I'd want to think about it. It can be metadata, it can be content, and may depend on the circumstances.

Mr. CHAFFETZ. But is there a database that anybody knows of that——

Mr. MUELLER. I do not know of a database that specifically is addressed to geolocation, apart from anything else, investigative activity that is solely a geolocation database.

Mr. CHAFFETZ. Post-Jones, does the FBI believe that there should be a lower or different standard for law enforcement to access geolocation information from smart phones or other mobile devices than the standard for attaching tracking devices to cars under Jones?

Mr. MUELLER. I'd have to get back to you on that. I apologize. I can see you gave me the questions, and I did not get briefed on. It's my own fault for getting briefed on the questions so I'm better able to answer them.

Mr. CHAFFETZ. I appreciate it.

And, Mr. Chairman, it's terribly disappointing to come to this point, talk about something that is in the headlines of every newscast. I gave the questions in advance.

Mr. MUELLER. And they noted that I would be asked on that, I might add. So it's my fault.

Mr. CHAFFETZ. Your staff did some great work, I guess, but it's terribly frustrating, sir. You're the head of the FBI. You're the Director of the FBI. This is an important discussion and dialogue. And I know I won't get an answer and that's the——

Mr. MUELLER. I will be happy to meet with you after I have had a chance to review the questions that you have and the answers that you need.

Mr. CHAFFETZ. What would be a reasonable timeframe for me to start to call and say, hey, where is this information?

Mr. MUELLER. A week.

Mr. CHAFFETZ. Okay. I appreciate it. Thank you, sir.

Yield back.

Mr. GOODLATTE. I thank the gentleman.

And we will again reinforce our urging that these questions be answered as promptly, and in this case a meeting take place with the gentleman from Utah. He has a very good issue that needs to have your input.

And the Chair now recognizes the gentleman from New York, Mr. Jeffries, for 5 minutes.

Mr. JEFFRIES. I thank the distinguished Chair.

And I also want to thank the Director for your presence here today and certainly for your service to this great country.

Edward Snowden has been characterized by many, as a villain by some. His actions have been called courageous or heroic. It's not my place, I believe, to characterize him one way or the other. A court of law, hopefully, will assist in coming to a conclusion as to what took place in accordance or in violation of our laws.

But it is clear that he has become a lightning rod that has sparked what I think is a very important debate in this country that we in the Congress should have as to the proper balance between legitimately held security concerns and concerns for privacy and liberty which are essential to the preservation of our democracy. And so in that spirit, just wanted to get a sense of some of the particulars, to the extent that you can discuss them in an open Committee hearing, related to the recent 215 acquisition of information connected to the Verizon metadata.

Now, presumably, that was acquired based on a conclusion by yourself, the FBI, the Department of Justice, other relevant actors, that the metadata for all Verizon customers in the United States of America and beyond for a 3-month period was relevant to a counterterrorism investigation or to foreign intelligence acquisition. Is that correct?

Mr. MUELLER. If you're talking about the relevance and the finding of relevance, I'd really have to defer you to the FISA Court. But yes, there is an order that had been issued—and I might add, it's just one piece of the order, there are other aspects of it—that deemed that this information that was accumulated satisfies the relevance standard in the statute.

Mr. JEFFRIES. Right, in order for the FBI to come to the conclusion that it can legitimately pursue this information, I presume that you also have to conclude that it's relevant information. Is that right?

Mr. MUELLER. Yes, for access to this information, it's very, very limited. There has to be a showing of the reasonable, articulable suspicion that the number that you are seeking to search for is associated with terrorism. And there is a very limited search of the data that is done to answer that particular question. And that process satisfies the relevance standard under the FISA Court.

Mr. JEFFRIES. Now, once you pursue information based on that reasonable suspicion standard, what is the process for attempting to acquire content information connected to that metadata, presumably on a forward-looking basis?

Mr. MUELLER. Well, if you want to get additional information relating to that particular telephone number, you would have to get additional legal process. For instance, subscriber information. If you ultimately wanted to obtain a wire interception, then there are additional legal processes that you have to go through.

Mr. JEFFRIES. Now, under the general relevance standard is it fair to say that it would be the FBI's position that this type of metadata information should also be made available pursuant to a court decision if it's sought connected to other service providers beyond Verizon?

Mr. MUELLER. Well, I can't talk to the specifics of the program.

Mr. JEFFRIES. Okay. Is there anything that you can say as it relates to why Verizon was deemed or Verizon users were deemed particularly relevant in such a broad way as it relates to every single user over a 3-month period of time across the country of more than 300 million people?

Mr. MUELLER. Well, again, it goes into the details of the program that I can't get into in open session. I don't know whether they got

into this when you had the classified session on Tuesday, but in open session it would be difficult for me to respond.

Mr. JEFFRIES. Okay. Well, thank you. I respect that.

Switching topics, in terms of the sequestration impact that it's had on the FBI, recently, I think the FBI has increased its efforts connected to illegal piracy in the intellectual property space.

Mr. MUELLER. Yes.

Mr. JEFFRIES. That's an important step that you've taken. Piracy impacts, obviously, commerce and our economy in increasingly significant ways. Are those FBI efforts impacted in any adverse way connected to your increased enforcement efforts in the intellectual property space?

Mr. MUELLER. I don't think this year. Next year they will be. They will be impacted.

Mr. JEFFRIES. They have been impacted this calendar year?

Mr. MUELLER. Across the board, my expectation is we have to consider rather dramatic and drastic reductions across the board.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. JEFFRIES. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank you, Mr. Chairman.

I'm way over here, Director. I want to talk about a constituent from Houston, Texas, named Catherine Engelbrecht. In July of 2010, she and her husband, business owners, started two groups, a nonprofit—hoping to be a nonprofit group—True the Vote and King Street Patriots. December of 2010, the FBI Domestic Terrorism Unit inquired about their attendees. January of 2011, the FBI Domestic Terrorism Unit inquired about one of their attendees. January of 2011, Catherine Engelbrecht Enterprises were audited for 2008 and 2009. January of 2011, True the Vote, IRS questions their nonprofit application. That was the first round.

March of 2011, the IRS questions—excuse me, May of 2011, King Street Patriots were visited by—rather members of King Street Patriots went to the FBI after their request about questions, how are they doing, anything you need to tell us or report. October of 2011, True the Vote, IRS questions their application. They wanted to know who their Facebook people were, all of their tweets, who they were tweeting to, wanted personal knowledge about their family, every place they had ever spoken—this is Catherine—every place she intends to speak, who they were speaking to, the names of the participants, copies of transcripts, everywhere they intended to speak, and they asked about 300 questions, including who is doing the training, what are the backgrounds of the trainers. And then they ask who your lawyers were and the background of the lawyers that represented them and the qualification of the lawyers, et cetera. I will furnish you the 300 questions, Mr. Director.

Three more visits by mail, or by rather phone by the FBI, June, November, and December to the King Street Patriots. And then the IRS in February of 2012 questions the nonprofit status again of True the Vote. This was the third round.

At that time, I sent to your office—excuse me, the Department of Justice—an inquiry saying, is this group, these people under investigation for criminal offenses? I get a letter back from the Jus-

tice Department that says, they are not under criminal investigation. But it continues. They were visited later by the ATF. They were visited by OSHA, they were visited by TCEQ. They were visited again by the IRS, fourth round.

All of these IRS questions are coming from Cincinnati, and they get finally another question from the IRS from Utah. That was in March of this year. April of this year, here comes the ATF again, another unscheduled visit to their business.

Now, I have read the civil rights law. It's important, and you have a Civil Rights Division in the FBI to enforce civil rights violations. The way I understand the law, you can't target a certain group because of their beliefs. The IRS has already said, we targeted—some people in the IRS—has already targeted certain tea party groups because they were tea party groups.

My question, without going into details, my question, in a hypothetical case, IRS targeting groups with this information that you have seen there inquired about, ironically, four different agencies all inquiring about a group for over several years, does that appear to be something that if a complaint was filed with the FBI, the FBI would investigate as a civil rights violation?

Mr. MUELLER. Sir, I think that's part of the—would be part of the ongoing investigation, I should say—of the circumstances relating to the IRS that was initiated a number of weeks ago. My expectation is this would be a piece of that investigation.

You also indicate, though, that FBI agents visited these individuals. I will go back and look at the predication for that particular visit ourselves to follow up on that aspect of it to the extent that these persons were paid visits by the Bureau.

Mr. POE. All right, thank you, Mr. Director.

I yield back my time. Thank you.

Mr. GOODLATTE. The Chair thanks the gentleman, and recognizes the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Director, I want to thank you for your service to our country in the military as a prosecutor and as a law enforcement officer.

I wanted to touch on three different areas. I want to start with the Rosen affidavit because it states, in pertinent part, there is probable cause to believe that a reporter has committed a violation of the Espionage Act—and this is the phrase I want to focus on—at the very least, either as an aider and abetter and/or a co-conspirator. If the standard is probable cause, why in the world would the affiant add the phrase, at the very least, if they weren't contemplating a prosecution?

Mr. MUELLER. I don't know why the person would have added those, that statement.

Mr. GOWDY. Well, you were a very distinguished Federal prosecutor. I was not at all distinguished, but I was a prosecutor. I don't remember ever adding surplusage, extra wording, to an application for a search warrant. So I am vexed by why the affiant would say, at the very least.

Mr. MUELLER. I just don't know.

Mr. GOWDY. Also in the application for search warrant they requested a nondisclosure order citing the five different reasons.

Now, it was my experience and I assume yours that the affiant is under oath when they appear before a judge.

Mr. MUELLER. Yes.

Mr. GOWDY. Do you know which of the five categories that would need to be shown for a nondisclosure order was testified to in this case, which of the five reasons statutorily that you can seek a nondisclosure order were at play?

Mr. MUELLER. I'm not that familiar with the facts to be able to answer that.

Mr. GOWDY. But you would agree with me that when you're before a judge and you're swearing out your affidavit, if you ask for a nondisclosure order you have to have some evidence that one of those five factors is in play?

Mr. MUELLER. Well, I am not all that familiar with the statute. I will say that when you file an affidavit everything in there ought to be accurate and you ought to be prepared to swear to every item in that.

Mr. GOWDY. Do you ever recall discussing the Rosen investigation with the Attorney General?

Mr. MUELLER. No.

Mr. GOWDY. Well, let me ask you this. If the affiant said at the very least there is probable cause to believe a crime has been committed, was there a discussion of indicting Rosen?

Mr. MUELLER. Not that I had.

Mr. GOWDY. If you had more than probable cause why would there not be discussion of indicting?

Mr. MUELLER. Well, there may have been discussion, as you well know, with the Assistant United States Attorney and the agent in terms of what went in the affidavit. You have done any number of, hundreds probable of affidavits yourself, and the discussion between the lawyer and the agent is for the lawyer to get what the agent knows in the course of the investigation, can get it written up so that you can get the approvals that you need. I'm sure that happened here. It did not come up, does not come up to my level to have that kind of discussion.

Mr. GOWDY. All right. So it is fair to say that you were not part of any conversations with respect to whether or not something along the lines of an indictment should be considered for the reporter, but you do not know whether or not the conversations took place. But you yourself were not part of them.

Mr. MUELLER. I was not and had not.

Mr. GOWDY. Okay. Does the Bureau have a policy with respect to shopping judges or not shopping judges? If you go to a magistrate or you go to an Article 3 judge and you're denied, is there a policy within the Bureau on judge shopping?

Mr. MUELLER. No. Not that I'm aware of.

Mr. GOWDY. All right, let me switch gears. There was an allegation this week of American diplomats being involved in the alleged solicitation of prostitution overseas. Would the Bureau have jurisdiction to investigate that?

Mr. MUELLER. Have to look at that. Initially, I would say—well, I'd have to look at it. I'd say no, but there may be, off the top of my head, maybe I am missing something. I have to get back to you on that.

Mr. GOWDY. If there were an allegation that the State Department attempted to interfere with or influence the investigation, is that something the Bureau would have jurisdiction over?

Mr. MUELLER. In the first instance, I'm not certain. We may. Going back to the question about the activities overseas, if it implicated the disclosure of U.S. secrets, for instance, then we would have, perhaps, some predication for being involved in the overarching investigation. As to the second question, I just can't say.

Mr. GOWDY. I've been out of the business for a while, but I think it may be a crime to travel for the purpose of soliciting underaged sex. I could be wrong about that.

Mr. MUELLER. Underage, yes. I do believe that that would be covered. But I have to check on that.

Mr. GOWDY. All right.

Mr. MUELLER. Like you, I have not done this work for some time.

Mr. GOWDY. Yes, sir. All right. Finally, with respect to Benghazi, and this is not a trick question, I think the answer is obvious, the quicker you get to a crime scene, the better you're going to be able to investigate it and process it, right?

Mr. MUELLER. Absolutely.

Mr. GOWDY. All right. And the Bureau did not get to the crime scene in Benghazi for how long?

Mr. MUELLER. I think 2 weeks.

Mr. GOWDY. And why did the Bureau not get to the crime scene in Benghazi for 2 weeks?

Mr. MUELLER. There were a number of factors, and the first one relates to the state of security in Benghazi. There was no security.

Mr. GOWDY. All right, I want to just stop you there because I want to ask one more question and my time is out. I am asked all the time back home in South Carolina, if Benghazi was not safe enough for the premier law enforcement agency in the world to go, how was it safe enough for us to send diplomats?

Mr. MUELLER. That's another question that is not in my bailiwick. I understand the question is being asked. I presume it is a rhetorical question.

Mr. GOWDY. It is rhetorical unless you know the answer. I can't answer it. I don't know.

Mr. MUELLER. All I am saying is, rhetorical or not, I can't answer.

Mr. GOODLATTE. It is a good question, but the time of the gentleman has expired.

Mr. GOWDY. Thank you.

Mr. GOODLATTE. And we will look for opportunities to ask it again.

And the Chair now recognizes the gentleman from Georgia, Mr. Collins, for 6 minutes.

Mr. COLLINS. Mr. Director, I appreciate you being here, and I appreciate—by the time we get to this, there are sometimes rhetorical questions that seem to pop their heads up. And I think this question, my friend from South Carolina brings a very good point. There are things that people out in the world look at and they see, and they are honest, hard-working folks, and they look at these things and they say, this doesn't make sense. And I think it just attributes to the disconnect that many times happens with the

folks who get up and go to work every morning, and they look on their TV and they see what is happening up here, and they say it just doesn't pass the smell test. And I think that's some of the things that we're concerned about.

But I want to go in a different direction. We've covered the gamut. Our country wants to be safe. The people in the Ninth District, they want to know that their government is watching out for them. They want to know that there is sharing, legal sharing, and not overreach, but legal work that is hard work between police and law enforcement agencies and the Justice Department.

My father was a state trooper for 31 years in Georgia. I get it. But there needs to be a balance in there. So there is a program called the Joint Regional Intelligence Group, and I want to switch gears here. The Director of National Intelligence issued a directive establishing the Joint Regional Intelligence Group pilot program. The purpose of this program will be to coordinate information sharing between foreign and domestic intelligence communities.

We have been hearing from State and local law enforcement that the FBI has largely taken control of standing up the pilot program and that they have been excluded. Is that the case, or is that your understanding of what is going on right now?

Mr. MUELLER. And who would be excluded?

Mr. COLLINS. The State and locals feel like they're being excluded here.

Mr. MUELLER. This issue I think we've addressed in terms of the regional intelligence centers. I know there was some concern at some point that this is a new vehicle. We have, I think, explained sufficiently to State and local law enforcement that this is not anything new. It's a greater integration of the intelligence capacity around the country.

Mr. COLLINS. So you're saying this is an existing program and what the Director of National Intelligence is saying is not new?

Mr. MUELLER. Well, I'm not certain exactly which program the Director of National Intelligence is talking about. I thought you said regional——

Mr. COLLINS. The Joint Regional Intelligence Group.

Mr. MUELLER. Joint Regional Intelligence, yes. It certainly includes State and local law enforcement and there are various parts of that particular undertaking, and you have to differentiate between the various parts of that undertaking. For instance, part of it is the role of our special agents in charge is being in the various divisions or districts as being in charge and being the person who is in charge for intelligence collection, or coordination, I should say, under the ODNI.

Mr. COLLINS. Okay, so and again, the understanding here, tell me a little bit more about this program. Maybe we're talking about the same program, maybe we're not. Because this seemed to be more of a pilot program which would mean that it was more—it was either integrating stuff that was already there or starting something from you that may have been. Where is this being located out of?

Mr. MUELLER. Well, I guess I am confused in terms of specifically what programs you're talking about under the ODNI. I would be happy to get back to you——

Mr. COLLINS. Okay.

Mr. MUELLER [continuing]. Specifically on this, as I can read it, and assimilate it.

Mr. COLLINS. All right. In light of that—and we'll move on and I appreciate you getting back to me about those questions—a lot has been said about the Electronic Communications Privacy Act. We sort of danced around a little bit of that. As you're sort of in your last little bit here, I want to sort of open this up and say, is it out of date? Would it be helpful for law enforcement to have a clear standard of collection? And if so, what do you believe that would be?

Mr. MUELLER. Well, yes, I do think it is outdated. It does need review. As I indicated before, I would caution against raising standards for obtaining basic non-Fourth Amendment information because you eliminate much of the data that provides predication for further investigation. And so as one looks at it, I would look at it to be updated, but also I have some concern about raising standards, which would impact on our ability to conduct cases, whether it be terrorism or otherwise.

Mr. COLLINS. Well, as I have a law professor who's basically lamented many times on the demise that there was even a Fourth Amendment even existing today in light of a lot of things in cases that have been going on. Is there a way though that we balance this in a new age and environment, in which it seems to be metadata? We call it these things where it's collection, but we're collecting on such large scales in this electronic life. We've got a pretty hard line to focus here in which we are protecting civil liberties yet giving access where need be, where I think people would understand there would be a reason to investigate.

Mr. MUELLER. I do think that given the new technology, the ability to communicate in any number of ways, that the statute needs to be upgraded.

The concern comes, you can identify terrorists by looking at substantial accumulations of non-Fourth Amendment protected data. And in the case of a terrorist who wants to undertake an attack to kill Americans, it may well be worth that balance. On the other hand, what you want to protect against is abuse of that collection of data.

Mr. COLLINS. And that hits. And the concern I have had—and our time is done, but the quick question—depending on many-year-old court decisions on what is, quote, "metadata" and what is protected, I'm concerned that we're in a situation now to where some of the older rules of things that didn't understand this kind of technology may be balanced in a way that we're going to have to look at it differently. Instead of saying, well, it's always been okay under these circumstances, and now try to apply it. Now, I think we may be trying apples and oranges, and I think people are concerned about that.

Thank you, though, for your service. Thank you for being here to answer the questions.

And I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman.

The gentleman from Idaho, Mr. Labrador, is recognized for 5 minutes.

Mr. LABRADOR. Thank you.

Thank you, Director, for being here, and thank you for your service.

I was a criminal defense attorney, and I'm a little bit confused by the answer from the Administration about the Rosen investigation. It seems to me that how many times as an FBI Director, or as an attorney, or in your law enforcement practice, have you had the opportunity to investigate somebody who you did not intend to prosecute?

Mr. MUELLER. Well, as I said before, that happens all the time, I mean.

Mr. LABRADOR. No, the question is—I want to be very specific about this. Not that you don't prosecute after the investigation, because that is the purpose of the investigation, is to find out if you need to prosecute somebody, but to actually look into people's private information, private communications who you don't intend to prosecute. Do you understand my specific question?

Mr. MUELLER. I think I do, but I think we're maybe on—we're passing each other, because you can—it can be a husband and wife team that are avoiding taxes.

Mr. LABRADOR. Correct.

Mr. MUELLER. At the outset you have probable cause to believe that the wife was——

Mr. LABRADOR. Yeah, but you have probable cause to believe that they are both committing a crime. And then you determine after the investigation that one committed the crime and one did not commit the crime, right?

Mr. MUELLER. That's an option, yes.

Mr. LABRADOR. So tell me how often a prosecutor investigates somebody who is not intended to be prosecuted, that they don't intend at any time to file charges. Because it seems to me that's much broader than the Fourth Amendment. If that's what prosecutors are doing, then you're going beyond the extent of the Fourth Amendment.

Mr. MUELLER. You're a defense counsel, you know the dialogue between defense counsel and the prosecutor as to whether or not the person is going to be prosecuted in terms of testimony.

Mr. LABRADOR. Correct.

Mr. MUELLER. We make the decision day in and day out, and we are not going to prosecute a particular person if they cooperate with us. Now, often it'll be we will investigate him for a period of time, then make a decision the person is better as a cooperator, and consequently we have no thought about prosecuting him. We want their testimony.

Mr. LABRADOR. But what this Attorney General said and what you have said is that Mr. Rosen was never intended to be prosecuted. I have never heard of an investigation, ever, where you went after an individual when there was no intention to find out if that person was going to be prosecuted. And that's what I am having a hard time with.

Mr. MUELLER. I am not certain I said that because I was not in that position to make that determination.

Mr. LABRADOR. Well, that's what the Attorney General said in this Committee. He said that there was never an——

Mr. MUELLER. I'd have to go back and look specifically at what the Attorney General said.

Mr. LABRADOR. But wouldn't you think that would be inappropriate then, to go after somebody that you don't intend to ever prosecute, because that has been the excuse of this Administration. I'm having a hard time with that excuse.

Mr. MUELLER. I'd have to give thought about that, but I do think there are a number of occasions as a prosecutor where we have the ability, the capability, and maybe the intent at the outset, and then we make a determination, for whatever reasons, whether we want the cooperation or other things, where we make a determination that we're not going to go forward.

Mr. LABRADOR. And I agree with you.

Mr. MUELLER. And there are competing interests.

Mr. LABRADOR. When you make a determination after the investigation has occurred. But the problem with the Rosen subpoena, and the problem that we had with this investigation, is that Mr. Rosen was never intended to be prosecuted, according to the Attorney General. So this was a fishing expedition, something that I think went beyond the Fourth Amendment, which wasn't necessary. And that's why they had to go around shopping for different judges who would actually approve of this subpoena.

Mr. MUELLER. Well, I don't perceive it as being a fishing expedition at all. As I indicated previously, in these investigations you focus on, we, the FBI, focus on the leaker from the Federal Government. That's the person who we want to identify and to ultimately prosecute. To do that we have to show that the information went from this person to the person who ultimately published it. And as part of the investigation, you gather facts in terms of how that information got from the individual who had the security, or had the——

Mr. LABRADOR. But when you go to the judge, you tell the judge that you are intending to prosecute this person, or this person has violated the law in some way, or you have reasonable suspicion to believe that this person has violated the law. How often have you as a law enforcement officer submitted a subpoena to a judge saying that somebody—you suspect somebody violated the law when you had no intention to ever prosecutor that person, you didn't think that your investigation was going to lead to the prosecution of that person?

Mr. MUELLER. I have to think about it. Under those circumstances, the way you say them, I have to think about it.

Mr. GOODLATTE. Would the gentleman yield?

Mr. LABRADOR. Yes.

Mr. GOODLATTE. I thank the gentleman, because he is asking a very important line of questions and I would ask him if he would allow me to ask this question.

If the allegations made in that case with regard to Mr. Rosen violating the Espionage Act, saying that he was—that there was probable cause to find that he was not—he was at least an aider, abetter, or co-conspirator in violation of the Espionage Act, later said that he was a flight risk, and you asked that the record be sealed for 18 months, if those indeed were the facts, if those indeed were the case, why wouldn't you prosecute the individual?

Mr. MUELLER. There may be other competing interests.

Mr. GOODLATTE. Like what?

Mr. MUELLER. The First Amendment.

Mr. GOODLATTE. What's that?

Mr. MUELLER. The First Amendment. There can be other competing interests. The First Amendment.

Mr. GOODLATTE. Okay, but that just goes right back to the question asked by the gentleman from Idaho. If the First Amendment, which I think is of paramount importance here, is indeed that consideration, then why would it be appropriate to go before the court, before the judge, and say all of these things about the individual in order to get a search warrant to go through his email records without his knowledge?

Mr. MUELLER. I'm not familiar——

Mr. GOODLATTE. If you're not going to prosecute him, why not tell him? Why not tell him?

Mr. MUELLER. I am not that familiar with the discussions that went on, first of all, at the level of the Assistant United States attorney and the agent who was on it, or as it went through the Department of Justice.

Mr. GOODLATTE. Thank you.

I thank the gentleman for yielding. And I'll yield him an additional minute if he wants to pursue the question.

Mr. LABRADOR. Thank you. Mr. Chairman, you have asked my questions.

Thank you very much for being here.

Mr. GOODLATTE. Now, this concludes the hearing today. Director, we thank you. You have given us more than 3 hours of your time. You have answered a lot of questions, a lot of difficult questions, and we very much appreciate that. I will join all of my colleagues and I think virtually every one of them thanked you for your service. If they did not, I'm sure it is because they neglected to do so. You have a remarkable record as Director of the FBI. I do think there are some questions here that remain that you were not able to answer. We will submit questions to you in writing. And I think you have made a few commitments yourself to do that. We would find that very important to have those additional pieces of information.

And without objection, all Members will have 5 legislative days to submit additional written questions for the witness or additional materials for the record.

And with that, with our thanks again, the hearing is adjourned.

[Whereupon, at 1:10 p.m., the Committee was adjourned.]

○