Journal of Legislation

Volume 41 | Issue 2 Article 1

7-29-2015

Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism

Congressman Peter T. King

REMEMBERING THE LESSONS OF 9/11: PRESERVING TOOLS AND AUTHORITIES IN THE FIGHT AGAINST TERRORISM

Congressman Peter T. King

INTRODUCTION

As Chairman of the Subcommittee on Counterterrorism and Intelligence, a Member of the House Permanent Select Committee on Intelligence, and a Congressman from New York, 9/11 was a very personal experience that continues to resonate with me. I lost over 150 neighbors, friends and constituents on September 11th, but no one has a monopoly on grief. This issue went to the soul of the entire country, and touches our lives nearly 15 years later.

That day forces us to acknowledge, whether some of us want to or not, that we have an unyielding enemy, vicious and bitter, that will resort to any tactic to achieve its goal of destroying our pluralistic society, and any who do not submit to their view of Islam.

Since then, the nature of the terror threat changed. Technology progressed. An act of betrayal compromised one of our best defenses against terror. And then both business and political support for lawful and necessary counterterror measures waned. Responsible leaders in the public and private sectors must act now to preserve and enhance the tools our intelligence agencies and law enforcement organizations need to protect the Homeland.

THE THREAT TO THE HOMELAND

Since 9/11, the United States and our allies have spent many billions of dollars and made great efforts to increase security and track down terrorists around the globe. President George Bush eliminated Al Qaeda's sanctuary in Afghanistan in 2001, and President Barack Obama killed its leader Usama bin Laden in Pakistan in 2011, to the everlasting credit of both men. And it is now more difficult for terrorists to travel to the U.S. and Europe to conduct complex, large-scale attacks, on the scale of 9/11, or even multi-site bombings such as London in 2005.

In response, Al Qaeda in the Arabian Peninsula (AQAP), the Islamic State in Iraq and Syria (ISIS) and other terror groups tactically evolved to make grassroots appeals via social media to radicalize homegrown extremists. Their radical Islamist ideology inspired attacks in the West: American and allied soldiers killed in Little Rock, Fort Hood, London, and Ottawa; policemen stabbed in New York; and civilians murdered in Tolouse, Boston, Brussels, Paris, and Sydney. These smaller operations still captured the world's attention, and served to fundraise and recruit for

the terrorists' cause.

Meanwhile Somalia, Libya, Syria, Iraq and Yemen are now failed states. These nations may serve as terror safe havens the way Afghanistan did in the 1990s and Pakistan did in the first decade of this century. And West African nations are under siege by Islamists as well.

So-called "core" Al Qaeda in northwest Pakistan may be on the defensive, reportedly due to drone strikes conducted by the Central Intelligence Agency, but ISIS has capably filled the jihadi leadership void. ISIS' totalitarian and genocidal Islamist caliphate is spreading throughout Iraq and Syria, and drawing support throughout the Middle East, Asia and even into Africa. ISIS built its brand of terror through the seizure of territory, and the cowardly butchering of innocent civilians, including American journalists and aid workers. Its robust social media campaign is attracting over 20,000 deranged malcontents from around the world, including thousands from Europe and even hundreds from the United States.[1]

Despite all of these challenges the U.S. still prevented several dozen planned attacks against the Homeland in the past thirteen-plus years. These quiet successes are directly attributable to the capabilities of our intelligence agencies to collect, analyze, and disseminate actionable counterterror information. This intelligence enables policymakers to order specially trained men and women, usually agents of the Federal Bureau of Investigation (FBI) but sometimes military or special operations forces, to take direct action against our enemies.

I know firsthand how effective our intelligence has been in preventing terrorist attacks, such as the 2009 attempted New York City subway bombing, which would have killed hundreds of civilians. While visiting Germany in 2013 President Obama stated that, "We know of at least fifty threats that have been averted because of this [intelligence] information not just in the United States, but, in some cases, threats here in GermanyFalse So lives have been saved."[2]

EDWARD SNOWDEN

Al Qaeda and other terrorist organizations use communications tradecraft to conceal their recruiting, fundraising and plotting. As such the National Security Agency (NSA), America's signals intelligence service, is a key player in protecting us from attack.

As the only Member of Congress serving on both the homeland security and intelligence committees, I have for several years now been briefed on most of America's classified counterterrorism programs. This knowledge has left me with two particular impressions.

1. *Hearing to Receive Testimony on Worldwide Threats Before the Senate Committee on Armed Services*, 114th Cong. 12-14 (2015) (statement of James R. Clapper, Director, Office of the Dir. of Nat'l Intelligence).

2. Justin Elliott & Theodoric Meyer, *Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence*, PROPUBLICA (Oct. 23, 2013, 8:59 AM), http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence (quoting President Obama's speech in Germany on June 19, 2013).

One, respect for the courage, ingenuity and skill of the professionals who implement these operations. And two, how carefully regulated and heavily lawyered these activities are by overlapping executive, congressional and judicial oversight.

It is important to note that any grant of power by the government to persons comes with the potential for the abuse of that authority by individual representatives of the government. This is true of any organization.

But from what I have observed on the intelligence committee, which receives copies of mandated reports from the Justice Department about the Intelligence Community's compliance with the legal limits placed on its collection, the frequency and severity of the abuse of the signals intelligence authorities of our government, are vanishingly small. And any violations are punished when they (rarely) occur. Critics of these programs have not pointed to any abuses of them tolerated by intelligence or law enforcement agency leaders.

In 2013 former NSA contractor Edward Snowden stole national secrets he pledged to protect. He sought refuge in China and Russia, where there is little doubt he cooperated with hostile intelligence services. He and his co-conspirator Glenn Greenwald then published scores of highly classified documents.

Snowden deliberately exposed sensitive methods for gathering signals intelligence, constraining our ability to identify, track, and apprehend those who seek to do us harm. His disclosures further suggested the identities of human sources suspected of possibly helping the U.S. in such operations, lives at risk, and certainly discouraging others from helping the U.S. in the future.

Snowden's treason undermined our ability to defend ourselves against ISIS, AQAP, core Al Qaeda and others waging war on us. His and Greenwald's betrayal of our country severely damaged information sharing with our foreign partners, and set back allied efforts to dismantle terror networks and disrupt plots against Western civilians.

Unfortunately, instead of condemning Snowden, many opinion-makers and politicians embraced him. Snowden's defenders include some, shamefully, from my own Republican Party such as Rand Paul,[3] and other so-called libertarians.

Critics of counter-terrorism surveillance confuse legitimate concern with the growing role and size of government in the domestic economy, with an unhealthy suspicion of those who carry out lawful national security missions – including, in the case of the NSA, uniformed military personnel. It has been the disappointment of my political lifetime to see Republican colleagues fall hook, line and sinker for a disinformation campaign orchestrated by Snowden and his allies.

Instead of rallying behind those carrying out the NSA and FBI's wartime missions, many in both the GOP and the Obama Administration have headed for the tall grass, endangering political support and legal authority for programs which keep us safe, such as PATRIOT Act and CALEA.

3. *See* Katie Glueck, *Rand Paul backs Snowden, bashes Clapper*, POLITICO (Jan. 5, 2014, 10:37 AM), http://www.politico.com/blogs/politico-live/2014/01/rand-backs-snowden-bashes-clapper-180571.html.

PATRIOT ACT REAUTHORIZATION

It is imperative that Congress reauthorize the Patriot Act before it sunsets on June 1, 2015, including support for the legal authority for domestic surveillance provided by Section 215 of that program.

According to a spokesman for the National Security Council staff, if Congress does not renew Section 215 authority the Obama Administration will not continue the program, even though the President agrees that its absence would damage America's national security.[4] NSC spokesman Ned Price stated, "Allowing Section 215 to sunset would result in the loss, going forward, of a critical national security tool that is used in a variety of additional contexts that do not involve the collection of bulk data."[5]

These comments are yet another example of the lack of leadership in the current Administration on national security matters. The President more than anyone is aware of how these authorities have been used to successfully keep Americans safe at home and abroad, and the fact that he's willing to let them expire, with no plan to supplement them, is truly concerning. When the NSA faced withering criticism after the Snowden leaks, I asked the President to visit the NSA, as I did, to show support for the institution and thank the people who toil in obscurity to protect our nation and execute his orders as Commander-in-Chief. By refusing to press Congress to renew the Section 215 authorities and educate the public on why this is important, the President is yet again abdicating his responsibilities as Command-in-Chief. In light of the current threats facing our country, this silence is inexcusable.

Former FBI Director Robert Mueller testified to Congress that the PATRIOT Act "changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act."[6]

The bipartisan FBI 9/11 Review Commission[7] conducted an assessment of five recent counterterrorism cases.[8] The Commission found that these cases demonstrated the importance of maintaining sufficient legal authorities to conduct counterterrorism investigations.[9] The Commission noted that the Electronic Communications Privacy Act (ECPA), Communications Assistance for Law Enforcement Act

4. Tom Risen, *Would NSA Data Surveillance End With Patriot Act?*, U.S. NEWS & WORLD REPORT (March 25, 2015, 4:38 PM), http://www.usnews.com/news/articles/2015/03/25/would-nsa-data-surveillance-end-with-patriot-act (quoting Ned Price, a spokesman for the National Security Council).

5. *Id.*

6. *Hearing on the Sunset Provisions of the USA Patriot Act Before the Senate Committee on the Judiciary*, 109th Cong. 1 (2005) (statement of Robert S. Mueller, III, Director, Fed. Bureau of Investigation).

7. The FBI 9/11 Review Commission was established in January 2014 pursuant to a congressional mandate which directed the Bureau to create a commission with the expertise and scope to conduct a "comprehensive external review of the implementation of the recommendations related to the FBI that were proposed by the National Commission on Terrorist Attacks Upon the United States" (commonly known as the 9/11 Commission). BRUCE HOFFMAN ET AL., THE FBI: PROTECTING THE HOMELAND IN THE 21ST CENTURY, REPORT OF THE CONGRESSIONALLY-DIRECTED 9/11 REVIEW COMMISSION TO THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION 3 (2015) (citing Consolidated and Further Continuing Appropriations Act, Pub. L. 113-6, § 4, 127 Stat. 198 (2013)).

8. HOFFMAN ET AL., *supra* note 7, at 38-52.

9. *Id.* at 49.

(CALEA), the Foreign Intelligence Surveillance Act (FISA), and the PATRIOT Act were all essential to the investigations in each case, and highlighted the critical value of the FBI's existing authorities in detecting and countering terrorist threats.[10]

The Commission cited FISA applications including Section 702[11] authorizations and National Security Letters (NSLs)[12], as particularly helpful to the investigations.[13] The Commission concluded that monitoring, preserving and upgrading these laws is essential to enable the FBI to keep pace with the evolving terrorist threat, and noted that as the terrorism threat continues to evolve in the years ahead.[14] Congress may even need to expand these authorities, the Commission added.[15]

The Commission further urged the FBI to ensure that Congress is aware of the critical value of these programs.[16]

While I would expect a number of bills and amendments from Members of Congress, who do not have a good grasp of current national security challenges, to be introduced to strip the NSA of its authorities, I am pleased that Senate Majority Leader Mitch McConnell is on the record that current lawful NSA powers are necessary,[17] and hope that he will support full renewal of the Patriot Act this spring.

TECHNOLOGY CHALLENGES

Compounding the political problem of opposition to current surveillance authorities is the rapid advance in technology that began with the Internet, and accelerated with society's widespread embrace of mobile wireless communications systems. The benefits of these new technologies have not gone unnoticed by criminals and terrorists who constantly develop new techniques to evade detection and facilitate their illicit activities.

Attorney General Eric Holder recently said, "Recent technological advances have the potential to greatly embolden online criminals, providing new methods for abusers to avoid detection."[18] Technology enables criminals and terrorists to estab-

10. *Id.*

11. Title VII, Section 702 of the Foreign Intelligence Surveillance Act (FISA), covers "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons." 50 U.S.C. § 1881a (2008). This authority allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad. *See id.*

12. "A National Security Letter (NSL) seeks customer and consumer transaction information in national security investigations from communications providers, financial institutions and credit agencies." CHARLES DOYLE, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND AND RECENT AMENDMENTS 1 (2009). "Section 505 of the USA PATRIOT Act expanded the circumstances under which an NSL could be used." *Id.* (citing Pub. L. 1-7-56, 115 Stat. 365 (2001)).

13. HOFFMAN ET AL., *supra* note 7, at 49-50.

14. *Id.* at 50.

15. *Id.* at 151.

16. *Id*. at 37.

17. Julian Hattem, *McConnell: NSA reform would help ISIS*, THE HILL (Nov.18, 2014, 10:41 AM), http://thehill.com/policy/technology/224505-mcconnell-nsa-reform-would-help-isis.

18. Eric H. Holder, Jr., Attorney Gen., U.S. Office of the Att'y Gen., Remarks by Attorney General

lish safe havens online and conduct activities across borders, without regard to jurisdictions, and at very low cost compared to traditional crime.

Since the 1990s law enforcement has raised concerns that emerging technologies such as digital and wireless communications made it increasingly difficult to conduct court authorized surveillance. At the request of Congress, the Government Accountability Office examined the increasing use of digital technologies in public telephone systems, and found it to be a factor that could potentially inhibit the FBI's wiretap capabilities. To help law enforcement maintain the ability to execute authorized electronic surveillance, Congress enacted the Communications Assistance for Law Enforcement Act.[19]

CALEA requires telecom carriers to ensure that if they enable customers to communicate, they will enable law enforcement to conduct court-ordered surveillance.[20] CALEA's requirements were administratively expanded by the FCC in 2006 to apply to broadband Internet access and Voice-Over-Internet-Protocol providers.[21] This rule was subsequently upheld as reasonable by a U.S. Court of Appeals in 2006.[22] However, CALEA's requirements did not cover electronic mail, instant messaging, peer-to-peer communications, or social media.

In 2007 Apple introduced the iPhone, the first widely adopted smart phone, capable of communicating across a number of different platforms, and storing large pieces of data including photographs and video. CALEA is not viewed as applying to data contained on smart phones, and there has been a great deal of debate about whether it should be expanded to cover this content.

In 2009, the FBI briefed Congress about the "Going Dark" problem, and drafted legislation to amend CALEA to cover internet companies such as Apple, Facebook, Google, and Twitter that developed communications technologies not covered under the current act.

FBI general counsel Valerie Caproni warned Congress that the FBI's surveillance capabilities might diminish as technology advanced. Caproni, now a Federal judge, singled out e-mail, social-networking sites, and peer-to-peer communications as problems leaving the FBI "increasingly unable" to conduct lawful wiretapping.[23]

An FBI representative told the technology website CNET that rapidly changing technology poses significant challenges to the FBI, creating a growing gap between the existing statutory authority of law enforcement to intercept communications

Holder at the Biannual Global Alliance Conference Against Child Sexual Abuse Online (Sept. 30, 2014) (transcript available at http://www.justice.gov/opa/speech/remarks-attorney-general-holder-biannual-global-alliance-conference-against-child-sexual).

19. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103, 108 Stat. 4279 (1994).

20. *Id. See also Communications Assistance for Law Enforcement Act*, FED. COMMC'NS COMM'N ENCYCLOPEDIA, http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act (last updated Nov. 24, 2014).

21. *See Communications Assistance for Law Enforcement Act*, FED. COMMC'NS COMM'N ENCYCLOPEDIA, *supra* note 13.

22. *See* American Council on Educ. V. FCC, 451 F.3d 226 (D.C. Cir. 2006).

23. *See* Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites – Now*, CNET (May 4, 2012, 9:24 AM), http://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/.

pursuant to court order and the practical ability to do so. The Bureau believes that if this gap continues to grow, "there is a very real risk of the government 'going dark, resulting in an increased risk to national security and public safety."[24]

Draft legislation sought by the FBI was approved by the Justice Department, but the White House, less inclined than the Bureau to initiate a bruising privacy battle, never sent the proposed CALEA amendments to Capitol Hill. A representative for Senator Patrick Leahy, then chairman of the Senate Judiciary Committee and an original co-sponsor of CALEA, said in 2012 that, "we have not seen any proposals from the Administration."[25] FBI Director Mueller said in December 2011 that CALEA amendments will be "coordinated through the interagency process," meaning they would need to receive Administration-wide approval, which has not yet been forthcoming.[26]

Stewart Baker, former assistant secretary for policy at the Department of Homeland Security, said the FBI has "faced difficulty getting its legislative proposals through an Administration staffed in large part by people who lived through the CALEA and crypto fights of the Clinton Administration, and who are jaundiced about law enforcement regulation of technology—overly jaundiced, in my view."[27]

As a Senator, Vice-President Biden introduced the Comprehensive Counter-Terrorism Act of 1991, a bill that corresponded to the FBI's current CALEA reform proposals.[28] That bill provided that companies should "ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."[29] Vice-President Biden's previous support for giving law enforcement and the intelligence community robust tools to fight terrorism shows that this is not a political issue. It is a matter of national security that is supported across government.

Expanding CALEA to cover new technologies does not mean expanding wiretapping. Any law enforcement agency will still need to obtain a court order from a judge, based upon probable cause, to conduct electronic surveillance. Again, as a member of the Intelligence Committee and past Chairman of the Homeland Security Committee, briefed regularly on these issues, I am unaware of any authorized government surveillance of the content of any American citizen's communications, absent an Article III judge's order to do exactly that.

Under an amended CALEA regime, if a court order is required today, one will be required tomorrow as well. The substantive Fourth Amendment law and the Federal Rules of Criminal Procedure and Evidence will not change. The point of amending CALEA is only to make sure that if a wiretap is duly authorized by a judge, it can practically be executed. The sub rosa communications of criminals and terrorists must be legally exploit-able by the FBI in order to bring them to jus-

24. *Id*.
25. *Id*.
26. *Id*.
27. *Id*.
28. Comprehensive Counter-Terrorism Act of 1991, S.266, 102nd Cong. § 2201 (1991).
29. McCullagh, *supra* note 23.

tice.

Appearing before my Subcommittee on Counterterrorism and Intelligence, International Association of Chiefs of Police (IACP) President Richard Beary testified about the challenges facing police departments across the country: "Unfortunately, those of us who are charged with protecting the public aren't always able to access the evidence we need to prosecute crime and prevent terrorism *even though we have the lawful authority to do so.* We have the legal authority to intercept and access communications and information pursuant to appropriate legal processes, *but we lack the technological ability to do so.*"[30] He added, "The law hasn't kept pace with technology, and this disconnect has created a significant public safety problem, which is what we mean when we refer to 'Going Dark.'"[31]

Chief Beary noted that, "Law enforcement is not seeking broad new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Rather, we are simply seeking the ability to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders – information of potentially significant consequence for investigations of serious crimes and terrorismFalse [CALEA] needs to be changed to incorporate new communications technologies."[32]

"Critical investigations increasingly rely on digital evidence lawfully captured from smart phones, tablets and other communications devices. [Law enforcement's] inability to access this data, either because we cannot break the encryption algorithm resident in the device, or because the device does not fall under CALEA or the developer has not built the access route, means that lives may well be at risk or lost, and the guilty parties remain free."[33]

CORPORATE AMERICA LOSES ITS NERVE

In reaction to Snowden's illegal releases of classified material, and political pressure from Europe, when Apple released its latest mobile operating system in September 2014, it included a new privacy policy regarding password-protected personal data stored on devices running iOS 8.

Apple stated that the company cannot now bypass its customers' pass-codes, and therefore cannot access their data. Apple concluded, "So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."[34]

Soon after, Google declared that the next version of its Android operating sys-

30. *Subcommittee Hearing: Addressing Remaining Gaps in Federal, State, and Local Information Sharing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Sec.*, 114th Cong. (2015) (statement of Chief Richard Beary, President, International Association of Chiefs of Police).

31. *Id.*

32. *Id.*

33. *Id.*

34. Privacy, *Government Information Requests*, APPLE (2015), http://www.apple.com/privacy/government-information-requests/.

tem would include privacy protections—including default encryption of data only accessible by entering a valid password, to which Google does not have a key, similarly absolving the company of the ability to unlock devices for anyone.[35]

FBI Director Comey has rightly responded to these developments, discussing his concerns about these policies and law enforcement access to what the FBI calls "data at rest." In a speech last year at the Brookings Institution, Director Comey stated, "law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need."[36]

Director Comey continued, "Apple argues that its users can back-up and store much of their data in 'the cloud' and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement. And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data. Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?[37]

Director Comey cited a number of examples where data stored on a smart phone was critical to solving violent crimes and dismantle criminal enterprises, including:

A Louisiana sex offender posed as a teenage girl to entice a boy to a meeting where he murdered the boy, and then tried to delete evidence on their cell phones to cover up his crime. Both phones showed that the suspect enticed the boy into his taxi.

Los Angeles police investigated the death of a toddler from blunt force trauma to her head. There were no witnesses. Text messages on her parents' cell phones proved the mother caused the girl's death and that her father knew what was happening but failed to stop it, and that both parents "failed to seek medical attention for hours while their daughter convulsed in her crib" and "even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911." Confronted with text message evidence, both parents confessed.

35. Craig Timberg, *Newest Androids will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sep. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

36. James Comey, Director, Fed. Bureau of Investigation, Speech at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (transcript available at http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).

37. *Id.*

In Kansas City, the Drug Enforcement Administation used text message evidence to convict heroin dealers whose lethal product caused twelve overdoses, and five deaths, including several high school students.

The California Highway Patrol used red light cameras and phone data to convict a hit-and-run driver who killed a young couple and their four dogs.

Kansas police used cell phone evidence to exonerate several teens accused of rape.[38]

Law enforcement is to be commended for the creative use of technological evidence in each of these cases. Which of these cases would opponents of the CALEA amendments wish have turned out differently?

Director Comey is correct that there is a misconception that building a lawful intercept solution into a system requires a so-called "back door," that can be exploited for nefarious purposes. Law enforcement is not seeking a back-door approach. This process can and should be done with clarity and transparency, clearly laid out in law.

In all my discussions with law enforcement, I have found that they are fine with court orders and legal process to access the evidence and information they need to investigate crime and prevent terrorist attacks. Police have worked that way throughout the history of our country, at least since the adoption of the Exclusionary Rule.

A reasonable person might ask why the police cannot just compel the owner of the phone to produce the password? It is not clear how that might work, given the Fifth Amendment's protections against self-incrimination.

And even if it were possible in the ordinary course of criminal investigations to obtain such passwords, and admit evidence thereby obtained, without resorting to the "third degree", what happens if there is an imminent threat of a terrorist attack? Or a clear and present danger to the welfare of a child?

Does law enforcement have the time to navigate through the legal process in these circumstances when public safety is at risk? And worse, a criminal or terrorist would have a choice to sit through a contempt of court charge, for the length of the empanelment of a grand jury, rather than expose his plot or heinous crime.

But before such a tragic occurrence and the inevitable litigation takes place, American business should step back and return to the better traditions of their predecessors and cooperate with the U.S. government.

It is disappointing to see well-known U.S. companies back down to misinformed alarmists in order to preserve sales in foreign countries. As with our political leadership, America needs these companies to exhibit more leadership on these matters, as the private sector has in the past, partnering with the U.S. government to win World War II and the Cold War. These companies need to show more backbone and tell the public that they can sell good products that protect their Constitutional rights while taking into account the need for adequate public safety protections.

38. *Id.*

Conclusion

Criminals, cyber-spies and terrorists will exploit any vulnerability they find. It makes sense from a cost, policy and legal perspective to develop lawful intercept solutions during the design phase of new products, rather than resorting to patch-work solutions when law enforcement comes knocking with a warrant after the fact. With the advent of sophisticated encryption, there might be no solution in a critical and difficult case, leaving U.S intelligence and law enforcement agencies and American citizens at a dead end—all in misguided pursuits of privacy and network security.

As Chief Beary and Director Comey have said, more criminal evidence is being stored on a phone or a laptop, sometimes with a password that cannot be decrypted. Are we willing to accept that homicide cases could remain unresolved, terrorists could continue plotting unobstructed, and child exploitation could go undiscovered, all because of a locked smart phone or an encrypted computer? I am not willing to take that risk.

Unfortunately, the choices before us are neither simple, nor perfect, but I am confident that they can be balanced to afford citizens a right to privacy, while providing law enforcement and intelligence agencies tools they need to keep us safe.

Some "leaders" in Washington today attack the institutions that keep us safe. I have visited with the men and women who form the backbone of these institutions, including the NSA, FBI and the New York Police Department (NYPD). They are dedicated public servants, committed to keeping America safe, in compliance with robust congressional, executive and judicial oversight.

Some of my colleagues in Congress enjoy talking about the importance of freedom and liberty, while at the same time criticizing the very institutions that safeguard these values. As public figures whom Americans look to for leadership, they cannot have it both ways. The freedoms and liberty that we take as a right today, are in large part due to lawful security measures authorized by Congress and carried out by our intelligence and law enforcement agencies. America needs more leaders who value our right to privacy from government interference, but are also willing to articulate the role of national security in safeguarding the homeland from a complex global terrorist threat that is agile and constantly evolving. To that end, Congress must renew the PATRIOT Act, including Section 215 and 702 authorities, and amend CALEA to deal with twenty-first century threats.