

**THE CIPHER**  
BRIEF

SPECIAL REPORT

AMERICAN DILEMMA:

# SECURITY VS. PRIVACY





**The U.S. government is in a bind: It wants to stop criminals and terrorists, but it also wants to fulfill its obligations to respect its citizens' right to privacy.** Navigating this quandary has been a problem for years, and with the popularity of social media, the volume of data about individuals' lives that is available to be analyzed—and exploited—has increased exponentially. Not only does this mass of data have the potential to overwhelm intelligence analysts and law enforcement officers if they tried to crunch it all, it raises the question: what information is fair game in today's world and for what causes? As then-FBI Director James Comey once said, “Are we so mistrustful of government—and law enforcement—that we are willing to let bad guys walk away... willing to leave victims in search of justice?”

But Michelle Richardson, deputy director of the Center for Democracy & Technology's Freedom, Security, and Technology Project, is among a number of privacy advocates who argue that the government is scooping up far too much personal information in the name of a “generic national defense catchall [statute] that sweeps in all kinds of legal conduct” such as discussions of climate change and intellectual property theft.

*The Cipher Brief takes an in-depth look at how the expanding digital world has been a challenge for those charged with keeping Americans safe, while at the same time protecting their most cherished civil liberties.*

[Digital Tools: Creating the Haystack to find the Needle](#)

[Defining A Reasonable Expectation of Privacy](#)

[Does Technology Trump the Law?](#)

[Security vs. Privacy: Do Other Nations Have It Figured Out?](#)

# Digital Tools: Creating the Haystack to find the Needle

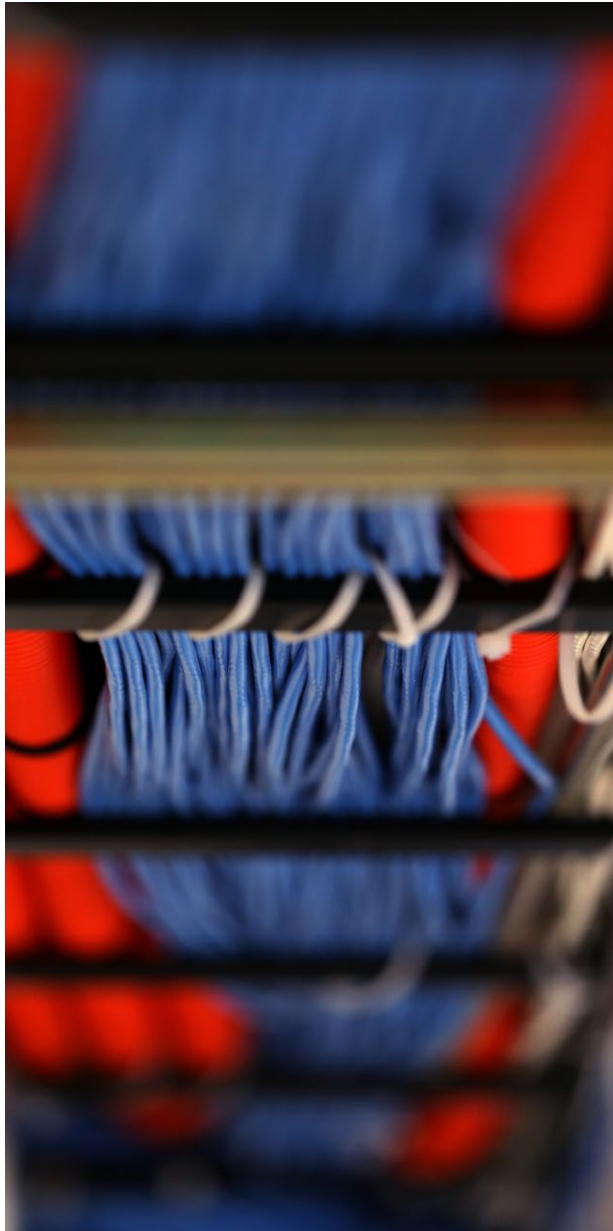
By Levi Maxey

Intelligence collection has changed enormously since the end of the Cold War. Governments certainly still cultivate deeply embedded human intelligence sources, who hear, firsthand, some of the most sensitive national security information. But the growth of cyberspace changed espionage dramatically.

General Michael Hayden, the former director of both the NSA and CIA, refers to this period in history as “the golden age of SIGINT,” or signals intelligence – a field that includes intercepting both military and civilian radio signals, satellite links, telephone traffic, internet activity, and data gleaned from breaching computer networks.

The expansion of U.S. reliance on signals intelligence arrived alongside the wars in Iraq and Afghanistan, and the fight against terrorism, which has expanded to Syria, Yemen, Libya, Somalia, Nigeria, and Pakistan. Between 2001 and 2010, the NSA [bolstered](#) its workforce by one-third to 33,000 and nearly doubled its budget. And its dependence on private contractors grew from 150 in 2001 to nearly 500 by the end of 2010.

But the NSA is not the only government body conducting signals intelligence collection, so do others such as the FBI, DEA, DIA, and CIA.



Source: Getty Images/Michael Bocchieri

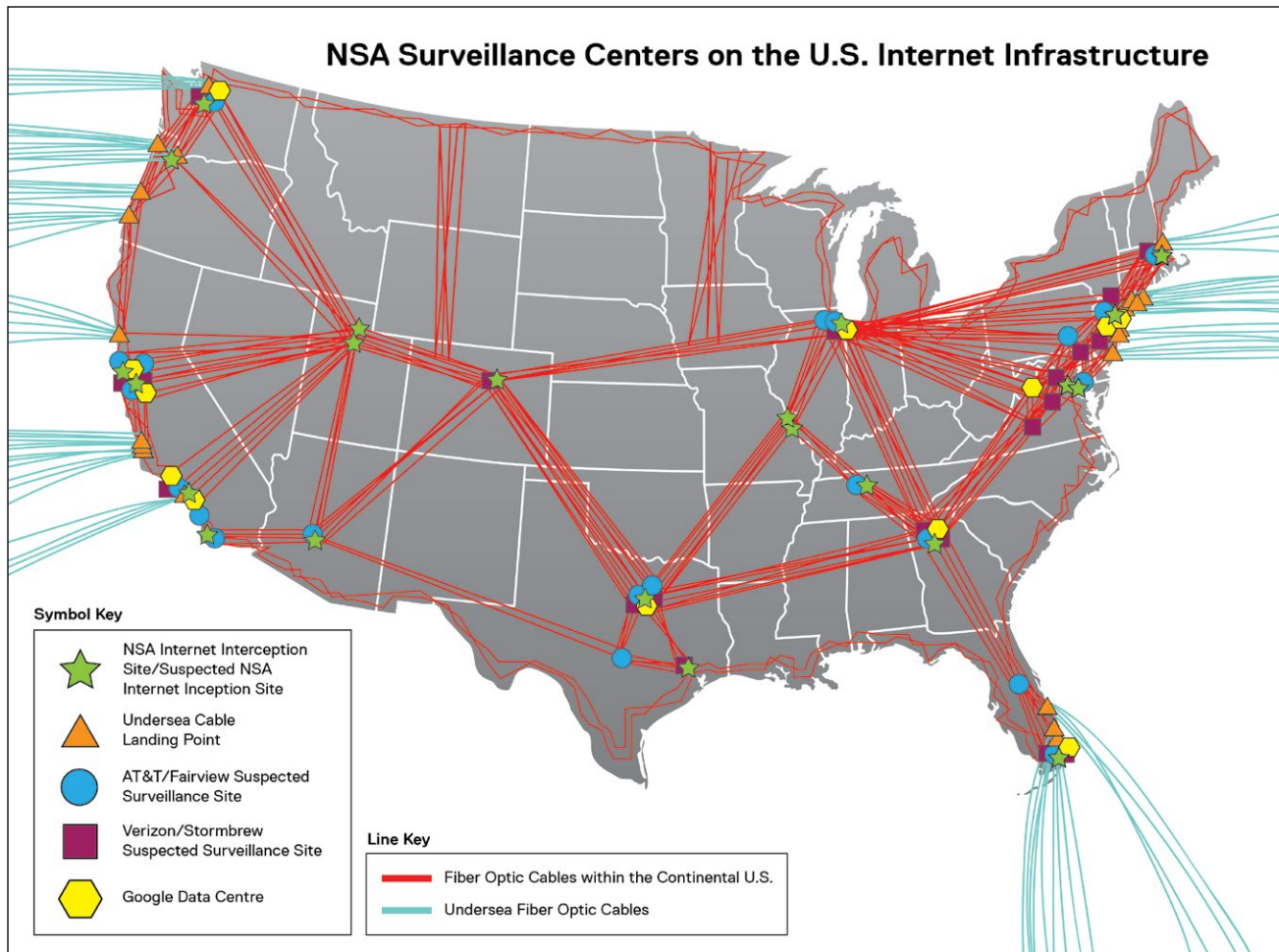
The CIA has made major strides in collecting digital communications as part of its new Directorate of Digital Innovation and numerous exploits revealed in WikiLeaks's so-called Vault7 cache.

According to the Washington Post, of the \$52.6 billion set aside in the 2013 “[black budget](#)” for the U.S. intelligence community, some \$14.7 billion was designated for the CIA, a 56 percent increase since 2004. In comparison, the NSA – long considered the behemoth of the community – accounted for \$10.8 billion, still a 53 percent increase over the last decade.

While some of the CIA's growth can be attributed to an uptick in covert action and counterterrorism operations, the news report indicates the black budget summary refers to CIA “offensive cyber operations” and notes the CIA's “aggressive new efforts to hack into foreign networks to steal information or sabotage enemy systems.” The amount of digital information the CIA now collects has even prompted [changes](#) in how the agency analyzes and stores this data.

Phone-based communications provide insight into terrorists' networks and planning, as well as the political, military, and diplomatic happenings of foreign governments





Source: Loosely based off data obtained from [ixmaps.ca](http://ixmaps.ca) and the University of Wisconsin-Madison

around the world. By vacuuming up mobile phone communications with overhead drones and breaching the networks of local telecommunications companies and individual devices, both the NSA and CIA can access a wealth of data.

But the internet has expanded the amount of information available exponentially, both in terms of quantity and geography. A complex and vast array of fiber optic cables running along the ocean floor

into peering stations and data centers throughout the world drive the internet. This provides the means for foreign intelligence targets to communicate with each other across distances. But it often is done using U.S. internet services, such as Google, Facebook, AOL, Yahoo, and others – meaning their data is regularly stored within the United States.

What's more, internet communications are broken into a number of small packets of data that are sent independently, over whatever route is optimal for each, and reassembled at the destination – a process known as packet-switching. This means that portions of emails sent from Pakistan to Afghanistan, for example, often travel through U.S.-based internet infrastructure.

This combination of foreign intelligence targets using U.S. internet services and communications data transiting U.S. borders is the basis for bulk data collection under Section 702 of the Foreign Intelligence Surveillance Act, also known as the 2008 FISA Amendments Act. The

provisions allow NSA and other agencies to request data from major internet companies that hold both the content and metadata – or the who, when, where, and how of internet communications. This process is called 'downstream collection,' and companies are required to provide the information. Section 702 also authorizes 'upstream collection' by which the NSA is also able to tap right into the physical infrastructure of the internet, siphoning off data as it travels by.

“When discussing bulk data collection, there are always references to

finding the needle in the haystack as if the haystack existed already,” Robert Eatinger, the former Senior Deputy General Counsel at the CIA and Cipher Brief expert, notes. “But what it is really like is that you have to make your own haystacks because the straws are just flying by, and if you miss it, it’s gone. You can’t search it.” Instead, “you have to collect all the straws to have the haystack to begin with before you can search inside of that for the needle,” he argues.

This problem is especially difficult when the NSA knows there are terrorists, criminal syndicate leaders, or foreign intelligence officers out there, but they do not yet know their specific identifiers – such as a name, email address, phone number, or credit card number affiliated with an individual of interest – and therefore cannot attain a specific FISA warrant for them. “At that point,” Doug Wise, the former Deputy Director of the Defense Intelligence Agency and a Cipher Brief expert, says, “we can no longer have targeted collection, so that is the whole purpose of bulk collection – whether its bulk metadata, bulk emails,



Source: iStock/baranozdemir

“  
*You have to collect all the straws to  
have the haystack to begin with  
before you can search inside of  
that for the needle.*

– Robert Eatinger

”

bulk financial transactions, or bulk transportation data like plane, train, and ship tickets.”

After collecting all of that, you can attempt to sift through the reams of data to find individuals of interest. But only once a precise identifier affiliated with an individual – known as a selector – is discovered, can “you can go back and see if he has said anything in the past,” says Eatinger. “It can only be retrospective, and that is only if you have a selector.”

The inevitable problem with such indiscriminate collection is that the communications of U.S. citizens will inadvertently get picked up during foreign-focused collection, creating concerns over civil liberties and privacy infringement.

“Innocent people conducting innocent transactions are all mixed up with nefarious people conducting nefarious transactions,” says James Clapper, the former U.S. Director of National Intelligence and Cipher Brief expert. “We do our best to try to separate those, but sometimes inadvertent collection happens, particularly if you don’t know the identity of the target.”

Concerns over privacy infringement under bulk collection peaked after disclosures made by the former NSA contractor Edward Snowden in 2013. The authorities under 702 are due to expire at the end of the

year if Congress does not authorize their renewal. Many in the national security realm fear that if not renewed, the collection authorities lost could greatly impact the U.S. intelligence community's ability to measure security threats. Rob Joyce, the Cybersecurity Coordinator at the National Security Council, argues that "we can't afford to have a blind spot" simply because "America has great technology" that foreign people choose for their communications.

What such bulk collection does offer is the ability to map out networks of individuals through association. As Rhea Siers, the former Deputy Associate Director for Policy at the NSA and Cipher Brief expert, points out, "network knowledge is an important element of tracking potential terrorists or criminals, and understanding their organizational dynamic is critical to assessing threats or potential impact." This is particularly true after a terrorist attack, whereby investigators then can follow a trail of digital breadcrumbs to a broader network of affiliated individuals.

"The difficult question is when do we 'drill down' from network indicators to specific individuals," says Siers. "Understanding that some terror or criminal organizations have a series of concentric functions – such as strategists, money, operations, logistical support, and followers – does help us focus on key nodes." This kind of social network mapping enables intelligence agencies to focus their limited resources and personnel on those most serious threats and intervene when the need arises.

But despite its apparent utility, bulk collection presents challenges of its own. Following a series of recent terror attacks in the United Kingdom, the flood of data is [overwhelming](#) the limited number of intelligence analysts. British security services have an estimated 3,000 suspected terrorists within the UK on their radar but do not necessarily have the resources or legal basis to closely monitor all of them, all of the time. Accordingly, some slip past security nets. Terabytes of communications data flow into intelligence coffers daily. To put that in perspective, a single terabyte is 1,024 gigabytes; one

gigabyte can hold some 1.5 million WhatsApp messages.

Human analysts cannot possibly navigate this burgeoning pool of digital intelligence manually. And intercepted communications are only one source of intelligence. The amount of open source information available can also be extraordinary. "Imagine trying to search through YouTube for every video clip of a martyrdom or somebody teaching people how to produce an improvised explosive device," says Jason Matheny, the Director of the Intelligence Advanced Research Projects Activity (IARPA). "The impossibility of somebody doing that manually is clear. We have to have some method for automatically analyzing its contents to figure out if this is the sort of video that an analyst is trying to find."

Leveraging data analytic tools to scrutinize the deluge of information now available can alleviate the workforce burden placed on intelligence services. Advances in artificial intelligence and machine learning can help recognize patterns for valuable insight, augmenting the efforts of human analysts and helping them to work more efficiently and effectively.

"There are two main capabilities these analytical tools have," says Mark Testoni, the President and Chief Executive of SAP NS2, a data analytic company working in national security. "Through this morass of information, we can identify nefarious groups, actors, and direction of movement," he says. "Once we identify them, we can identify patterns of behavior for individuals and groups they are linked to, and from there, determine through behavioral changes whether they are preparing to do something malicious." For example, sudden halts in communication between militants and their leadership can indicate a move toward enhanced operational security awareness – potentially signaling an attack is forthcoming.

The challenge is not only analyzing large quantities of data, but also bringing together data from disparate sources, such as audio, images, text, video, and geospatial data across classified and publically available

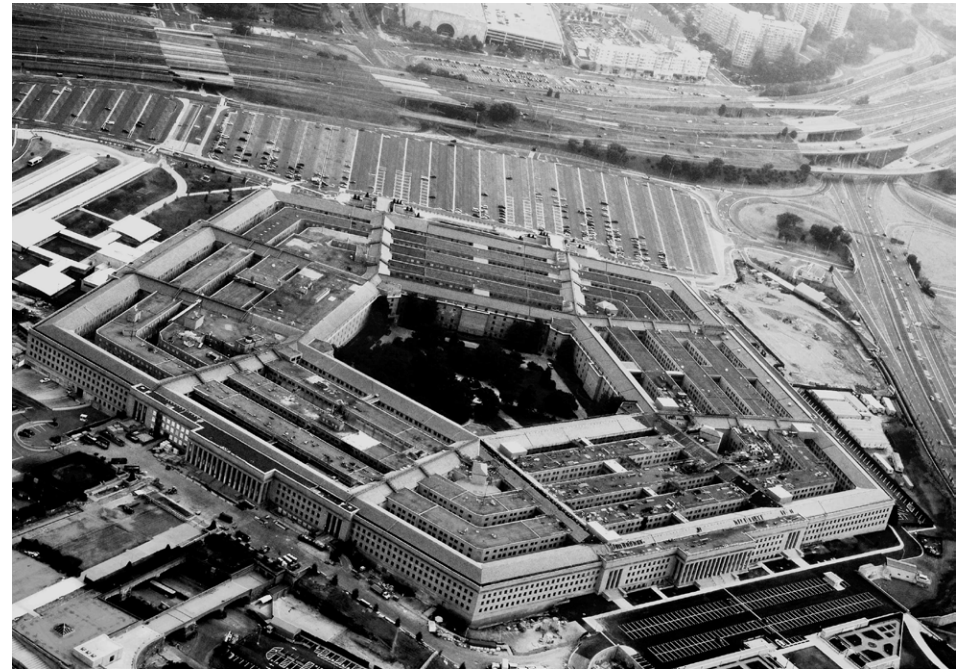


platforms. Larger societal events, such as disease outbreaks, political instability, and economic crises, can be extrapolated in real time – perhaps even before they occur – from data such as food and gas prices, overhead imagery of crowding at clinics, or collective action organizing through social media platforms.

“You can learn a lot about the world if you combine indicators and signals from different kinds of data,” says Matheny. “Each kind of data has its own problems, its own biases, so it is really by combining these indicators across the data that you can make a reliable forecast.” A single indicator can mislead analysts, obscuring the full picture, particularly regarding the dynamic events that intelligence agencies deal with every day.

One example of bringing together diverse sources of intelligence is the Pentagon’s military intelligence, surveillance, and reconnaissance program called Insight, which is run by the Defense Advanced Research Projects Activity (DAPRA). The program is designed to break down the barriers between signals, human, open source, and geospatial intelligence through automated integration that is fused into a single cloud-based repository. This allows analysts to get a broader picture of events on the ground.


“One of the problems with current systems is that they are stove-piped databases and other repositories that are sometimes even specific to the sensor,” says Steve Jameson, the Insight Program Manager at DARPA. Intelligence platforms like Insight allow analysts to query the system, see automatic updates the system is providing, inspect the underlying data, understand what the rationale is for the results that the system is presenting to them, and, if necessary, adapt or change the results that the system provides. Jameson argues that “this ability to drill down from the top-level product, all the way down to the underlying source data, is key not only to improve the ability of the analyst to do their job, but to improve their ability to trust the system.”



Source: iStock/Mlucas

Known as “explainable” artificial intelligence, the systems allow humans to transparently understand why it selected certain behaviors and individuals for indicators – a crucial component of any predictive analytic tool designed to help forecast, and in turn preempt, prevent, and plan for courses of action.

Take, for example, an enemy force that has multiple routes by which to approach a friendly force. Anticipating how the enemy force will maneuver is largely a manual process at present, but soon indicators can be fed into an artificially intelligent platform designed to augment operational planning, highlighting “each course of action as a hypothesis about what the enemy is doing and what they are going to do,” says Jameson. With this information, military commanders will be able to better determine which routes opposing forces will take, and therefore better fortify themselves, lay traps along the way, or even maneuver for their own offensive.



The fear, however, is that the underlying algorithms of artificial intelligence could perpetuate biases encoded in them, even potentially leading to self-fulfilling prophecies; anticipating violence can often lead to violence.

Moreover, “there are still debates over the amount of data necessary to correctly track threats and whether there is a sufficient data feedback loop to avoid a high error rate,” says Siers. “A high error rate means a lot more human analysis or eyes on the problem,” the very challenge these technologies are seeking to resolve. False positives could mislead analysts, and ill-advised indicators could divert attention from where the focus should be.

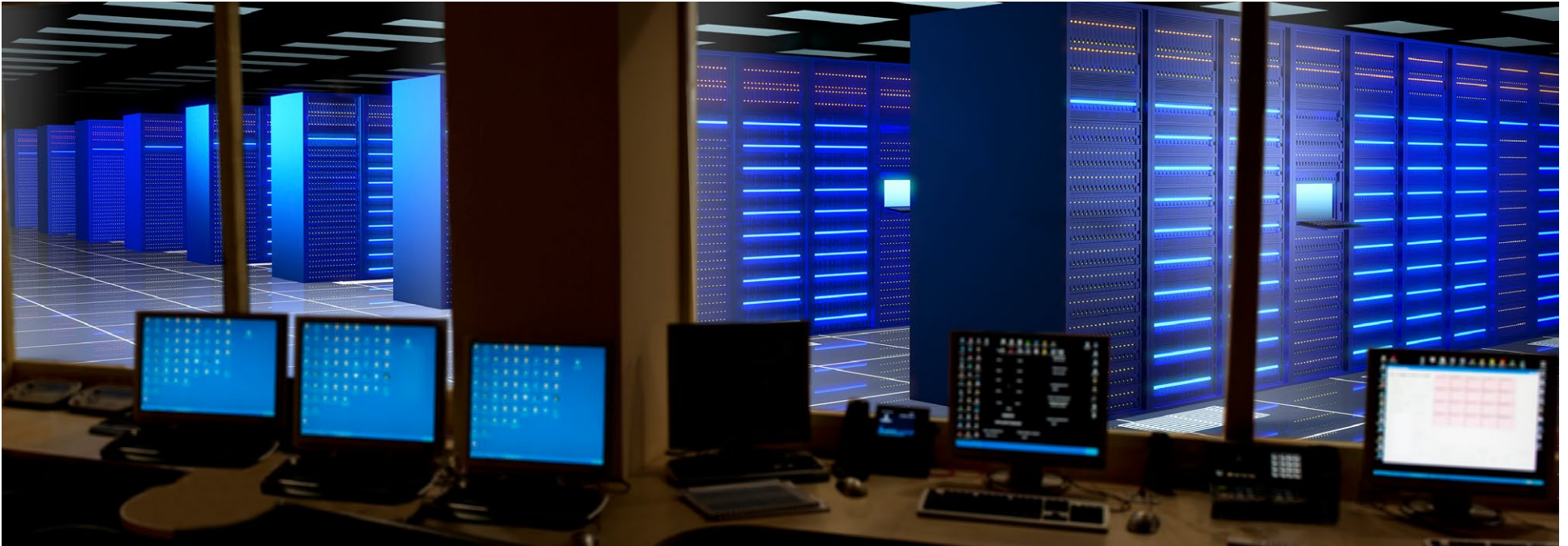
But while intelligence analysts may be limited in their ability to effectively sift through the troves of data available to them, the data is out there. Commanding it can help societies understand the threats posed against them. Data analytic platforms that leverage machine learning and artificial intelligence have the potential to alleviate the analytical burden on intelligence services while allowing them to zoom in and out of a more comprehensive and dynamic portrait of the national security landscape. The path towards such a future, however, will need to be deliberative, transparent, and approached with caution.

Source: Getty Images/Dean Mouhtaropoulos



# Defining A Reasonable Expectation of Privacy

By Mackenzie Weinger



Source: Getty Images/baranozdemir

In today's information world, with social media, open source material, and the internet of things generating extraordinary amounts of data, national security professionals must sift through a massive pool of information as they seek to combat threats to the United States. And, as technology develops, the government must grapple with the pressing question of how to exploit that information without violating the rights of its citizens to privacy.

"We'd like to have total privacy and total security. We're not going to get either," General Michael Hayden, former NSA and CIA director, says. "We're going to have to balance. The fulcrum might change from country to country and based on recent events, like terrorist attacks and the willingness of the population to give up something in order to

get something. That's the process of governing."

For U.S. citizens, "the fundamental legal protection for privacy, which is the Fourth Amendment, hasn't changed," Elizabeth Goitein, who co-directs the Brennan Center for Justice's Liberty and National Security Program, says.

"But it just becomes harder, I think, to translate what that means when you are living in the digital age... there are new technologies that change the way in which people communicate and the ways in which they share or seek to protect their personal information," she says.

Machine learning, big data, and artificial intelligence are boosting the

capabilities of the government to synthesize and analyze massive amounts of information. Social media and open source information gleaned online offer a potential windfall to law enforcement and the intelligence community — and bad actors such as illicit traffickers and terrorists, too, who use these technologies to communicate, transfer funds, and radicalize others.

As the former special envoy and coordinator of the State Department's Global Engagement Center, Michael Lumpkin worked during the Obama administration to combat extremists in the online space. With ISIS treating the information battlefield with the same seriousness it does the physical battlefield, the U.S. faces a significant threat even as the group splinters and loses territory. ISIS has demonstrated a propensity for and effectiveness in targeting people susceptible to their messaging online.

“Working in the information space, trying to counter violent extremism in the information environment, is probably the most complex job I’ve ever had by far. Our adversaries are not constrained by ethics, the truth, or, frankly, the law. We, on the other hand, are. And rightly so. But it puts us at a competitive disadvantage,” he says.

The U.S. must confront significant threats — terrorist recruitment and homegrown radicalization, for instance — where synthesizing mass amounts of information could prove significant in determining who to potentially target for preventative or offensive purposes. And it must do so under the law, in consideration of the Fourth Amendment, the Privacy Act of 1974, which governs the collection, maintenance, use, and dissemination of information about people that federal agencies maintain in their records, and other legal limitations.

There is a wealth of information available for those in the national security space to sift through, and new technologies are increasingly

able to help the U.S. government navigate that pool of data. But these advances often must be weighed by the courts first, and balanced with the established and intrinsic rights of U.S. citizens.

“There are clearly First and Fourth Amendment issues that are of great concern here. Further, we need to recall the lessons of the ‘bulk collection’ debate we’ve experienced recently — even when we can supply a legal basis for the effort, we need to be cognizant of balancing the public’s trust in law enforcement and intelligence,” Rhea Siers, former Deputy Associate Director for Policy at the National

Security Agency, and the scholar in residence at George Washington University’s Center for Cyber and Homeland Security, says.

There have been suggestions that the U.S. deploy “bots” against social media — Artificial Intelligence Targeting Personas, or AITP — to look for possible evidence of radicalization of individuals, Siers notes. These social media bots would automatically engage with individuals online and then report back to a human if any signs of extremism are discovered. “In this case, there are many potential dangers, beyond potentially discriminatory data, to a broad impact on free speech,” she says.



Source: Getty Images

The U.S. is still in the midst of this conversation about privacy and national security, and the rapid transformation of digital and technological capabilities “requires legal and technology experts who can carve out policies and potential changes, if needed, to the law on a continuous

“  
*We’d like to have total privacy and total security. We’re not going to get either. We’re going to have to balance.*”

– General Michael Hayden



basis,” according to Siers.

This is urgently needed, given the capabilities that these analytical tools offer those in the national security space, allowing them to navigate through the morass of information to identify nefarious actors or groups and then, once they’ve been detected, find possibly significant patterns.

“

*Our adversaries are not constrained by ethics, the truth, or, frankly, the law. We, on the other hand, are.*

– Michael Lumpkin

”

“It really can be a potential boon to law enforcement and the intelligence space to see if we see behavior patterns either changing or concentrations of individuals or open source activity that, because of historical patterns, may indicate something is about to happen and where it may happen,” Mark Testoni, president and CEO of SAP NS2, says.

When it comes to data mining programs at the national level, federal agencies are required to put out reports if they are doing pattern-based data mining instead of subject-based data mining, Rachel Levinson-Waldman of the Brennan Center for Justice at NYU Law School, notes. This provides information for privacy experts to review when assessing the programs.

But even with transparency requirements in place, there is often very little information into how such programs work or what purpose they serve.

“There’s a concern for how pattern-based data mining could be used,

especially in the counterterrorism context,” Levinson-Waldman, a senior counsel to the Liberty and National Security Program at the Brennan Center, says. “There’s a lot of skepticism on the privacy and civil liberties front about the utility of doing this kind of data crunching and especially predictive work from a national security point of view, in large part because it is simply much harder to predict national security threats, at least with this kind of big data analysis.”

There are areas where predictive technologies have been largely seen as successful — for example, targeting credit card fraud, where there are hundreds of millions of data points to crunch, she said.

However, in that example, “if you get it wrong, it’s not that big of a deal. Getting it wrong on something like predicting a terrorist threat, predicting a national security threat, has very concrete civil liberties consequences. And there’s basically no way not to get it wrong probably a pretty high percent of the time,” Levinson-Waldman points out.

And in the U.S., although the government may seek ways to exploit new technologies to try to counter threats – including terrorist threats – to national security, the law explicitly protects U.S. persons.

“Terrorists are private citizens. I think that’s important. The fact that you call somebody a terrorist doesn’t mean they lose their Fourth Amendment rights if they are a U.S. citizen or someone inside the United States,” Goitein notes.

That’s a particularly American view of privacy, Hayden says. “We divide the world into people who are protected and people who are not protected by the Fourth Amendment. If you’re not protected, tough,” he says.

The government and the private sector must also wrestle with the U.S. legal concept of the so-called ‘third-party doctrine.’ Every call made or click online can leave a digital trail that could be stored and



Source: Getty Images/Patrick Lux

subsequently analyzed. But on top of that, there are concerns about the privacy vulnerability created by the concept that people who voluntarily give third parties — such as a social media companies, apps, or cloud-based services — information do not have a reasonable expectation of privacy.

In 1979, the Supreme Court ruled in *Smith v. Maryland* that a person has no legitimate expectation of privacy from warrantless government access to information voluntarily revealed to a third party.

“I’m a little notorious for a line — metadata is powerful, we kill people based on metadata — which is only a slight exaggeration,” Hayden says. “So maybe *Smith v. Maryland* ought to be reconsidered. And again the question becomes, where does privacy become invoked — access, collection, or actual use? I want to be able to access anything. I don’t want to collect everything. And, with regard to how I go into the database, the collection privileges may be far broader than the privileges I have to go into the database.”

And U.S. courts are contending anew with this issue in the digital age. The Supreme Court will soon hear a case, *Carpenter v. United States*, about whether the Fourth Amendment protects the government’s warrantless seizure and search of phone location records, for example.

“We’re getting into an era where we may need to redefine reasonable expectations of privacy, Hayden says.

“

*The fact that you call somebody a terrorist doesn’t mean they lose their Fourth Amendment rights if they are a U.S. citizen or someone inside the United States.*

– Elizabeth Goitein

”



According to the Brennan Center's Goitein, there certainly exists an argument under the third party doctrine regarding people sharing personal information with social media platforms, "but I think that people are increasingly coming to understand that that is a specious way of looking at things."

"I think things get trickier when you start to talk about information, for example, something people post on Twitter where they have in theory indicated they want that information to be available to the public," she says.

Great changes in the digital and technological realms do not mean there should be shifts in the U.S. government's approach to the concept of privacy, Goitein says.

"If we're talking about private information — which is either information that somebody has clearly sought to keep private or it's private information that's being teased out of public information through technology — that's protected. And that protection means that the government, generally, depending on certain exceptions to the warrant requirement, has to get a warrant. And there's no reason for that principle to change as a result of technology," she says.

The U.S. must flesh out the privacy framework, however, to look beyond the tech we can comprehend in today's world. "Ultimately there will need to be more guidance to sort of put better flesh on the bones of the reasonable expectation of privacy test if we want to have answers for new technologies that come down in the future," according to Goitein.

"Finding a way of looking at these questions that will survive the next wave of technologies — that is a challenge, and I don't think we're much further along on that," she says.

AI, machine learning, and data analytics will make it easier to find persons of interest for those working in the counterintelligence and

counterterrorism realm, and that will significantly impact intelligence activities and national security in the near future, James Lewis, a senior vice president and director of the Strategic Technologies Program at CSIS, notes.

"One of the problems for the U.S. is we have a dysfunctional political system, so we may not be able to do things — but that doesn't mean other people aren't going to be able to do them," he says. "The reliance on digital devices means everyone's creating an ever-expanding data footprint, and those can be exploited for commercial purposes, for intelligence or law enforcement purposes. It's better to do it under a democracy, under the rule of law, but we may not be able to keep up."



Source: Getty Images/Dean Mouhtaropoulos

# Does Technology Trump the Law?

By Elaine Shannon

If you have something to hide, whether it's justifiably secret – your revolutionary new business plan, your bank passwords, your texts goofing on your brother – or guilty knowledge – details of an arms deal with a blood-thirsty militant band, the number of your drug dealer – you live in uncertain times.

Technology is often on your side, even when the law isn't. Many encryption programs, routinely installed in hundreds of millions of smartphones, computers, tablets, cloud storage, and other Digital Age information storage and communications devices are now more powerful than codes devised by hostile states during the darkest days of World War II and the Cold War.

“The advent of ubiquitous strong encryption is making more and more of the room in which the FBI investigates dark,” then-FBI Director James Comey said at a cyber security conference at Boston College last March. “Encryption has become...a feature of the work of the less sophisticated – of drug dealers, armed robbers, terrorists, pedophiles, of bad people of all sorts. That shadow is spreading from the corner across more and more of our work.”



Source: Getty Images/Wachiwit

Comey was making an impassioned plea for public support for legislation to force makers of phones, computers, and other digital devices to build back doors into their encryption programs so that law enforcement personnel who obtained court-approved search warrants could gain access to targeted devices or information held by internet service providers or cloud storage vendors.

The issue had been building for years but came to a head in December 2015, when Comey and his agents tried and failed to convince Apple, the computer giant, to unlock an iPhone used by Syed Rizwan Farook, a gunman who killed 14 people in San Bernardino, California. Farook died in a hail of police gunfire, and the FBI agents were racing against time, fearing that Farook might have been in touch with confederates plotting more terrorist attacks.

Apple insisted it didn't have a key to unlock Farook's phone, couldn't make one, and wouldn't consider adding a key system to the software for the next generation of iPhones.

“For many years, we have used encryption to protect our customers’



personal data because we believe it's the only way to keep their information safe," Apple chief executive Tim Cook said in an [open letter posted on the company website](#). "We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."

After three months of wrangling in the courts, Congress, and public meetings, the FBI found a private vendor – reportedly, an Israeli contractor – who unlocked Farook's phone without Apple's help. But that didn't solve the massive dilemma now facing American law enforcement and the court system: a large percentage of phones and other devices are encrypted.

Comey took to a college lectern in Boston, not an FBI-friendly venue, to try to build public support for limits on encryption. Over the final quarter of 2016, he said, the FBI and its partners had obtained court orders to search 2,800 phones and other devices in criminal, counterintelligence and terrorism investigations but could not gain access to 1200 of them – 38 percent – because they lacked the technical means. Uncounted thousands more devices seized at crime scenes or found in the effects of deceased victims of crimes are sitting in evidence lockers across the country, because local police forces are powerless to break their encryption.

The part of Comey's speech that made headlines was this blunt assertion: "There is no such thing as absolute privacy in America. There is no place outside of judicial reach...We all value privacy, I hope. We all value security. We should never have to sacrifice one for the other."

He took it further, saying "even our memories are not absolutely private in America. Any of us can be compelled in appropriate circumstances to say what we remember, what we saw. Even our

“

*The advent of ubiquitous strong encryption is making more and more of the room in which the FBI investigates dark.*

– James Comey

”

And while no one seriously questions the courts' authority, humans seem genetically programmed to seek a private space, judging by the booming market for encrypted devices and apps. [WhatsApp](#), a popular messaging and calling service that promises "end-to-end encryption, meaning that no third party including WhatsApp can read or listen to them," claims to have 1 billion users in 180 nations.

"The American public and the Congress have to decide where they want the line to be," says Elaine Lammert, formerly the FBI's deputy general counsel and a Cipher Brief network expert. "We saw right after 9/11 that the balance shifted toward the fear of not knowing when the next attack was coming and how it was coming. We did see a shift within society that said, security more than civil liberties."

But Lammert believes that over the past decade, as al Qaeda has tried and failed to pull off more spectacular attacks in the United States, public sentiment drifted back toward the privacy side of the equation.

However, Lammert says the threats have not gone away, and the

“

*...we believe the contents of your iPhone are none of our business.*

– Tim Cook

”

communications with our spouses, with our clergy members, with our attorneys are not absolutely private in America. In appropriate circumstances, a judge can compel any of us to testify in court about those very private communications."

All true, but sobering nonetheless.

And while no one seriously questions the courts' authority, humans seem genetically programmed to seek a private space, judging by the booming market for encrypted devices and apps. [WhatsApp](#), a popular messaging and calling service that promises "end-to-end encryption, meaning that no third party including WhatsApp can read or listen to them," claims to have 1 billion users in 180 nations.

"The American public and the Congress have to decide where they want the line to be," says Elaine Lammert, formerly the FBI's deputy general counsel and a Cipher Brief network expert. "We saw right after 9/11 that the balance shifted toward the fear of not knowing when the next attack was coming and how it was coming. We did see a shift within society that said, security more than civil liberties."

But Lammert believes that over the past decade, as al Qaeda has tried and failed to pull off more spectacular attacks in the United States, public sentiment drifted back toward the privacy side of the equation.

However, Lammert says the threats have not gone away, and the

government needs access to information to address the threats.

“I think people are very protective of their privacy, and they want secure devices that protect the information,” Lammert says. “You don’t want anybody to get into your phone – until something happens.” A parent whose teenager is dead or gone missing may suspect that he or she was in contact with a drug dealer, ISIS recruiter, sex offender, or gangbanger. That parent may be eager to have the police examine the kid’s calls and texts. By that time, it’s usually too late. The person who’s absent is the only one who possesses the password to the phone.

“

*We all value privacy, I hope. We all value security. We should never have to sacrifice one for the other.*

– James Comey

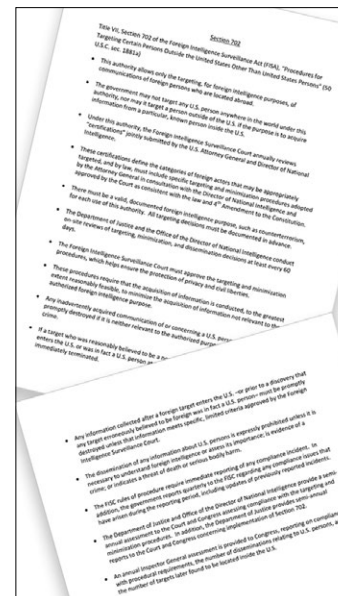
”

Most people know about cell phone encryption because most people have at least one mobile phone. According to the cell phone industry trade group, last year, there were 395.5 million cell phone subscriptions in the United States, one and a fifth phones for every man, woman and child in the population.

Year	Cell phone subscriptions in the United States
2016	395.5 million

Less well understood, and equally controversial, is the U.S. government’s use of intercepts to collect personal and business communications throughout the world. If you have something to hide, the powerful technology at the NSA may find it out, despite your best efforts.

Governments have been eavesdropping on one another and prominent individuals as long as electronic communications have existed. Wiretapping technology appeared [in the 1890s](#). In [1968](#), in response to a series of U.S. Supreme Court rulings and Congressional investigations, Congress passed a law requiring judicial warrants for wiretaps in criminal and so-called domestic security cases. The statute and rulings exempted wiretaps conducted for foreign intelligence purposes. In 1978, in the wake of the Watergate and intelligence agency scandals, Congress passed the Foreign Intelligence Surveillance Act (FISA), which set up a warrant process under the auspices of a new Foreign Intelligence Surveillance Court.



After the attacks of September 11, 2001, the administration of President George W. Bush initiated a warrantless surveillance program aimed at detecting communications of al Qaeda and other jihadist groups operating inside the U.S. and abroad. Congress codified the program in 2008 in amendments to the FISA act. Among other things, this law added a new section, 702, that allowed the government to target the communications of foreigners outside the United States without individual warrants, based on a joint certification by the Director of National Intelligence and the Attorney General. This section was reauthorized in 2012, with a sunset date of December 31 of this year.

Although the targets are foreigners who are overseas, they may be communicating with U.S. persons anywhere in the world, including in the United States.

In 2014, the [Washington Post reported](#) that files made public by NSA contractor Edward Snowden showed that “ordinary Internet users,



“

*You don't want anybody to get into your phone – until something happens.*

– Elaine Lammert

”

American and non-American alike, far outnumber legally targeted foreigners in the communications” swept up under the Section 702 program. Snowden’s disclosures have galvanized a coalition of civil liberties groups to lobby to let 702 expire, on grounds that it is permitting the NSA to gather massive amounts of information about Americans.

How many Americans have wandered into the NSA’s net has not been disclosed. The annual “transparency report” on the law issued in April by the Director of National Intelligence (DNI) said that the intelligence community targeted 106,469 people in 2016, up from 89,138 people in 2013. The word “target” is key. Since only foreigners can be designated as targets under Section 702, Americans who communicated with them are classified as “incidentally collected.”

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016
Estimated number of targets of such orders	89,138	92,707	94,368	<b>106,469</b>

In an exclusive interview with The Cipher Brief CEO Suzanne Kelly, White House cybersecurity coordinator Rob Joyce maintained that there has been “no intentional misuse” of 702. He called it a vital tool for the intelligence and law enforcement communities. “Just because America has great technology in which foreign people choose to communicate in an internet service provider that happens to come through the United States—we can’t afford to have a blind spot there,” Joyce said.

On June 7, DNI Daniel Coats; NSA Director Adm. Michael Rogers; Deputy Attorney General Rod Rosenstein and Acting FBI Director Andrew McCabe delivered a joint statement to the Senate Intelligence Committee advocating that Section 702 be reauthorized, this time, without a sunset provision.

The statute, they said, “provides critical foreign intelligence that cannot practicably be obtained through other methods.” For example, they said, by using 702, the intelligence community had:

- Identified the “personal network of an individual providing support to a leading terrorist in Iraq and Syria;” a successful military operation remov[ed] the terrorist from the battlefield.
- Alerted a foreign intelligence service to an al Qaeda sympathizer; he was recruited as a source against al Qaeda and ISIS.
- Arranged the arrest of two ISIS-affiliated militants who had traveled from Turkey to Africa and were planning to attack “U.S. personnel and interests.” After the arrests, the CIA “uncovered actionable intelligence on an ISIS facilitation network and ISIS attack planning,” the statement said.

Privacy advocates aren’t persuaded.

“They say it’s about targeting foreigners abroad, which we understand, but these people talk to Americans, so our privacy is implicated too,” says Michelle Richardson, deputy director of the Center for Democracy & Technology’s Freedom, Security, and Technology Project.

Richardson says that the statute’s language is overly broad, with a “generic national defense catchall that sweeps in all kinds of legal conduct,” such as discussions of climate change and intellectual property theft.

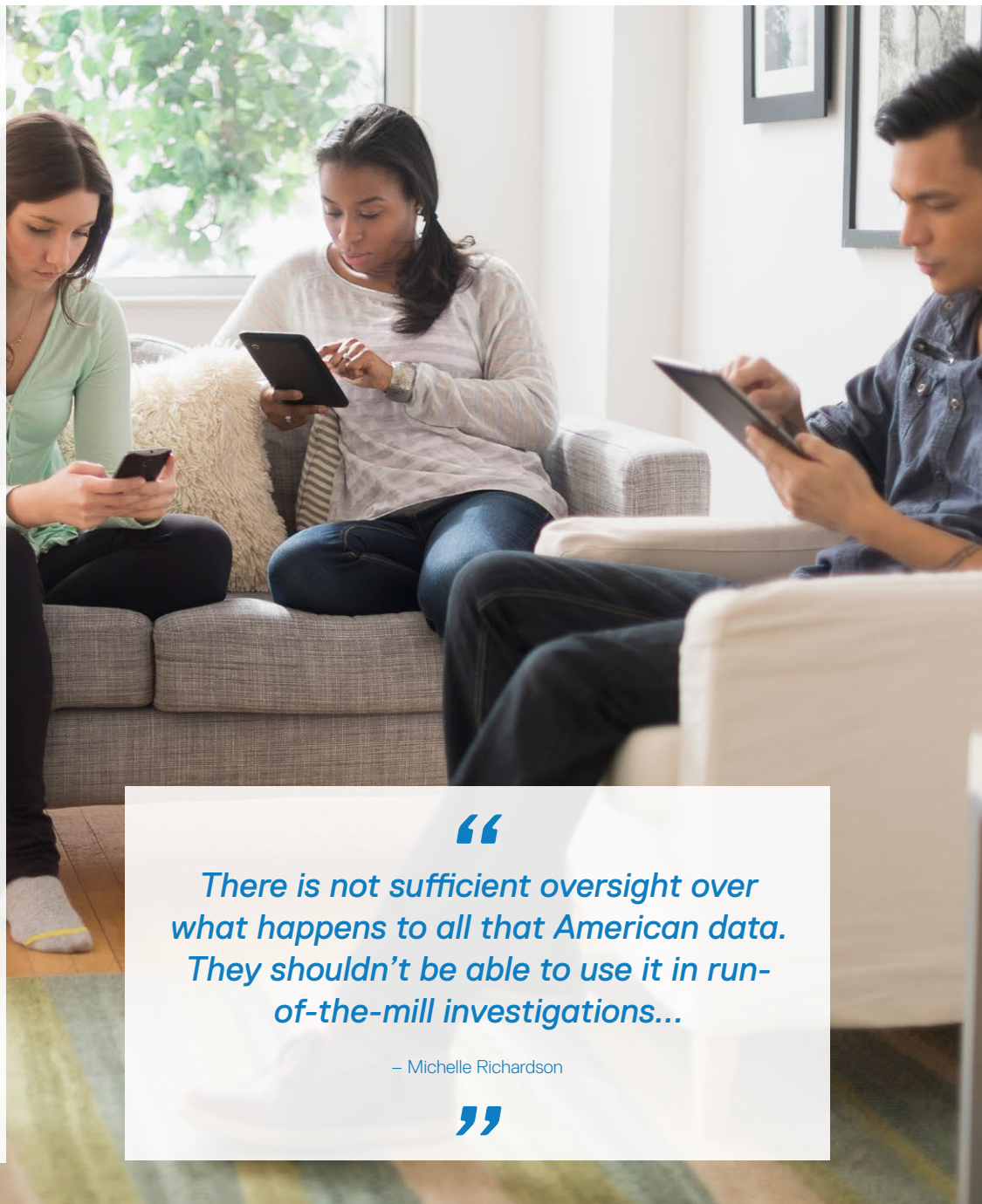
Many Americans won’t encounter Section 702. But if you do, chances

are, you'll never find out. That foreign private equity investor who calls you from Istanbul or Tirana or Paris and wants to talk about your revolutionary business plan – if he's on a target list, your communications with him may come up on some government screen. That possibility, however slim, has to worry people in international business, especially those who buy or sell goods and services in the classified world.

“They describe all the Americans who are on the other end of those phone calls or emails as incidental collection,” Richardson says. “Once you're in the database, the FBI can search through it for evidence of crimes. It's very possible they're doing an end-run around traditional criminal justice procedures that have clear statutory requirements and are designed to actually protect people who are being prosecuted. There is not sufficient oversight over what happens to all that American data. They shouldn't be able to use it in run-of-the-mill investigations, and that's what they're doing.”

Government officials deny this charge. They say they have neither the desire nor resources to spy on hundreds of thousands of Americans.

So, if you have something really important to hide, you may want to just say it in person. In a park. To someone you know isn't wearing a wire. Not that you could tell – that technology has gotten powerful and tinier too.



“  
*There is not sufficient oversight over what happens to all that American data. They shouldn't be able to use it in run-of-the-mill investigations...*  
”

– Michelle Richardson



# Security vs. Privacy: Do Other Nations Have It Figured Out?

By Kait Lavinder



Source: Flickr/Argonne National Laboratory

Edward Snowden's revelations in 2013 about the National Security Agency's surveillance programs thrust the age-old privacy versus national security debate into the spotlight. And while it certainly pushed the debate into the mainstream, to some experts, it was a false dichotomy.

Former Homeland Security Secretary Michael Chertoff explains, "You can't really have privacy if you don't have security, because then the promise of privacy is an empty promise. On the other hand, if you don't have privacy as a value, what are you securing? Because ultimately we're securing our values."

How do we create a world that is "not locked down so much we have no liberty, and not so open that anyone can come in?" asked NSA Research Director Deborah Frincke at the recent Cipher Brief Threat Conference in Sea Island, Georgia.

It depends both on the relationship between the people and their government, and on external circumstances. Adam Segal, Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, calls it the "pendulum." The idea is this: Events like terrorist attacks and current relations between the governed and governing will swing the pendulum to one side or the other.

"That's the process of governing," says General Michael Hayden, Cipher Brief expert and former Director of the CIA and NSA.

In the United States, legal revisions following the 9/11 terrorist attacks – including the PATRIOT Act, which broadens the collection of data, and Section 702 of the Foreign Intelligence Surveillance Act (FISA), which allows for incidental collection of Americans' data when the target of data collection is a foreigner outside the U.S. – swung the

“

*You can't really have privacy if you don't have security, because then the promise of privacy is an empty promise. On the other hand, if you don't have privacy as a value, what are you securing?*

– Michael Chertoff

”

pendulum to the side of greater data collection for national security purposes.

“The pendulum started to swing back after the Snowden revelations,” says Segal, adding, “So then with the USA Freedom Act, we had greater constraints placed on how long the government holds that data, for how many hubs they can collect it from, and some other kinds of reforms about how that data is collected and who has access to it.”

This side of the so-called process – the pendulum swing – occurs when there is pushback from civil society. But what happens in non-liberal democracies or authoritarian regimes, where civil society is not strong enough or taken seriously enough to propel a change in the law?

In countries like Russia, China, and Iran, the approach to cyberspace – along with the whole privacy versus national security debate – is fundamentally different than in Western liberal democracies, national security practitioners told The Cipher Brief.

“The Chinese government puts a very high priority on stability, and that shows up in a whole bunch of different ways, including how they approach cyberspace. ... they want to exert more control there than we in the West want. Same thing with Russia,” says Michael Daniel, Cybersecurity Coordinator at the White House under President Barack Obama.

Daniel, who is now President of the Cyber Threat Alliance, adds that cyberspace is “an area in which states will pursue their interests, and we will have cooperation and, frankly, conflict.”

That doesn’t necessarily mean liberal democracies and authoritarian regimes cannot find common ground on access to data. For example, notes Daniel, in the fall of 2015, the U.S. worked out an arrangement with China in which “the Chinese agreed to limit the theft of

intellectual property through cyber means for economic benefit.”

Still, there will “always be some limitation on the ability to reach an agreement on access to information when you’re dealing with a country that has a radically different system,” says Chertoff.

“For example,” he continues, “if a foreign country wants to get information in order to prosecute people who articulate ideas that they don’t like, probably the U.S. would not agree to that kind of an arrangement because it would violate our constitution.”

At the same time, he says, there may be other areas, like with credit card fraud, “where there would be a willingness to have a stream-lined way of exchanging information.”

Ultimately, though, the international framework for data collection and regulation “needs to be determined by countries that have a clear dedication to the rule [of law], to open societies, to freedom of speech, and all of those things which are the hallmarks of liberal democracies,” says Steven Hall, a former member of the CIA’s Senior Intelligence Service.



Source: Getty Images/Win McNamee





Source: AP Images/Alexei Druzhinin

Hall, a Russia expert, says the goal of data collection activities in Russia is to “have access to all information about all Russian citizens inside of Russia.” This goes back to the tsarist times, he says, “when you’ve got to be able to monitor internal dissent, you’ve got to be able to crush it with your secret services, with your intelligence services as quickly as possible.”

Therefore, the Russians create laws for things like data localization, in which any company that wants to hold information on a Russian citizen must have the server holding that data located inside of Russia’s border. LinkedIn, for example, declined to do this and has been shut out of the Russian market.

The Russians will use a “western approach,” says Hall, in which they will point to western data collection practices and say this is why we have to have data localization, but “that’s all just a façade.”

Director of National Intelligence under President Obama, James Clapper, agrees, telling The Cipher Brief, “Countries like Russia and China have different motives, different concerns. Theirs have more to do with internal control over what

is available to their citizens, rather than ... what we collect.”

At the same time, there are a number of concerns that could support the need for data localization laws. One is that these laws can be “a device to promote... local companies, in terms of hosting data,” notes Chertoff. If Google, for example, wants to hold information on Chinese citizens and China has strict data localization laws, then a local Chinese company, instead of Google, which is headquartered in the U.S., will have to host that data, “promoting” that local company by giving it business. Another concern is that in the digital age, crimes can be committed remotely, and therefore, “local law enforcement and others are frustrated that they can’t get the kind of data they want to deal with criminal activity,” Daniel points out.

Segal explains that if you’re a Brazilian magistrate judge and two Brazilians commit a crime that they plotted on Facebook, “if you want access to that data, Facebook won’t give it to the [Brazilian] government directly, you have to go ... to the [U.S.] Department of Justice, and that process can take up to 10 months.”

The problem is that “if you take localization to its extreme, you wind up with a fragmented internet ... It becomes the local web. And that has much less value to everybody,” says Chertoff.

So, proposes Daniel, maybe we should be thinking about a different kind of regime for data that doesn’t “rely on where the ones and

zeroes happen to reside in a given moment in time,” but that deals more with “issues of data ownership... Maybe even pursuing – on a broader scale – some of the agreements that we were trying to reach with the United Kingdom... where we would grant certain countries that met certain criteria [the ability] to query U.S. information

***Countries like Russia and China have different motives, different concerns. Theirs have more to do with internal control over what is available to their citizens...***

– James Clapper

information technology companies and internet service providers directly about their national.”

The UK-U.S. bilateral agreement on data access is still in the works. UK Deputy National Security Advisor Paddy McGuinness wrote in a statement that the UK government “hopes that Congress can pass relevant legislation as a priority in 2017.”

There is currently a push “from a public policy standpoint to see if we can reach some global uniform understanding about how you get lawful access to data, what rules apply to data, and how to avoid situations where a company that handles data globally is subjected to inconsistent legal obligations,” says Chertoff, adding that liberal democracies are behind trying to maintain a global sense of stability in the cyber world.

The European Union (EU) and the U.S., for example, developed the EU-U.S. Privacy Shield Framework in 2016, which replaces the EU-U.S. Safe Harbor Framework and provides a scheme for U.S. companies to comply with EU data protection requirements when transferring personal data from the EU to the United States.

The EU has stringent privacy laws. “It’s a big deal in Europe,” says Clapper, adding that there were “all kinds of challenges there post-Snowden in dealing with European privacy concerns.”

The UK, however, recently implemented the Investigatory Powers Act – dubbed the “Snooper’s Charter” by privacy advocates – which is far more intrusive than surveillance regimes in neighboring European countries and in the United States.

But, Chertoff says, “Even in some countries that may have a different political philosophy [there’s] value in recognizing that they benefit economically as well by having a true world wide web, and not having fragmented networks.”



Source: Getty Images/Vertigo3d



# Conclusion

*As the U.S. government grapples with legal and philosophical questions surrounding privacy and national security, technological leaps in AI, machine learning, and big data analytics demand answers — and soon.*

*The courts likely will be the ultimate arbiter of these vexing issues, although the sheer volume of information available at lightning speed may prevent either side of the argument from ever feeling satisfied. Still, experts and IC professionals agree, the immense possibilities that come from leveraging these tools must be weighed against the rights of citizens.*

*One test will come this fall, when Congress decides whether to reauthorize provision 702 of the Foreign Intelligence Surveillance Act without a sunset. That provision enables the intelligence community and law enforcement to use their digital tools to target, without a warrant, the communications of foreigners reasonably believed to be overseas, even though some of those communications may be with U.S. citizens or U.S. persons. Privacy advocates believe the language of 702 is too broad, and they will fight to persuade Congress to amend it.*

*As General Michael Hayden, former NSA and CIA director says, “We’d like to have total privacy and total security. We’re not going to get either. We’re going to have to balance.”*

*Privacy advocates want more sunlight on the process of collecting, storing, and analyzing information about Americans. They say the intelligence community shouldn’t be trusted to make such decisions unilaterally, excluding Congress and the courts.*

*“There is not sufficient oversight over what happens to all that American data” collected without a warrant, says Michelle Richardson of the Center for Democracy & Technology. The intelligence community and the FBI “shouldn’t be able to use it in run-of-the mill investigations, and that’s what they’re doing.”*

*In a democracy where liberty and values are paramount, enshrined in the very idea of being an American, striking that balance may not happen before the next technical innovation changes the game entirely.*

# Public and Private Sector Experts



**General Michael Hayden**

Former Director,  
CIA and NSA,  
The Cipher Brief Expert



**Rhea Siers**

Former Deputy Associate Director for  
Policy,  
National Security Agency,  
The Cipher Brief Expert



**Michael Lumpkin**

Former Special Envoy and Coordinator,  
The State Department's Global  
Engagement Center



**James Clapper**

Former U.S. Director of National Intelligence,  
The Cipher Brief Expert



**James Lewis**

Senior Vice President and Program Director,  
CSIS,  
The Cipher Brief Expert



**Rachel Levinson-Waldman**

Senior Counsel,  
The Liberty and National Security Program,  
The Brennan Center for Justice,  
NYU Law School



**Michael Chertoff**

Former Secretary of Homeland Security,  
The Cipher Brief Expert



**Rob Joyce**

Cybersecurity Coordinator,  
National Security Council



**Michelle Richardson**

Deputy Director,  
Freedom, Security, and Technology Project,  
Center for Democracy & Technology



**Doug Wise**

Former Deputy Director,  
Defense Intelligence Agency,  
The Cipher Brief Expert



**Jason Matheny**

Director,  
Intelligence Advanced Research Projects  
Activity (IARPA)



**Deborah Frincke**

Research Director,  
NSA



**Robert Eatinger**

Former Senior Deputy General Counsel,  
CIA,  
The Cipher Brief Expert



**Mark Testoni**

President and Chief Executive,  
SAP NS2



**Adam Segal**

Director,  
The Digital and Cyberspace Policy Program,  
The Council on Foreign Relations



**Elaine Lammert**

Former Deputy General Counsel,  
FBI,  
The Cipher Brief Expert



**Steve Jameson**

Insight Program Manager,  
Defense Advanced Research Projects  
Activity (DAPRA)



**Michael Daniel**

Former Cybersecurity Coordinator,  
National Security Council



**Steven Hall**

Former Member,  
Senior Intelligence Service,  
Central Intelligence Agency,  
The Cipher Brief Expert



**Elizabeth Goitein**

Co-Director,  
The Liberty and National Security Program,  
The Brennan Center for Justice,  
NYU Law School

Report Underwritten by:

**NS2** <sup>TM</sup>



NATIONAL SECURITY SERVICES