CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

STRATEGIC TECHNOLOGIES PROGRAM

December 2014

Underestimating Risk in the Surveillance Debate

James Andrew Lewis

Executive Summary

Americans are reluctant to accept terrorism is part of their daily lives, but attacks have been planned or attempted against American targets (usually airliners or urban areas) almost every year since 9/11. Europe faces even greater risk, given the thousands of European Union citizens who will return hardened and radicalized from fighting in Syria and Iraq.

The threat of attack is easy to exaggerate, but that does not mean it is nonexistent. Australia's then-attorney general said in August 2013 that communications surveillance had stopped four "mass casualty events" since 2008. The constant planning and preparation for attack by terrorist groups is not apparent to the public. The dilemma in assessing risk is that it is discontinuous. There can be long periods with no noticeable activity, only to have the apparent calm explode.

The debate over how to reform communications surveillance has discounted this risk. Communications surveillance is an essential law enforcement and intelligence tool. There is no replacement for it. Some suggestions for alternative approaches to surveillance, such as the idea that the National Security Agency (NSA) only track known or suspected terrorists, reflect wishful thinking, as it is the unknown terrorist who will inflict the greatest harm.

The Evolution of Privacy

Some of the unhappiness created by the Edward Snowden leaks reflects the unspoken recognition that online privacy has changed irrevocably. The precipitous decline in privacy since the Internet was commercialized is the elephant in the room we ignore in the surveillance debate. America's privacy laws are both limited in scope and out of date. Although a majority of Americans believe privacy laws are inadequate, the surveillance debate has not led to a useful discussion of privacy in the context of changed technologies and consumer preferences.

Technology is more intrusive as companies pursue revenue growth by harvesting user data. Tracking online behavior is a preferred business model. On average, there are 16 hidden tracking programs on every website. The growing market for "big data" to predict consumer behavior and target advertising will further change privacy.

Judging by their behavior, Internet users are willing to exchange private data for online services. A survey in a major European country found a majority of Internet users disapproved of Google out of privacy concerns, but more than 80 percent used Google as their search engine. The disconnect between consumer statements and behavior reduces the chances of legislating better protections.

We have global rules for finance and air travel, and it is time to create rules for privacy, but governments alone cannot set these rules, nor can a single region impose them. Rules also need to be reciprocal. NSA bears the brunt of criticism, but its actions are far from unique. All nations conduct some kind of communications

surveillance on their own populations, and many collect against foreign targets.

Getting this consensus will be difficult. There is no international consensus on privacy and data protection. EU efforts to legislate for the entire world ignore broad cultural differences in attitudes toward privacy, and previous EU privacy rules likely harmed European companies' ability to innovate. Finding a balance between privacy, security, and innovation will not be easy since unconstrained collection creates serious concerns while a too-restrictive approach threatens real economic harm.

Espionage and Counterterrorism

NSA carried out two kinds of signals intelligence programs: bulk surveillance to support counterterrorism and collection to support U.S. national security interests. The debate over surveillance unhelpfully conflated the two programs. Domestic bulk collection for counterterrorism is politically problematic, but assertions that a collection program is useless because it has not by itself prevented an attack reflect unfamiliarity with intelligence. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success. Success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture.

In practice, analysts must simultaneously explore many possible scenarios. A collection program contributes by not only what it reveals, but also what it lets us reject as false. The Patriot Act Section 215 domestic bulk telephony metadata program provided information that allowed analysts to rule out some scenarios and suspects.

The consensus view from interviews with current and former intelligence officials is that while metadata collection is useful, it is the least useful of the collection programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215, but this would not come without an increase in risk. Restricting metadata collection will make it harder to identify attacks and increase the time it takes to do this.

Spying on Allies

NSA's mass surveillance programs for counterterrorism were carried out in cooperation with more than 30 countries. Unilateral U.S. collection programs focused on national security problems: nonproliferation, counterintelligence (including Russian covert influence operations in Europe), and arms sales to China. The United States failed to exercise sufficient oversight over intelligence collection, but the objectives set for NSA reflect real security problems for the United States and its allies.

The notion that "friends don't spy on friends" is naive. The United States has friends that routinely spy on it and yet are strong security partners. Relations among powerful states are complex and not explained by simple bromides drawn from personal life.

The most startling thing about U.S. espionage against Germany was the absence of a strategic calculation of risk and benefit. There are grounds for espionage (what other major power has a former leader on Russia's payroll?), but the benefits were outweighed by the risk to the relationship. The case for spying on Brazil is even weaker. While Brazil is often antagonistic, it poses no risk to national security. If economic intelligence on Brazil is needed, the private sector has powerful incentives and legitimate means to obtain information and usually has the best data.

Risk Is Not Going Away

Broad surveillance of communications is the least intrusive and most effective method for discovering terrorist and espionage activity. Many countries have expanded surveillance programs since the 9/11 attacks to detect and prevent terrorist activity, often in cooperation with other countries, including the United States.

Precise metrics on risk and effectiveness do not exist for surveillance, and we are left with conflicting opinions from intelligence officials and civil libertarians as to what makes counterterrorism successful. Given resurgent authoritarianism and continuing jihad, the new context for the surveillance debate is that the likelihood of attack is increasing. Any legislative change should be viewed through this lens.

New Requirements for Surveillance: Better Congressional Oversight, More Transparency

No president will take the risk of ending surveillance programs, but continuing them without increasing oversight and transparency will erode public confidence and trust. Surveillance programs create serious and legitimate concerns about oversight and constitutionality that must be addressed by the Congress.

Congress needs to modify the 1970s intelligence oversight process to provide greater accountability on the size, scope, and accuracy of domestic collection programs, and increase transparency for FISA (Foreign Intelligence Surveillance Act) decisions. Much of what is secret could be made public in summary form without harm to national security. The United Kingdom, for example, publishes an annual report on surveillance programs that at a minimum makes the public aware of these activities and their scope. Our goal should be to increase accountability without an unacceptable increase in risk. Some proposed measures would do the exact opposite. Adding a permanent advocate to the FISA Court, for example, could return the United States to pre-9/11 gridlock for counterterrorism.

The United States should reconsider foreign espionage activities in light of political risk and availability of other sources of information. We have not adjusted intelligence collection to the information age, where the availability of intelligence reduces the need for collection. Collection against some foreign targets can be eliminated without harm, given the availability of commercial information sources. The United States should also act to protect American companies against retaliatory trade practices, where countries use surveillance as an excuse to promote their own industries.

Almost all countries approach communications interception as an untrammeled privilege of the sovereign that requires little oversight or consent by citizens. This needs to change, not just in the United States. A good outcome would be to create an initiative to develop international norms for responsible state behavior in cyberspace that constrains surveillance by all actors and protects both personal data and intellectual property.

Underestimating Risk in the Surveillance Debate

James Andrew Lewis

The echoes of September 11 have faded and the fear of attack has diminished. We are reluctant to accept terrorism as a facet of our daily lives, but major attacks—roughly one a year in the last five years—are regularly planned against U.S. targets, particularly passenger aircraft and cities. America's failures in the Middle East have spawned new, aggressive terrorist groups. These groups include radicalized recruits from the West—one estimate puts the number at over 3,000—who will return home embittered and hardened by combat. Particularly in Europe, the next few years will see an influx of jihadis joining the existing population of homegrown radicals, but the United States itself remains a target.

America's size and population make it is easy to disappear into the seams of this sprawling society. Government surveillance is, with one exception and contrary to cinematic fantasy, limited and disconnected. That exception is communications surveillance, which provides the best and perhaps the only national-level solution to find and prevent attacks against Americans and their allies. Some of the suggestions for alternative approaches to surveillance, such as the recommendation that NSA only track "known or suspected terrorists," reflect both deep ignorance and wishful thinking. It is the unknown terrorist who will inflict the greatest harm.

This administration could reasonably argue that everything it has done is legal and meets existing requirements for oversight, but this defense is universally perceived as legalistic hairsplitting. If the government can be faulted, it is for obsessive secrecy. The public debate over NSA's surveillance programs routinely exaggerates risks and errors,[1] but in the absence of a compelling official narrative, the space was filled with conjecture and distortion. This has not helped a crucial debate where a wrong answer could mean more bombings.

When the surveillance programs became public, there was uproar. To an extent, this uproar was a creature of the media and of deliberate intent by entities with a powerful anti-American agenda. But it also reflects public discomfort and reasonable concerns over secret programs. These concerns point to the need for change. No president will take the risk of ending surveillance programs, but continuing them without improved oversight and transparency will erode public confidence and trust. The existing approach to the authorization of intelligence programs and their oversight, created by Congress and the administration in the 1970s, needs to be updated and strengthened to take into account both new and very different threats in combination with the challenges and risks created by new communications technologies. The 40-year-old oversight structure, designed for a simpler era, is no longer adequate. There are clearly changes that need to be made in oversight, transparency, and restraint.

If oversight is inadequate for the new political environment in the United States, it is completely lacking in the rest of the world. Most nations still take the traditional view that espionage is the prerogative of the sovereign and tell their legislatures and public nothing of what is being done in the name of security. This is as true for democracies (the United Kingdom being a notable exception) as it is for authoritarian states. The long-established practices for the conduct of espionage by states need adjustment to fit the Internet age and its demands for greater knowledge and involvement. Most countries engage in some form of communications surveillance, and "surveillance" in the form of tracking online consumer behavior is the preferred business

[1] By risk we mean the probability of an attack or other damaging event. Risk is determined by a number of factors: hostile intent, opponent and defender capabilities, and external circumstances.

model for the Internet. The fundamental conclusion is that mass surveillance is already omnipresent and essential for effective counterterrorism, but the use of this powerful tool by both companies and governments needs greater oversight and transparency.

The Evolution of Privacy

Some of the unhappiness created by the Snowden leaks reflects the fear that privacy, at least online, is irrevocably lost. This is probably right. Privacy has evolved in ways we did not expect when the Internet entered into widespread use. The Internet has changed in ways that make privacy extraneous. In 1998, Scott McNealy, then the CEO of Sun Microsystems, said, "You have zero privacy anyway, get over it." At the time, his remark seemed intemperate, but however much privacy existed in 1998, only a fraction remains now. We live in a world of mass surveillance by both governments and private actors. All this has occurred under the gaze of a range of privacy groups who continue to espouse ideas about privacy that may no longer accurately reflect public attitudes and are likely outdated.

Old-style privacy has been designed out of the Internet. The "digital footprints" left by Internet activity are routinely tracked and stored by companies. Networks of increasingly cheap and capable sensors can generate and record voice, email, and video data for analysis by sophisticated algorithms. Communications in any form sent over a network can be intercepted and recorded. Privacy safeguards were always weak, lagging far behind the deployment of digital technologies, and some languages do not even have a word for privacy.

The business model of the public facing Internet depends upon harvesting user data. This was not always the case. In the 1990s, people put things on the web because it gave them satisfaction to share and to gain recognition. This "free" model for the Internet may not have been sustainable. It did not extract the full value of Internet transactions. The years since the Internet was commercialized have seen companies develop business models and technologies to identify value online and extract it. Every year, technology becomes more intrusive as companies seek to continue to show revenue growth. The steady progression of advertising and marketing functions from an ancillary activity to an unavoidable part of browsing is driven by the need to show the financial markets increasing revenues.

The Internet still seems to offer free services. In fact, users pay for services with their data, and many Internet business models rely on technologies that commoditize data collected from Internet users. Advertising is one way that users pay for "free" services. Companies refine business models to maximize the revenue stream from advertising (and data mining), only letting users access certain services if they log in (which links them to a data profile) or requiring that downloads come through a store that monopolizes purchases and data. "Real time bidding" is a commercial process where a user's visit to and actions on a website are instantly correlated with stored personal information about the visitor (age, income, race, behavior) and his or her browsing history. This customer is then offered to online advertisers who bid to place their ads on the webpage while the customer is still on it. The entire process is almost instantaneous, taking only milliseconds.[2]

The desire for better targeting of advertisements is only one reason to collect data on web users. The ability of computers to aggregate and analyze masses of data with statistical programs to understand and predict is one of their virtues. Statistical programs for manipulating large databases have existed for decades. Companies can create specialized algorithms to predict consumer behavior and link these predictions to specific individuals.

[2] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

The key to prediction is not only the algorithm but the availability of huge amounts of data—the more data there is, the more accurate the prediction. The recent White House review of "big data" expressed concern over the risks of aggregation but proposed no concrete actions to mitigate it.[3]

On average, there are 16 tracking programs on every website.[4] This means that when you visit a website, it collects and reports back to 16 companies on what you've looked at and what you have done. These programs are invisible to the user. They collect IP address, operating system and browser data, the name of the visiting computer, what you looked at, and how long you stayed. This data can be made even more valuable when it is matched with other data collections. Everything a consumer does online is tracked and collected.

There is a thriving and largely invisible market in aggregating data on individuals and then selling it for commercial purposes. Data brokers collect utility bills, addresses, education, arrest records (arrests, not just convictions). All of this data is recorded, stored, and made available for sale. Social networking sites sell user data in some anonymized form so that every tweet or social media entry can be used to calculate market trends and refine advertising strategies. What can be predicted from this social media data is amazing—unemployment trends, disease outbreaks, consumption patterns for different groups, consumer preferences, and political trends. It is often more accurate than polling because it reflects peoples' actual behavior rather than the answer they think an interviewer wants to hear. Ironically, while the ability of U.S. agencies to use this commercial data is greatly restricted by law and policy, the same restrictions do not apply to foreign governments.

The development of the Internet would have been very different and less dynamic if these business models had not been developed. They provide incentives and financial returns to develop or improve Internet services. There is an implicit bargain where you give up privacy in exchange for services, but in bargains between service providers and consumers, one side holds most of the cards and there is little transparency. But the data-driven models of the Internet mean that it is an illusion to think that there is privacy online or that NSA is the only entity harvesting personal data.

It is also likely that consumers are more comfortable with trading personal data for Internet services than the privacy debate would indicate. In practice, people routinely surrender data in exchange for a new app or service, and while it is legitimate to say many are not fully aware of the trades they are making, greater knowledge (and control) might not lead to radical changes in behavior.[5] This is a contentious issue, as changing attitudes toward privacy are both difficult to measure and challenge long-standing orthodoxies.

Some commentators hope that the United States can return to a simpler time when persons who wished to keep their information private did not have to disconnect entirely or live in a remote hut in Montana. Technological change has ended this era of de facto privacy and only a de jure approach can replace it. As more activities increasingly require some connection to the Internet (where they will be recorded and tracked) and as networked digital sensors become pervasive in our physical environment, simply amending the laws that govern the actions of U.S. agencies without affecting either private companies or foreign intelligence agencies will have little effect.

There is no international consensus on how to protect data. The European Union put forward regulatory

[3] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[4] Personal communication, Dan Geer, computer security analyst and risk management specialist.
[5] Mark Scott, "Principles Are No Match for Europe's Love of U.S. Web Titans," *New York Times*, July 6, 2014, http://www.nytimes.com/2014/07/07/technology/principles-are-no-match-for-europes-love-of-us-tech-titans-like-amazon-and-facebook.html.

frameworks in 1995 and again in 2012, but this effort to create a global approach to privacy has process problems (a regional body lacks the legitimacy to impose global rules) and the rules have been strangely applied—European Court of Justice decisions on Google smacks both of censorship and anti-Americanism. Consensus cannot be imposed by a body that does not represent the governed. Nor should we dismiss the possibility that heavy privacy regulation has had a damaging effect on Europe's tech sector. Despite repeated pledges and digital agendas that promise to make Europe a center of innovation, the IT industry has shifted west and is centered on the Pacific Rim. Too little privacy protection is worrisome; too much protection or protections badly implemented inflict real economic harm.

Finding the balance between privacy, security, and innovation will not be easy. Despite more than a decade of noisy debate over privacy, fundamental policy issues remain unresolved. Just as we have global rules for finance or air travel, it may be time to create global rules for privacy in cyberspace, but this process cannot depend only on governments as participants or be determined by a single region. As with other cyber issues, the international community lacks both the mechanisms and the experience to make rapid progress in developing an acceptable approach to privacy.

Espionage and Surveillance

Espionage, particularly domestic espionage, presents a difficult problem for policy because, unlike commercial activities, it involves a trade between privacy and public safety. Google may know my every online move but if I evade Google it does not mean bombs in Times Square (nor can Google arrest me). We can divide communications surveillance into three categories: direct battlefield support for deployed forces; "traditional" collection against political and military targets; and mass collection of domestic communications for counterterrorism purposes.[6] NSA's "cryptologic enterprise," which was publicly acknowledged in the 1990s, performs all three missions. The latter two raise unavoidable political issues, but there is a tendency to conflate them, as if the attention NSA pays to a world leader's mobile phone is applied to millions of consumers. This conflation reflects larger concerns over the decline of privacy in the digital environment, but it confuses two sets of issues: the role of domestic surveillance in effective counterterrorism and the need for political and military espionage against allies.

The relationship between Americans and espionage has always been uncomfortable. In times of great peril, leaders like Washington or Lincoln created secret intelligence services but these were temporary and disbanded at conflict's end. Otherwise, the Republic was happy to plod along, largely uninformed, and not needing much information given its isolation from great-power conflicts, its self-absorbed role in the world, and a world where geographic distance and primitive technologies combined to eliminate the risk of attack. This happy ignorance ended at 1:49 PM, Eastern Standard Time, on December 7, 1941, with Japan's surprise attack on the U.S. Pacific Fleet. Some would say that the ignorance should have ended earlier, but the period where America could stand apart from the world and not be drawn into its conflicts ended then and will not come back.

The United States was a latecomer to communications interception and surveillance. Its rudimentary signals intelligence capability expanded rapidly in World War I, working to break foreign encryption and read the telegraphs and mail of both foreign entities in the United States and American citizens suspected of being foreign agents. The Cipher Bureau created for World War I was closed in 1929 by Secretary of State Henry Stimson, who said, "Gentlemen do not read each other's mail," a stuffy sentiment repeated with much less

[6] Domestic includes both U.S. and European collections, programs done in partnership with European governments for public safety purposes.

honesty in Europe today.[7] European nations have been reading each other's mail, and that of their citizens, at least since the Treaty of Westphalia in 1648 and likely well before then.

Communications intercepts have been with the world since the start of electronic communication using the telegraph. Radio increased the role of signals intelligence—the radio entered widespread use by navies in 1912 and competitors realized that they could receive the signals the other side was sending. Within months, leading powers had created signals intercept capabilities. Before 1914, nations realized that others could hear what they were saying or determine their armies' or ships' location, and sought technological solutions, including encryption, in a race between security and intercept that continues to this day. "Metadata" analysis appeared well before that, as European powers developed techniques to identify clandestine groups using the information on the outside of envelopes sent through the mail.[8]

All nations engage in communications interception. Most programs have a domestic focus, but many countries also collect against foreign targets, to the extent of their resources and interests. Most countries approach communications interception as an untrammeled privilege of the sovereign that requires little oversight, knowledge, or consent by the citizens. This has not been part of the surveillance debate, which has sought to portray NSA's behavior as unique. Surveillance is universal and, in many countries, largely ungoverned and certainly not transparent to citizens. There will never be formal international agreement on espionage since no country will stop spying, but it is possible to address the problem indirectly. Agreements that protect individual and company data would constrain espionage, but the surveillance debate triggered by the Snowden revelation, perhaps because of its anti-American spin, has failed to consider how to develop global rules for data.

Domestic Mass Surveillance

Mass surveillance of domestic communication began soon after the September 11 attacks under a presidential authorization when it was widely believed that additional attacks were imminent. The intent of the program was to provide early warning of impending terrorist attacks in the United States. The 9/11 attacks showed that the legal and operational structure for domestic counterterrorism was inadequate for dealing with the new kind of threat posed by transnational groups. Both Congress and the White House have struggled since September 11 to adjust the law to fit technological and operations requirements of a new global environment for terrorism while preserving constitutional constraints on surveillance.

The Constitution provides the president with broad authority to undertake actions necessary for the security of the nation, consistent with other constitutional strictures on executive authorities and with the Bill of Rights, which protect against unreasonable search and seizure. This is not a blanket prohibition against search or against the interception of communications. The key word is reasonable. The Constitution makes clear that it is the courts, the Congress, and the executive branch that decides what is reasonable, which requires processes to assess risk to both public safety and civil liberties, and to mitigate it.

The United States conducts surveillance under a patchwork of legal authorities and protections. The first domestic surveillance program, called the "President's Surveillance Program," was of dubious legality. Senior intelligence officials responsible for the program said they were reluctant to seek legislation in 2002, when Congress would have likely granted broad authorities, because they feared this would warn opponents of the

[7] NSA, "Pearl Harbor Review—The Black Chamber," March 2012, http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/pearl_harbor_review/black_chamber.shtml.
[8] This and other surveillance innovations were developed by European counterintelligence services in the nineteenth century (chief among them the Austro-Hungarian Empire's Geheime Kabinettskanzlei, or secret chancellery).

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

nature and scope of surveillance and lead them to modify their behavior to evade collection.

After the program was revealed by the *New York Times* in 2005 (apparently as a result of leaks by U.S. officials uncomfortable with the program), it was put on sounder legal footing in January 2007 using the Patriot Act, which provided a broad range of new authorities, including an expansion of wiretapping and surveillance authorities. The two most important laws for surveillance are the Foreign Intelligence Surveillance Act (FISA) and the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act. Neither law is fully adequate for conducting surveillance on a dense cloud of message traffic that blends domestic and foreign.

The United States conducted mass surveillance under Section 215 of the Patriot Act using a provision that requires a FISA Court order for the government to obtain business records for intelligence and counterterrorism purposes. The FISA Court issues two orders when it approves collection under this statute. One court order directs phone companies to provide the metadata to the government. An accompanying court order limits how the government can use the data. For some reason, while an example of the order to service providers to provide data was leaked in the press, the second order limiting how it can be used was not made public.[9]

The most controversial aspect of the surveillance program involved metadata. Metadata is information describing a telephone call, such as the number from which the call was placed, the number called, and the date, time, and length of the call. The content of the phone call (e.g., the conversation) is not collected. No locational data is collected, although commentators seem confused on this point. Metadata analysis gave NSA the ability to identify individuals in the United States or individuals outside the United States who are in contact with terrorist groups.[10] In 2012, NSA looked at 288 primary telephone numbers and through "call chaining" analysis reviewed 6,000 other numbers connected to these primary numbers. The 288 people had some connection to terrorism and NSA looked at the 6,000 people with whom they talked to see if they were also involved.

Metadata acquired and retained under Section 215 of the Patriot Act program could only be queried when there is "reasonable articulable suspicion" that a telephone number is associated with foreign terrorist organizations. If a query merits further investigation, which requires looking at either content of the individual unmaking the call, this requires a specific, individual court order based on probable cause. If there is one constitutional requirement that was not fully observed in the metadata program authorized under the Patriot Act, it was that search requires a warrant from a court rather than an internal approval by the executive branch agency itself.[11] This was a significant error.

The 215 program allows law enforcement and intelligence officials to determine if a terrorist event is an isolated incident or the first of a serious of attacks, and whether the attacker is a "lone wolf" or connected to a larger terrorist organization. The most important decision in the immediate aftermath of an attack is whether the incident is the first of a series. If it is the first of a series of attacks, additional steps must be taken without delay, such as closing airports and other transportation hubs, putting police forces around the country on high alert, and mobilizing law enforcement agencies to locate and arrest the other attackers. These steps are both disruptive and expensive and knowing that they are not necessary provides immediate benefit.

The 2009 Fort Hood shootings are an example of this kind of inquiry, where counterterrorism officials could

[9] Statement by Robert Litt, general counsel of the director of national intelligence.
[10] "NSA inspector general report on email and Internet data collection under Stellar Wind—full document," *The Guardian*, June 27, 2013, http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.
[11] A similar criticism could be made of the approval process for National Security Letters.

query metadata and rapidly determined that the shooting was an isolated incident and the shooter a deranged and radicalized individual rather than a member of a group. While this would not count as "stopping an attack," it did let officials plan a rapid response to the incident.

Assertions that a collection program contributes nothing because it has not singlehandedly prevented an attack reflect an ill-informed understanding of how the United States conducts collection and analysis to prevent harmful acts against itself and its allies. Intelligence does not work as it is portrayed in films—solitary agents do not make startling discoveries that lead to dramatic, last-minute success (nor is technology consistently infallible). Intelligence is a team sport. Perfect knowledge does not exist and success is the product of the efforts of teams of dedicated individuals from many agencies, using many tools and techniques, working together to assemble fragments of data from many sources into a coherent picture. Analysts assemble this mosaic from many different sources and based on experience and intuition. Luck is still more important than anyone would like and the alternative to luck is acquiring more information. This ability to blend different sources of intelligence has improved U.S. intelligence capabilities and gives us an advantage over some opponents.

Portrayals of spying in popular culture focus on a central narrative, essential for storytelling but deeply misleading. In practice, there can be many possible narratives that analysts must explore simultaneously. An analyst might decide, for example, to see if there is additional confirming information that points to which explanation deserves further investigation. Often, the contribution from collection programs comes not from what they tell us, but what they let us reject as false. In the case of the 215 program, its utility was in being able to provide information that allowed analysts to rule out some theories and suspects. This allows analysts to focus on other, more likely, scenarios.

In one instance, an attack is detected and stopped before it could be executed. U.S. forces operating in Iraq discover a bomb-making factory. Biometric data found in this factory is correlated with data from other bombings to provide partial identification for several individuals who may be bomb-makers, none of whom are present in Iraq. In looking for these individuals, the United States receives information from another intelligence service that one of the bombers might be living in a neighboring Middle Eastern country. Using communications intercepts, the United States determines that the individual is working on a powerful new weapon. The United States is able to combine the communications intercept from the known bomb maker with information from other sources—battlefield data, information obtained by U.S. agents, collateral information from other nations' intelligence services—and use this to identify others in the bomber's network, understand the plans for bombing, and identify the bomber's target, a major city in the United States.

This effort takes place over months and involves multiple intelligence, law enforcement, and military agencies, with more than a dozen individuals from these agencies collaborating to build up a picture of the bomb-maker and his planned attack. When the bomb-maker leaves the Middle East to carry out his attack, he is prevented from entering the United States. An analogy for how this works would be to take a 1,000-piece jigsaw puzzle, randomly select 200 pieces, and provide them to a team of analysts who, using incomplete data, must guess what the entire picture looks like. The likelihood of their success is determined by how much information they receive, how much time they have, and by experience and luck. Their guess can be tested by using a range of collection programs, including communications surveillance programs like the 215 metadata program.

What is left out of this picture (and from most fictional portrayals of intelligence analysis) is the number of false leads the analysts must pursue, the number of dead ends they must walk down, and the tools they use to decide that something is a false lead or dead end. Police officers are familiar with how many leads in an investigation must be eliminated through legwork and query before an accurate picture emerges. Most leads are wrong, and much of the work is a process of elimination that eventually focuses in on the most probable threat. If real

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

intelligence work were a film, it would be mostly boring. Where the metadata program contributes is in eliminating possible leads and suspects.

This makes the critique of the 215 program like a critique of airbags in a car—you own a car for years, the airbags never deploy, so therefore they are useless and can be removed. The weakness in this argument is that discarding airbags would increase risk. How much risk would increase and whether other considerations outweigh this increased risk are fundamental problems for assessing surveillance programs. With the Section 215 program, Americans gave up a portion of their privacy in exchange for decreased risk. Eliminating 215 collection is like subtracting a few of the random pieces of the jigsaw puzzle. It decreases the chances that the analysts will be able to deduce what is actually going on and may increase the time it takes to do this. That means there is an increase in the risk of a successful attack. How much of an increase in risk is difficult to determine, but this is crucial for assessing the value of domestic surveillance programs.

If the risk of attack is increasing, it is not the right time to change the measures the United States has put in place to deter another 9/11. If risk is decreasing, surveillance programs can be safely reduced or eliminated. A more complicated analysis would ask if the United States went too far after 9/11 and the measures it put in place can be reduced to a reasonable level without increasing risk. Unfortunately, precise metrics on risk and effectiveness do not exist,[12] and we are left with the conflicting opinions of intelligence officials and civil libertarians as to what makes effective intelligence or counterterrorism programs. There are biases on both sides, with intelligence officials usually preferring more information to less and civil libertarians can be prone to wishful thinking about terrorism and opponent intentions.[13]

Interviews with current and former intelligence officials give us some guidance in deciding this. The consensus among these individuals is that 215 is useful in preventing attacks, but the least useful of the programs available to the intelligence community. If there was one surveillance program they had to give up, it would be 215 before any others, but ending 215 would not come without some increase in risk.

Foreign Surveillance and Espionage

Domestic collection raises difficult constitutional issues. Foreign collection raises diplomatic issues, since espionage is a normal practice among states. NSA carried out two kinds of signals intelligence programs: mass surveillance to support the counterterrorism efforts of allies, particularly in Europe (with the participation of European governments, even if their publics were unaware of this cooperation); and targeted collection to support national security interests to the United States.[14] This foreign intelligence activity was conducted under Section 702 of FISA and amendments, which provides NSA the authority to collect foreign communications.

Mass surveillance serves counterterrorism purposes. It provides a means of identifying terrorists and their networks for targeted collection. The mass collection programs conducted by NSA were done in cooperative arrangements with European security services and those of other nations; that this was largely unknown to European populations and legislatures is more a reflection of the weaknesses of the oversight of their own

[12] Raphael Perl, "Combating Terrorism: The Challenge of Measuring Effectiveness," Congressional Research Service, November 23, 2005, http://fpc.state.gov/documents/organization/57513.pdf.
[13] The final panel of a June 2014 conference provides an excellent example of this. See "Ethos and Profession of Intelligence," Georgetown University, Washington, DC, June 12, 2014, http://www.georgetown.edu/news/cia-conference-2014.html.
[14] Office of the Director of National Intelligence, "Response to Question from the 5 June 2014 Hearing," June 27, 2014.

intelligence activities by Europeans.[15]

The United States had unique advantages for counterterrorism on a global level. These include its relationships with a range of foreign intelligence partners, its technical resources, and the information it obtained from its operations in Iraq and Afghanistan. A captured cell phone can provide names and numbers that allow for more precise targeting. Using sophisticated software and combined with information from other intelligence services, NSA was able to take the billions of calls and emails sent each day and winnow them down to a few thousand messages to which an intelligence analyst actually listened.

The nature of mass surveillance has been misrepresented, although this point is politically irrelevant. The chief error lies in the difference between collecting and exploitation. Millions of records were collected, very few were exploited. Sophisticated software programs sort through the records to find conversations linked to terrorism, or in some cases, to proliferation or espionage. Most conversations are boring. NSA devoted almost two decades to develop technologies that would let it sort automatically through millions of records to find those few conversations or messages of interest. The actual number of messages is staggering. One report estimates that there were more than 100 trillion messages on the Internet in 2010—more than 30 billion every day (if we discount "spam"). There are more than 3 billion email accounts globally.[16] There are more than 6 billion mobile phone users.[17] The idea that NSA and its partner services in Europe and Asia listened to each message or phone is ludicrous, even if firmly embedded in the public consciousness.

We do not know the full scope of success for these programs. The traditional explanation is that the failures of intelligence services will be on every front page but their successes will never be known. We do know that ending NSA's role in mass surveillance will not end mass surveillance in Europe or other parts of the world. What it will do is reduce cooperation among allied and friendly services and the United States and restrict access to extraregional counterterrorism data. Cooperation will not end, but will be less effective at a time when jihadi fighters are beginning to return from Syria. There will be an increase in the risk that a plot will go undetected, but how much risk will increase is difficult to estimate.

While the mass surveillance programs supported counterterrorism and were done in cooperation with European services, other NSA intelligence collection programs were focused on nonproliferation, counterintelligence (including Russian covert influence efforts), and arms sales to China. Unfortunately, Europe's record on these matters is open to question. Espionage does not occur in a vacuum but in a larger political and military context. U.S. leaders may have failed to exercise sufficient oversight over intelligence collection, but the objectives set for NSA reflect real problems.

One central issue is whether the notion that "friends don't spy on friends" makes any sense. Germany might actually follow the rule that friends do not spy on friends, but that would make it practically unique in the world. A recent internal review by the United States ranked France, for example, as the fourth-most-active nation engaged in economic espionage against it (the others were, in order, China, Russia, and another ally). In the mid-1990s, the director of central intelligence traveled to Paris to warn that French espionage was reaching

[15] Ryan Gallagher, "How Secret Partners Expand NSA's Surveillance Dragnet," The Intercept, June 18, 2014, https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.
[16] Pingdom, "Internet 2010 in Numbers," January 12, 2011, http://royal.pingdom.com/2011/01/12/Internet-2010-in-numbers/.
[17] MobiForge, "M-commerce insights: Mobile users and context," http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#uniquesubscribers.

intolerable levels.[18] There are other less public anecdotes that go back decades and make it clear that friends do indeed spy on friends. This does not mean that France (or the other ally) was not a friend. There is strong and essential cooperation with France on key security issues. It is a valued partner for the United States. What it means is that relations among powerful states are complex and not explained by simple-minded bromides drawn from personal life.

Espionage is not the best way to engage with Germany on the ambivalent attitude of many of its citizens toward the United States or *nostalgie de la boue* [nostalgia] when it comes to Soviet Russia,[19] but it is difficult to think of another former leader of a major power who is on Vladimir Putin's payroll. German military sales to China could justify U.S. espionage. Germany is not alone among European nations in making such sales, but sales such as the transfer of quiet diesel submarine engines from a German firm to China is troubling. France and

[18] R. James Woolsey, "Why We Spy on Our Allies," *Wall Street Journal*, March 17, 2000, http://online.wsj.com/news/articles/SB95326824311657269?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB95326824311657269.html.
[19] Christiane Hoffmann and René Pfister, "Part of the West? 'German Leftists Have Still Not Understood Putin,'" Spiegel Online, June 27, 2014, http://www.spiegel.de/international/germany/interview-with-historian-heinrich-winkler-about-germany-and-the-west-a-977649.html.

other European nations have also contributed advanced technology to Chinese military programs. Europe reluctantly maintains an embargo on arms sales to China because of the Tiananmen massacre; but the way around the embargo is to reclassify items as commercial, not military. Hence these are "commercial submarine engines."

The most startling thing about espionage against Germany is the complete absence of any strategic calculation by the United States about the risks and benefits. Germany's status and position in Europe and the world has changed. Germany is no longer a junior partner. The United States needs a closer partnership with Germany to achieve its foreign policy goals. Building this partnership will not be easy—German foreign policy is inadequate in ways that Germans may not appreciate—which is not surprising, since the Wilhelmine, Weimar, and "Post-Weimar" precedents are unfortunate, and German policy could focus on commercial issues when Germany was part of a larger alliance led by the United States. Sending troops to support NATO in Afghanistan but tightly limiting their ability to fight, for example, suggests Germany has the means and the form of power, but has not yet defined how to use it.

Both the United States and Germany would find it easier to achieve their foreign policy goals if they work together, but this will require them to redefine their partnership. Germany's traditional policy of letting commercial interests trump larger political and security concerns was tolerable in a junior partner; it is no longer an adequate basis for partnership. Similarly, the United States must reevaluate the risks of espionage against Germany. There are alternatives to espionage to gain information on Germany's relations with Russia, Iran, and China. If Germany rebuffed serious discussion or continued to place commercial gain above the security of an ally, espionage would be a justifiable. Public dialogue—public because the audience must include the Germans public and not just traditional foreign policy elites—could help shape a new partnership with Germany appropriate for its status, but the United States forfeited a chance to test and perhaps build its relationship with Germany. The benefits of espionage are outweighed by the risk to the bilateral relationship and to U.S. influence in the world, but there is no evidence that this calculation of gain, loss, and risk was ever considered.

The case for spying on Brazil is nonexistent. While Brazil is often antagonistic, it does not pose a risk to national security. Spying on Brazil reflects a failure of oversight that explains many of the excesses revealed by Snowden. If you ask an intelligence agency to get information, they will get it by spying. Intelligence agencies are given collection priorities by the White House that shapes their strategies and expenditures. Presumably someone in the White House or in a Cabinet agency, interested in Brazil, put it on a list of collection priorities for the intelligence community. Or they may have wanted to know if Brazil's president intended to continue her predecessor's policy of rapprochement with Iran. Neither subject justifies espionage against Brazil since such information was obtainable in other ways.

In most cases involving economic intelligence, the private sector, which has powerful incentives to obtain economic information and verify its accuracy, is a better source than espionage and cheaper as well. If you ask an intelligence agency a question, it uses espionage to get the answer even if a better answer is available from other sources. Espionage can confirm publicly available data or commitments,[20] but provides little added value. That said, intelligence agencies are loath to give up the economic portfolio for bureaucratic reasons and their policymaker clients often lack the connections to the financial community that could provide alternative sources of information.

[20] See, for example, Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach," *American University International Law Review* 19, issue 5 (2003): 1091–1113, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1176&context=auilr.

U.S. espionage was not driven by commercial motives. This differentiates it from the espionage activities of most of the countries that spy on the United States. The logic of Snowden's leaks is not one sided. If they have revealed a range of activities, what they have not revealed is equally important. Snowden has not produced any evidence of commercial espionage by the United States. Nor has be produced any evidence of the NSA programs being used for political advantage, to suppress debate or punish opponents.

Enquiries by the European Union in relation to charges about the alleged Echelon signals intelligence system found that the United States did not illicitly acquire business information or technology.[21] The United States does collect information on foreign companies in two specific areas: bribery and nonproliferation. This information is not shared with U.S. companies but with the involved governments as part of a diplomatic exchange to prevent such activities. There is some discussion of whether the United States needs to change its policy on illicitly acquiring technology or business information, but there is currently no serious effort to change existing law to allow this.

Snowden's revelations provided an opportunity to give expression to a not-so-latent anti-Americanism in Europe and Latin America. Contrary to the assertions of Brazil's president at the UN General Assembly, U.S. actions were not a violation of the customary practice among states, which routinely spy on each other. Brazil itself engages in espionage, along with widespread surveillance of its own population with almost no oversight. Nor were U.S. actions illegal under international law. There is no international treaty on espionage, nor is it prohibited. International law studiously ignores espionage that, by definition, is an agent of one country, operating legally under that country's laws, violating the laws of another country. Countries may dislike being spied upon, but it is not illegal.

The missing aspect of the Snowden discussion is that mass surveillance programs conducted by NSA in Europe were done in cooperation with European security services. Because European nations lack adequate oversight mechanisms for intelligence, the signal greatest inaccuracy in the Snowden debate is the failure to recognize that mass surveillance programs were done in cooperation with European partners to prevent terrorist incidents, part of a larger program of cooperation on counterterrorism. Information on these cooperative relationships is not easily found in public sources and it is not in the interests of those handling the Snowden material to highlight this cooperative aspect. European governments cooperated with NSA because it provided global capabilities that significantly improved their counterterrorism capabilities.

It is perfectly understandable that no European government was willing to stand up and say this—there is a strong tradition of keeping intelligence activities secret from their own publics in Europe, and there would have been considerable political risk to any elected official. Still, a blend of hypocrisy, anti-Americanism, and ignorance is not a strong foundation for the transatlantic relationship. NSA mass surveillance was done with the participation of European governments, and the United States need not apologize for the failure of European oversight.

The United States underestimated risk before 9/11 and relied on a cumbersome, legalistic, and fragmented defense. Creating new hurdles or restoring old ones increases the chance of a successful attack. If the probability of a terrorist attack is declining (or if the United States overestimates the probability of attack), curtailing some collection programs will not increase risk. If risk remains the same or is increasing, curtailing an effective intelligence program will increase risk. 9/11 was unprecedented in its audacity and scope, but circumstances that

[21] European Parliament, "REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)," July 11, 2001, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN.

allowed it to occur have changed in ways that make a repetition unlikely. Conventional attacks using firearms and explosives are attempted with such frequency, however, that we cannot say that risk has returned to pre-9/11 levels.

Addressing Surveillance Concerns

Broad surveillance of communications is the least intrusive method and most effective means for discovering terrorist activity. The alternatives to mass surveillance are straightforward. Countries can replace communications surveillance by increasing the number of security service personnel responsible for monitoring terrorism or they can decrease surveillance and accept some increase in the level of risk of a successful attack. The dilemma with choosing this course of action is that the number of agents required to replace communications surveillance is expensive and overtly intrusive in a way the communications surveillance is not. Hundreds of thousands of additional agents would be required to provide national coverage, may lack sufficient global reach to detect activity being planned or undertaken outside U.S. territory, and the creation of such a large force risks creating a much greater chilling effect on liberties

The other risk is political. A vocal minority in the U.S. audience asserts that surveillance has a chilling effect on free speech (although there is no evidence that either the quantity or volume of speech has been in any way affected). European audiences—in part because of a different sense of privacy that we must respect, in part because they lacked familiarity with the role and work of their own intelligence agencies, and in part because of anti-American sentiments—are also disturbed, creating real damage in the transatlantic partnership.

Some of this can be discounted—the European left asserting their disapproval of the United States is nothing particularly new. Saying that this disapproval by both U.S. and European audiences is unfair or undeserved, mistaken, or even driven by a larger anti-American agenda misses the point. The political reality is that surveillance programs have created serious concerns and these must be addressed, by beginning an honest discussion of risk, by putting surveillance in the larger context of resurgent authoritarianism and continuing jihad, and by examining whether existing mechanisms for public oversight of surveillance programs are adequate in the United States and in Europe. The only conclusion that can be drawn from the debate over political risk to democracies from surveillance is that adequate oversight is sadly lacking.

There are legitimate concerns about surveillance and espionage, but the way to address these concerns is not to end surveillance—that would create unacceptable risk—or to create layers of rules and bureaucracy that return us to pre-9/11 gridlock or try to recreate pre-Internet standards of privacy. Change is essential, and the United States could consider several modifications to its existing practices: increased transparency, strengthened oversight, a greater role for courts, modernizing federal privacy laws, and gaining international agreement on principles for data protection.

In 1976, the Final Report of the Church Committee (the Senate Select Committee created to study governmental intelligence activities and operations**)** stated:

> The capabilities that NSA now possesses to intercept and analyze communications are awesome. Future breakthroughs in technology will undoubtedly increase that capability. As the technological barriers to the interception of all forms of communications are being eroded, there must be a strengthening of the legal and operations safeguards that protect Americans.

The Committee was prescient in its predictions, and its report led to the congressional oversight committees we have today and to FISA. But this is one of the problems that created the furor over

surveillance—the oversight structure we now have is almost 40 years old and no longer fits the expectations of citizens for greater transparency into the operations of their government. A delegated approach, where only a few members of Congress were fully apprised of intelligence activities, was sufficient in the 1970s. It is not adequate today. New mechanisms for an appropriate degree of transparency into intelligence activities, particularly any domestic intelligence activities, are essential.

The oversight process that has served us since the 1970s must change to reflect the expectations of citizens for greater transparency and greater accountability. Delegating responsibility to representatives is no longer by itself sufficient. The United States can strengthen the case for intelligence activities by providing the American people examples of where and how these programs have prevented harm. People will not take on faith or assurances alone that the benefits of surveillance outweigh the risk to civil liberties, and we harm national security by not discussing what these programs have stopped.

Oversight involves more than Congress. The biggest change to intelligence oversight is that it must be expanded to include a greater degree of public oversight. This should involve annual reporting, more open hearings, and other activities, such as public speaking engagements by leaders of the intelligence community. The usual reason for not increasing public oversight is that intelligence programs are secret and must remain so. There is a degree of truth in this, but it should not be an excuse for avoiding all transparency. Whatever the merits of the argument that the surveillance programs cannot be made public even at some high level of detail as this would damage their effectiveness and warn our opponents that the lack of public knowledge and debate is what drives much of the public concern and misunderstanding. Democratic governance today requires greater transparency and debate, even for secret activities. Congress and the executive branch must expand its activities in this important public function. Ex post facto releases on intelligence programs and activities, while useful, do not really provide for accountability, as they are too late to provide guidance.

The more important structural change to oversight involves the executive branch. The intelligence agencies are the tool of the president for carrying out American foreign policy and for defense. Congress and the courts have the primary oversight responsibility for ensuring that agencies operate in a legal manner, but the president, while ensuring that espionage is conducted in accordance with the law, has primary responsibility for ensuring that agencies are operating in ways that make political and strategic sense. To do this, he or she must rely on the staff of the National Security Council. Success requires dynamic engagement and leadership among the agencies and a clear sense of U.S. goals. It is the NSC that must weigh, as in the cases of Germany and Brazil, when the political risks of espionage outweigh the benefits. A passive approach will lead either to excess or failure.

The greatest weakens in the oversight structure inherited from the 1970s is its lack of transparency. Adding a privacy advocate to the FISA Court does not solve the transparency problem. It continues the existing overreliance on representative oversight rather than increasing public knowledge. An overreliance on representation is a key flaw in the current oversight system. A privacy advocate would slow the processes of the count—and one of the criticisms of the FISA process as it existed before 9/11 was that it was cumbersome and this contributed to a situation where "the information flow withered."[22] Adding an advocate to the FISA Court smacks of elitism, and a more democratic approach is preferable in the new political environment created by the Internet, which has changed public expectations about how much access to information they should have and where they should have a voice.

The key to a prudent approach to surveillance is deciding what is "reasonable." In making this decision the

[22] National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004), 79.

court, Congress, and the president have acted as agents of the citizen body. This is not a decision that can be left to individual agencies or even to the executive branch. The courts alone decide when a specific search is reasonable, within the limitation defined by the Constitution and by legislation passed by Congress. Court authorization must be mandatory.

Some have argued that while this administration can be trusted to undertake surveillance in a responsible fashion, programs should be dismantled because some later government might be tempted to use them for political purposes. This is of course the origin of espionage oversight in America—the discovery that the president had used foreign intelligence agencies for domestic political purposes, leading to the Watergate crisis. As a result, the Congress placed a range of strictures on the domestic use of intelligence agencies and intelligence collection techniques. The oversight system we have now was designed to prevent such activities, and this safeguard would be strengthened by greater transparency and public awareness. The worry about misuse seems farfetched, and there has been no evidence that either this administration or its predecessor engaged in such misconduct.

This is not the place for a lengthy discussion of reforming privacy law. The United States has a hodgepodge of rules written decades ago. The weakness of privacy protection in the United States is one factor that contributed to the uproar over the Snowden leaks. There are two interconnected dilemmas in reforming privacy. First, an overly restrictive approach will hurt innovation and economic growth. Second, we are likely to get an overly restrictive approach if we do not recognize the change in public attitudes and behavior toward privacy. Privacy is not an absolute and consumers are less concerned about it (judging from their online behavior) than activists. It will take a long debate to reorient thinking about privacy and develop sensible laws, but starting this honest debate is essential.

A final adjustment is international. Most governments surveil communications, and most have little oversight and less transparency in their surveillance activities. Surprisingly, the American oversight system is almost unique in the world. This does not vitiate the reaction to the Snowden revelations, but it points in a useful direction. If NSA and America's closest allies were to end all their surveillance activities, surveillance would continue unabated and privacy would not be greatly improved. This is a global problem—in Washington, D.C., for example, perhaps as many as six nations engage in some kind of communications surveillance against American targets. While agreement on rules of espionage is unlikely, it would be possible to reach agreement on principles of national oversight and on principles to protect data, both of citizens and companies.

Data protection is an indirect way of approaching and regulating communications surveillance that avoids the problem that no sovereign will concede its ability to conduct espionage (and in many cases, even admit to it). The EU data protection rules are inadequate as they do not apply to Europe's national intelligence agencies (whose actions fall outside the scope of Commission authorities), and are not widely observed in other regions of the worlds. Common understandings on data protection and on oversight and transparency would help to regulate the conduct of espionage in a new technological environment.

The United States, Germany, and the United Kingdom have strong oversight systems and a degree of transparency into intelligence activities not found in most other countries. The UK model, with annual reporting (albeit redacted), comprises a special tribunal to receive and hear complaints.[23] These are not substitutes for

[23] See, for example, Office of Surveillance Commissioners, "Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2013–2014," September 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf.

strong congressional or parliamentary oversight but useful additions. While each nation's parliamentary culture is different, there are enough commonalities among democracies that best practices for oversight and transparency could be identified.

The Risk of Attack Is Not Going Away

These six steps would address the concerns created by surveillance programs. Now is not the time to dismantle them. But the use of communications surveillance for security must be reexamined and carried out in ways that do not pose risks to the values that are the ultimate foundation of our strength. Strong oversight mechanisms and greater transparency are the keys to acceptance and credible accountability. While every nation must undertake some activities in secret, democracies require that national priorities and policies be publicly debated and that government be accountable to the citizens for its actions. To rebuild trust and strengthen oversight, particularly for collection programs that touch U.S. persons, greater openness is essential. Too much secrecy damages national security and creates the risk that Americans will perceive necessary programs as illegitimate.

The phrase "terrorism" is overused, and the threat of terrorist attack is easily exaggerated, but that does not mean this threat it is nonexistent. Groups and individuals still plan to attack American citizens and the citizens of allied countries. The dilemma in assessing risk is that it is discontinuous. There can be long periods where no activity is apparent, only to have the apparent calm explode in an attack. The constant, low-level activity in planning and preparation in Western countries is not apparent to the public, nor is it easy to identify the moment that discontent turns into action.

There is general agreement that as terrorists splinter into regional groups, the risk of attack increases. Certainly, the threat to Europe from militants returning from Syria points to increased risk for U.S. allies. The messy U.S. withdrawal from Iraq and (soon) Afghanistan contributes to an increase in risk.[24] European authorities have increased surveillance and arrests of suspected militants as the Syrian conflict lures hundreds of Europeans. Spanish counterterrorism police say they have broken up more terrorist cells than in any other European country in the last three years.[25] The chairman of the House Select Committee on Intelligence, who is better placed than most members of Congress to assess risk, said in June 2014 that the level of terrorist activity was higher than he had ever seen it.[26] If the United States overreacted in response to September 11, it now risks overreacting to the leaks with potentially fatal consequences.

A simple assessment of the risk of attack by jihadis would take into account a resurgent Taliban, the power of lslamist groups in North Africa, the continued existence of Shabaab in Somalia, and the appearance of a powerful new force, the Islamic State in Iraq and Syria (ISIS). Al Qaeda, previously the leading threat, has splintered into independent groups that make it a less coordinated force but more difficult target. On the positive side, the United States, working with allies and friends, appears to have contained or eliminated jihadi groups in Southeast Asia.

Many of these groups seek to use adherents in Europe and the United States for manpower and funding. A Florida teenager was a suicide bomber in Syria and Al Shabaab has in the past drawn upon the Somali

[24] Jon Swaine, "NYPD terror chief: New Yorkers among American Islamists in Middle East," *The Guardian*, June 20, 2014, http://www.theguardian.com/world/2014/jun/20/nypd-terror-chief-new-yorkers-american-islamists-middle-east.
[25] Carlotta Gall, "Spanish Police Target Cells Recruiting War Volunteers," *New York Times*, June 16, 2014, http://www.nytimes.com/2014/06/17/world/europe/spanish-police-target-cells-recruiting-war-volunteers-for-insurgencies-from-western-africa-syria-iraq.html?ref=todayspaper.
[26] Representative Michael Rogers, first panel, "Ethos and Profession of Intelligence," Georgetown University, Washington, DC, June 12, 2014, http://www.georgetown.edu/news/cia-conference-2014.html.

population in the United States. Hamas and Hezbollah have achieved quasi-statehood status, and Hamas has supporters in the United States. Iran, which supports the two groups, has advanced capabilities to launch attacks and routinely attacked U.S. forces in Iraq. The United Kingdom faces problems from several hundred potential terrorists within its large Pakistani population, and there are potential attackers in other Western European nations, including Germany, Spain, and the Scandinavian countries. France, with its large Muslim population faces the most serious challenge and is experiencing a wave of troubling anti-Semitic attacks that suggest both popular support for extremism and a decline in control by security forces.

The chief difference between now and the situation before 9/11 is that all of these countries have put in place much more robust surveillance systems, nationally and in cooperation with others, including the United States, to detect and prevent potential attacks. Another difference is that the failure of U.S. efforts in Iraq and Afghanistan and the opportunities created by the Arab Spring have opened a new "front" for jihadi groups that makes their primary focus regional. Western targets still remain of interest, but are more likely to face attacks from domestic sympathizers. This could change if the well-resourced ISIS is frustrated in its efforts to establish a new Caliphate and turns its focus to the West. In addition, the al Qaeda affiliate in Yemen (al Qaeda in the Arabian Peninsula) continues to regularly plan attacks against U.S. targets.[27]

The incidence of attacks in the United States or Europe is very low, but we do not have good data on the number of planned attacks that did not come to fruition. This includes not just attacks that were detected and stopped, but also attacks where the jihadis were discouraged and did not initiate an operation or press an attack to its conclusion because of operational difficulties. These attacks are the threat that mass surveillance was created to prevent. The needed reduction in public anti-terror measures without increasing the chances of successful attack is contingent upon maintaining the capability provided by communications surveillance to detect, predict, and prevent attacks. Our opponents have not given up; neither should we.

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy.

[27] Michael S. Schmidt and Eric Schmitt, "Flights to U.S. Face Scrutiny after Threats Are Reported," *New York Times*, July 2, 2014, http://www.nytimes.com/2014/07/03/us/flights-to-us-tighten-security-after-threat-of-bombs.html.