I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

National Insecurity: The Impacts of Illegal Disclosures of Classified Information

MARK D. YOUNG*

> There had never been anything like it. In today's terms, it was as if an NSA employee had publicly revealed the complete communications intelligence operations of the Agency for the past twelve years-all its techniques and major successes, its organizational structure and budget-and had, for good measure, included actual intercepts, decrypts, and translations of the communications not only of our adversaries but of our allies as well.[1]

In the mid-summer of 2013, the British newspaper, *The Guardian*, published claims by a contractor for the National Security Agency (NSA), that millions of telephone records were being collected under an order from the Foreign Intelligence Surveillance Court. Throughout the summer and fall, additional disclosures about apparent surveillance operations seized headlines around the world. Accurately interpreting the meaning of the disclosures has been more complicated, but it is clear that there is great public interest in United States intelligence activities.

---

*Mark D. Young is the Senior Vice President and Chief Strategy Officer of National Security Partners, LLC. Previously he served as the Executive Director for the Directorate of Plans and Policy at United States Cyber Command, the Special Counsel for Defense Intelligence for the House Permanent Select Committee on Intelligence, and as a senior leader at the National Security Agency. The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. government. This article is derived entirely from open source material and contains no classified information.

[1] National Security Agency, *The Many Lives of Herbert O. Yardley*, CRYTPTOLOGIC SPECTRUM (Autumn 1981, Vol. 11 No. 4) at 10.

Despite being fired from his contractor position with Booz Allen Hamilton[2] and charged with espionage and theft, Edward Snowden continued to provide classified information to *The Guardian*. The paper has published more than 300 stories on signals intelligence methodologies, the statutes and court authorities under which the United States Intelligence Community conducts these operations, and the intelligence relationships between foreign governments and the United States.[3]

These disclosures of sensitive and classified information concern not only the United States, but also its allies. The material disclosed by Snowden has implicated the United Kingdom's Government Communications Head Quarters (GCHQ). British government concerns about the potential publication of classified data were significant enough to threaten *The Guardian* with legal action if the information was not destroyed. The threats prompted the destruction of hard drives containing information related to GCHQ.[4]

The national security implications of Snowden's actions are significant. According to the most experienced U.S. intelligence officer, Michael V. Hayden,[5] "Edward Snowden will likely prove to be the most costly leaker of America secrets in the history of the Republic."[6] The Chairman of the House Intelligence Committee has noted that Snowden has jeopardized U.S. national security by

---

[2] Shashank Bengali, *Edward Snowden Fired, Booz Allen Hamilton Says,* L.A. TIMES, June 11, 2013, *available at* http://articles.latimes.com/2013/jun/11/news/la-pn-edward-snowden-fired-booz-allen-20130611.

[3] James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far*, THE GUARDIAN, Aug. 21, 2013, *available at* http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations.

[4] Julian Borger, *NSA Files: Why The Guardian in London Destroyed Hard Drives of Leaked Files*, THE GUARDIAN, Aug. 20, 2013, *available at* http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london. This destruction has not prevented the further disclosures of classified data, however, since the reporter who first broke the story, had additional copies of the material in Brazil and in the United States. Nicholas Watt et al., *NSA Files: UK and US at Odds Over Destruction of Guardian Hard Drives*, THE GUARDIAN, Aug. 20, 2013, *available at* http://www.theguardian.com/world/2013/aug/20/nsa-david-miranda-guardian-hard-drives.

[5] General Michael V. Hayden is a career military intelligence officer who led the Central Intelligence Agency, the National Security Agency, and was the first Principal Deputy Director of National Intelligence. *See generally, Michael Hayden*, THE CHERTOFF GROUP, http://chertoffgroup.com/bios/michael-hayden.php (last visited Mar. 2, 2014).

[6] Michael Hayden, *Ex-CIA Chief: What Edward Snowden Did*, CNN (July 19, 2013), http://www.cnn.com/2013/07/19/opinion/hayden-snowden-impact/index.html.

exposing ongoing U.S. counterterrorism activities.[7] The Director of National Intelligence (DNI) stated, "[t]he unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation."[8] There are those, however, that dispute these claims by current and former high-ranking intelligence officials and elected representatives.[9]

Snowden claims that his disclosures–made in violation of law, regulation, and his solemn oath–are motivated by his judgment about the value of the intelligence. He removed and released data that allegedly shows how the NSA had collected information on civilian institutions, to include universities, hospitals, and businesses. Snowden claims these alleged NSA operations are dangerous and criminal: "These nakedly, aggressively criminal acts are wrong no matter the target."[10] Without referencing the multiple layers of intelligence oversight within the Department of Defense, the Office of the Director of National Intelligence (ODNI), the NSA's Inspector General, and the Intelligence Community Inspector General, Snowden concluded that "the public needs to know the kinds of things a government does in its name, or the 'consent of the governed' is meaningless."[11]

Regardless of one's sympathy for Snowden's conclusion, the scope and scale of the material he has revealed will have a continuing impact on U.S. national security. There are four areas where his actions will

---

[7] Evan McMurry, *GOP Rep. Rogers Blasts Snowden: Just Got To North Korea, Iran to Round Out 'Government Oppression Tour,'* MEDIATE (June 23, 2013) *available at* http://www.mediaite.com/tv/gop-rep-rogers-blasts-snowden-just-go-to-north-korea-iran-to-round-out-government-oppression-tour/.

[8] Press Release from James R. Clapper, Director of National Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information, Office of Director of National Intelligence (June 6, 2013) *available at* http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information.

[9] *See generally* Jon Mueller & Mark G. Stewart, *Secret Without Reason and Costly Without Accomplishment: Questioning the NSA's Metadata Program*, 9 ISJLP (forthcoming, Spring 2014) *available at* http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Mueller-and-Stewart.pdf; Klayman v. Obama, CV 13-0881 (RJL), 2013 WL 6598728 (D.D.C. Dec. 16, 2013).

[10] *Edward Snowden: NSA Whistleblower Answers Reader Questions,* THE GUARDIAN, June 17, 2013, *available at* http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

[11] *Id.*

diminish national security. First, the disclosure of the programs, relationships, and operations will facilitate operational changes in the behavior of adversarial groups such as al-Qaeda and Hamas.[12] It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Second, the disclosures will complicate U.S. foreign relations that directly contribute to U.S. security interests. Cooperation between U.S. and foreign intelligence organizations is critical to the security of the U.S.[13] Other countries are perpetually concerned about disclosing sensitive information collected by their intelligence services. Snowden has now exacerbated these concerns and weakened traditionally strong American assurances that information provided to the U.S. will be well protected with little risk of embarrassment or compromise to the providing country. It will become more difficult to cooperate with these partners when there is a stream of evidence that shows that the U.S. cannot keep a secret.

Third, Snowden's actions have impaired cooperation between the United States government and the U.S. private sector. It was already challenging to share information between the U.S. public and private sectors,[14] but the exposure of alleged relationships—whether voluntary or pursuant to a court order-between companies such as Verizon, Google, and Facebook has made corporate entities recoil from the U.S. government in fear of a diminished reputation or decline in stock value.

Finally, despite Snowden's claimed objective of exposing an "architecture of oppression,"[15] his violation of law, regulation, and

---

[12] *See generally* U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2005, 11 (Apr. 2006) *available at* http://www.state.gov/documents/organization/65462.pdf.

[13] The National Strategy for Information Sharing and Safeguarding highlights the importance of sharing with partner nations, "our national security depends upon an ability to make information easily accessible to Federal, state, local, tribal, territorial, private sector, and foreign partners in a trusted manner, given the appropriate mission context." PRESIDENT BARACK OBAMA, NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING 7 (Dec. 2012) *available at* http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

[14] *See generally*, Jennifer Martinez & Ramsey Cox, *Senate Votes Down Lieberman, Collins Cybersecurity Act a Second Time*, THE HILL (Nov. 14, 2012, 11:12 PM), http://thehill.com/blogs/hillicon-valley/technology/268053-senate-rejects-cybersecurity-act-for-second-time.

[15] Laura Poitras & Glenn Greenwald, *NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society That Does These Sort of Things'–Video* at 7:00, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

oath has eroded the confidence of the American public he was hoping to inform. In our representative democracy, this loss of public confidence will quickly transform into fewer resources for the very departments and agencies that enhance American security. Less authority and more scrutiny are sure to follow. It is understandable, but the reduction in funding, authority, and the increase in oversight are the type of emotionally satisfying reactions that will add nothing to U.S. national security.

These four consequences of Snowden's illegal exposures of classified data will diminish U.S. national security particularly in the short term. It is possible that the reforms and examination of technical collection and analysis will become stronger in the long term, but this is unlikely in the context of rapidly diminishing government funding, continuing economic hardships, and the erosion of the public appreciation for security threats. Not all the comments from public and private officials have been accurate or helpful, however.

Some national security officials have "welcomed the debate" surrounding the collection of metadata.[16] In this volume, Mueller and Stewart note that the debate is "much overdue."[17] This debate has been ongoing within the national security establishment for decades. The balance between the perils and necessity of governmental secrecy has been a preoccupation of our Republic since its founding.[18] Privacy debates surrounding electronic surveillance can be traced to the early 1900s:

> Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of government secrets during World War I. Later, it proscribed intercepting and divulging private radio messages in the Radio Act of 1927, but did not immediately reestablish a federal wiretap prohibition. By the time of the landmark Supreme Court decision in

---

[16] *See, e.g.*, U.S. President Barack Obama, Statement by the President at the Fairmont Hotel, San Jose, California (June 7, 2013) *available at* http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president; Dan De Luce, *Snowden Leaks Sparked Welcome Debate: US Spy Chief*, AFP, Sept. 12, 2013, *available at* http://www.google.com/hostednews/afp/article/ALeqM5hJp1lx8BXL3l1PYmyqNJ3vnbATMw?docId=CNG.c782a92a914963661ee705f89a1d7523.481.

[17] Mueller & Stewart, *supra* note 9.

[18] *See generally*, Gabriel Schoenfeld, Necessary Secrets: National Security, the Media, and the Rule of Law 55 (2010).

> *Olmstead*, however, at least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.[19]

Within the past ten years, there has been vigorous debate in the media and within Congress surrounding the scope and volume of data—including metadata relating to U.S. persons—the U.S. government was allowed to collect and analyze.[20] This debate is only new—or overdue—to those who have chosen to avoid engagement in a most difficult of legal and policy issues.

Perhaps there are those who feel as if there has been insufficient discussion of surveillance matters because they do not understand the mechanisms of intelligence oversight that have existed in the United States since the 1970s. The public does not have an unrestricted right to access information determined by the President to be classified.[21] The public is represented, including in the oversight of classified intelligence matters, by its elected officials. Declassified documents demonstrate that the public's elected officials—our representatives in the classified realm—were privy to the collection of bulk metadata under Section 215 of the USA PATRIOT Act.[22] This correspondence encourages the members of the congressional intelligence committees to provide the classified information to other congressional members

---

[19] GINA MARIE STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 7-5700, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 2 (2009).

[20] *See, e.g.*, ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL34143, P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2007); RICHARD A. BEST, JR., CONG. RESEARCH SERV., RL 30252, INTELLIGENCE AND LAW ENFORCEMENT: COUNTERING TRANSNATIONAL THREATS TO THE U.S. (2001)("[g]iven the clear possibility that the international role of law enforcement agencies will continue to grow, observers believe that greater consideration should be given to making less ambiguous distinctions between law enforcement and security policy and to the relationships between law enforcement and intelligence agencies."); JENNIFER ELSEA, CONG. RESEARCH SERV. RS21472, PROPOSED CHANGE TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) UNDER S. 113, (2003); CHARLES DOYLE, CONG. RESEARCH SERV., RL31377, THE USA PATRIOT ACT: A LEGAL ANALYSIS (2002).

[21] *See generally* Exec. Order No. 13526, 3 C.F.R. 13526 (2009).

[22] *See* U.S. DEP'T OF JUSTICE, REPORT ON THE NATIONAL SECURITY AGENCY'S BULK COLLECTION PROGRAMS AFFECTED BY THE USA PATRIOT ACT REAUTHORIZATION (2009).

because it would "be an effective way to inform the legislative debate about reauthorization of Section 215."[23]

Elected officials charged with oversight of intelligence within the House of Representatives also have the ability to disclose classified information. According to the Rules of the House of Representatives for the 113th Congress: "Nothing [within the House rules] shall be construed to prevent the select committee from publically disclosing classified information in a case in which it determines that national interest in the disclosure of classified information clearly outweighs any infringement on the privacy of a person."[24]

Thus, this debate has raged since the birth of our democracy and that elected officials have engaged in this debate on our behalf for a decade (this debate has increased in intensity since September 11, 2001). Those charged with representing the public interest in classified matters not only have been well-informed of the activities under Section 215 of the USA Patriot Act, but also have the legal authority to disclose these programs if they determined that it was in the national interest.

The current administration's National Security Strategy, published in May 2010 provides the focus for an examination of the impacts of the Snowden disclosures.[25] This strategy prioritizes American leadership by "shaping an international order that can meet the challenges of our time" and "recognizes the fundamental connection between our national security, our national competitiveness, resilience, and moral example."[26] U.S. national security interests are: Strengthening Security and Resilience at Home, the Disruption, Dismantling, and Defeat of al-Qaeda and its Violent Extremist Affiliates, the Use of Force only as a last resort, the Reverse of the Spread of Nuclear and Biological Weapons, the Advancement of Peace, Security, and Opportunity in the Greater Middle East, the Investment in the Capacity of Strong and Capable Partners, and the Securing of Cyberspace.

Consistent with the U.S. national security interests are the global and regional threats outlined by the DNI in April 2013. The Increasing

---

[23] *Id.*

[24] KAREN HAAS, RULES OF THE HOUSE OF REPRESENTATIVES, 113TH CONGRESS 15 (2013) *available at* http://clerk.house.gov/legislative/house-rules.pdf.

[25] U.S. PRESIDENT BARACK OBAMA, NATIONAL SECURITY STRATEGY (2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf [hereinafter NATIONAL SECURITY STRATEGY].

[26] *Id.* at 1.

Risk to U.S. Critical Infrastructure, Eroding U.S. Economic and National Security, and Information Control and Internet Governance put cybersecurity at the top of the DNI's Worldwide Threat Assessment.[27] Terrorism and Transnational Organized Crime, and the proliferation of weapons of mass destruction were also listed as global threats. With respect to regional threats, Middle East, and North Africa (Egypt, Syria, Iran, Iraq, Yemen, Lebanon, and Libya) were listed as threats because the transitioning governments within this region are at risk of failing to "address public demands for change" and "are likely to revive unrest and heighten the appeal of authoritarian or extremist solutions."[28] The information disclosed by Snowden is negatively affecting the national security community's ability to collect and analyze information concerning each of these regional and transnational threats.

I. OPERATIONAL SHIFTS

> "Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions."[29]

The classified material published by *The Guardian* and other media describes in significant detail the methodologies apparently employed by the NSA in the conduct of its mission. Established in 1952, the NSA produces signals intelligence[30] and protects U.S. communications from interception. According to David Kahn, "[i]n intelligence, [the NSA] intercepts, traffic-analyzes, and cryptoanalyzes the messages of other nations, friend as well as foe."[31] In addition, the NSA executes "the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States

---

[27] *Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm.*, 113th Cong 2 (2013)(statement of James R. Clapper, Director of National Intelligence) *available at* http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf.

[28] *Id.* at 14.

[29] Press Release, *supra* note 8.

[30] Intelligence comprising communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.

[31] DAVID KAHN, THE CODE BREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET 675 (2d ed. 1996).

Government."[32] This means that the agency must provide technical and practical means to ensure that no other parties can benefit from the collection of U.S. communications.

Current examples of the NSA's contributions to national security are difficult to find because of the sensitivity of the agency's mission. In recent congressional testimony, however, the DNI said that SIGINT is the primary contributor to counterterrorism intelligence and that multiple empirical studies have shown that signal intelligence, provided by the NSA, is the major contributor to answering the hardest intelligence challenges faced by the U.S.[33]

Although the claims in these books are unconfirmed, publications such as Counter Strike: The Untold Story of America's Secret Campaign Against Al Qaeda by Eric Schmitt and Thom Shanker and Operation Dark Heart: Spycraft and Special Ops on the Frontlines of Afghanistan–and the Path to Victory by Lieutenant Colonel Anthony Shaffer suggest that the NSA may have prevented significant terrorist attacks and provided critical intelligence during U.S. military operations.

These books, together with the claims of senior intelligence officials before Congress, strongly suggest that the NSA's efforts are the most effective shield against the acts of violence that harm U.S. and allied military members, Americans, and our national security interests. In response to apparent disclosures of NSA activities, President Obama directed the declassification of sensitive NSA collection conducted under the Foreign Intelligence Surveillance Act (FISA). In September 2013, multiple documents concerning "bulk telephony metadata" collection under Section 501 of FISA were declassified and publically released by the ODNI.[34] These disclosures included a Foreign Intelligence Surveillance Court finding of reasonable grounds that the call records were relevant to an authorized terrorism investigation.[35] The same order required the

---

[32] Exec. Order No. 12333, 46 Fed. Reg. 59941 (2008).

[33] *USHR19 Permanent Select Committee on Intelligence* at 4:36, USTREAM (Oct. 29, 2013) http://www.ustream.tv/recorded/40304984.

[34] *DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, Office of the Director of National Intelligence Newsroom (Oct. 28, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/954-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act (FISA Section 501 was amended by Section 215 of the USA PATRIOT Act in 2001).

[35] *In Re* Application of the Federal Bureau of Investigation for An Order Requiring The Production of Tangible Things From [Redacted], Docket No. BR 06-05 at 3 (FISA Ct.

NSA to establish "mandatory procedures strictly to control access to and use of the archived data collected pursuant to [the court's] order."[36] Additionally, the order mandated that the NSA's General Counsel monitor the designation of those with access to the data and act as an approval authority for the actual queries analysts wished to make of the data.[37]

In late October 2013, the ODNI released a number of additional documents related to the NSA's alleged collection programs. These documents include a 2009 NSA congressional notification describing the failure to comply with a Foreign Intelligence Surveillance Court order,[38] and a March 2009 Internal NSA Memorandum of Understanding required for access and query privileges of data collected through the NSA's bulk telephony metadata program.[39] These documents describe the legal justifications for and technical detail about how the NSA collects and uses intelligence.

This information was declassified and publically released to inform the public about what data was collected and analyzed by the NSA, to balance inaccurate speculations by the media about the NSA, and to facilitate the debate about U.S. Intelligence Community operations. When examined together, the information disclosed by Snowden and the declassified information released by the ODNI present a positive picture of prudent measures for national security. If the information about programs such as PRISM, FAIRVIEW, or OAKSTAR is accurate, then it appears as if the Intelligence Community has not only adjusted well to global technical advancements in telecommunications, but also learned significant lessons from the September 11, 2001 terrorist attacks.

2006) *available at* http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

[36] *Id.*

[37] *Id.* at 5-6.

[38] VITO T. POTENZA, MEMORANDUM FOR THE STAFF DIRECTOR, HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, CONGRESSIONAL NOTIFICATION: INCIDENTS OF NONCOMPLIANCE–INFORMATION MEMORANDUM (Feb. 25, 2009) *available at* http://www.dni.gov/files/documents/501/25%20Feb%2009%20NSA%20CN_SealedFINAL.pdf.

[39] The form can be found at: Office of Director of National Intelligence, *Memorandum of Understanding s2I4 HNCs,* http://www.dni.gov/files/documents/501/Mem%20of%20Understanding%20for%20H2I4%20HMCs_Sealed%20FINAL.pdf (last visited Feb. 28, 2014).

It was known in early 2001 that the NSA's effectiveness was challenged by the "multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states."[40] Any challenge about the value of an intelligence program must address the importance of data quantity and quality. First, since intelligence analysis depends on having access to relevant information, logic dictates that more data is always better. As noted by Mark Lowenthal:

> The issue then becomes how to extract the intelligence from the mountain of information. One answer would be to increase the number of analysts who deal with the incoming intelligence, but that raises further demands on the budget. Another possible response, even less palatable, would be to collect less. But, even then, there would be no assurance that the "wheat" remained in the smaller volume still being collected.[41]

Thus, quantity has an intelligence quality all its own. In addition, the type of information needed by the Intelligence Community is also important. Given the priorities noted in the National Security Strategy, the importance of NSA collection and analysis as noted in congressional testimony and the ever-present threats by terrorist groups and hostile nations the American public should vigorously endorse the type of programs viewed by Snowden as oppressive. It is troubling to see the disclosure of techniques allegedly used by the NSA to obtain "cryptographic details of commercial cryptographic information security systems through industry relationships,"[42] and the rampant speculation about the monitoring of the mobile phones of the heads of state from Europe.

It is not only logic that leads one to believe in the value of NSA collection, but also testimony by intelligence professionals. For example, according to the House Intelligence Committee, NSA activities have "been integral in preventing multiple terrorist attacks,

---

[40] RICHARD A. BEST, JR., CONG. RESEARCH SERV. RL30740 SUMMARY, THE NATIONAL SECURITY AGENCY: ISSUES FOR CONGRESS (2001).

[41] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 55 (2000).

[42] *NSA: Classification Guide for Cryptanalysis*, THE GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis.

including a plot to attack [sic] the New York Stock Exchange in 2009."[43] The PRISM program, a program reported to provide the NSA access to information from some of the largest technology companies, provided "critical leads" to disrupt more than fifty potential terrorist events in more than twenty countries. According to officials, the FISA authority—the congressional authorization to target communications of foreign persons who are located abroad for foreign intelligence purposes—contributed to more than ninety percent of these disruptions.[44]

The Deputy Attorney General has noted that the FBI benefited from the NSA's Section 702 collection in the fall of 2009. Using Section 702 collection and "while monitoring the activities of [al-Qaeda] terrorists in Pakistan, the [NSA] noted contact from an individual in the U.S. that the [FBI] subsequently identified as Colorado-based Najibulla Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with [al-Qaeda], as well as identify any foreign or domestic terrorist links."[45]

> The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi, upon indictment, pled guilty to conspiring to bomb the NYC subway system. Compelled collection (authorized under Foreign Intelligence Surveillance Act, FISA, Section 702) against foreign terrorists was critical to the discovery and disruption of this threat against the U.S.[46]

---

[43] Press Release, U.S. House of Representatives Permanent Select Committee on Intelligence, Chairman Mike Rogers and Ranking Member Dutch Ruppersberger Urge Support of Important NSA Counterterrorism Tool (July 23, 2013) *available at* http://intelligence.house.gov/press-release/chairman-mike-rogers-and-ranking-member-dutch-ruppersberger-urge-support-important-nsa.

[44] *National Security Agency Data Collections Programs* at 37:30, C-SPAN (June 18, 2013), http://www.c-span.org/video/?313429-1/nsa-chief-testifies-damage-surveillance-leaks [hereinafter CSPAN HPSCI Hearing].

[45] FOUR DECLASSIFIED EXAMPLES, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, *available at* http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section (last visited Mar. 2, 2014).

[46] *Id.*

Regardless of the accuracy of the information released by Snowden, the types of programs described by the material appear to directly contribute to national security; its release, regardless of its validity, will negatively impact U.S. security.

Homegrown Violent Extremists[47] continue to be inspired by global jihadist propaganda and the perceived success of plots such as the November 2009 attack at Fort Hood, Texas and the March 2012 attacks by an al-Qaeda-inspired extremist in Toulouse, France.[48] The threat from terror groups remains constant, urgent, and of great concern to the U.S. Intelligence Community. The revelations concerning the NSA's counterterrorism successes will motivate terror groups to reexamine how they communicate, plan, and execute these attacks.

Despite these publically acknowledged examples of the value of the bulk metadata program, multiple reports and a federal district court opinion have denied its efficacy. The Privacy and Civil Liberties Oversight Board[49] recommends discontinuing the program. The board noted, "an intelligence-gathering tool with significant ramifications for privacy and civil liberties cannot be regarded as justified merely because it provides *some* value in protecting the nation from terrorism."[50]

A panel of advisors that included former government officials such as Richard Clarke (former National Coordinator for Security, Infrastructure Protection, and Counterterrorism), Michael J. Morell (former deputy director of the CIA), and Cass Sunstein (former head of the Office of Information and Regulatory Affairs in the Obama

---

[47] *See generally* JEROME P. BJELOPERA, CONG. RESEARCH SERV., R41416, AMERICAN JIHADIST TERRORISM: COMBATING A COMPLEX THREAT 5 (2013) *available at* http://www.fas.org/sgp/crs/terror/R41416.pdf ([h]omegrown violent extremists are jihadist-inspired American citizens or legal permanent residents that plan or conduct terrorist attacks on the United States).

[48] *Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm., supra* note 27, at 4.

[49] An independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007; successor to the Board created within the Executive Office of the President under the Intelligence Reform and Terrorism Prevention Act of 2004. Privacy and Civil Liberties Board, http://www.pclob.gov/.

[50] PRIVACY AND CIVIL LIBERTIES BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 145 (Jan. 23, 2014) *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

White House) did not recommend the cessation of the bulk metadata program. In an unreleased report, commissioned by the president in August, the panel "went further than some of the agency's backers in Congress, who would make only cosmetic changes to it, but stopped short of calling for the program to be shut down, as its critics have urged."[51] They did, however question its value: "The [NSA] uses the telephone data to search for links between people in an effort to identify hidden associates of terrorism suspects, but the report says it 'was not essential to preventing attacks.'"[52]

The panel's report was provided to the president three days after a federal judge determined, in a case seeking an injunction to stop the NSA program, that the Government failed to cite a "single instance in which the analysis of the NSA's bulk metadata collection actually stopped an imminent attack or otherwise aided the government in achieving any objective that was time-sensitive in nature."[53] United States District Judge Richard J. Leon came to a dramatically different conclusion than United States District Judge William Pauley in similar cases dealing with the same program.[54]

In this volume, Mueller and Stewart claim that "the achievements of [the bulk metadata program] do seem to be decidedly underwhelming," despite acknowledging that in at least four cases, analysis of the metadata contributed to the arrest or locating of known terrorists or facilitators.[55] Their analysis is flawed in the same way as is Judge Leon's and the Privacy and Civil Liberties Board. The comments made by critics of the program appear to be motivated more by ideology than dispassionate assessment of analytical tradecraft. The complexities, technology, and ambiguity of the modern security environment make it unlikely that any single intelligence source or program will provide a "smoking gun" on a national security

---

[51] David E. Sanger and Charlie Savage, *Obama Is Urged to Sharply Curb N.S.A. Data Mining*, N.Y. TIMES, Dec. 18, 2013, *available at* http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html?pagewanted=1&_r=0.

[52] *Id.*

[53] Klayman v. Obama, CV 13-0851 (RJL)(D.D.C. Dec. 16, 2013).

[54] In *ACLU v. Clapper*, United States District Judge William Pauley granted a motion by the government to dismiss a suit filed in June by several groups led by the ACLU seeking to block the program authorized by Section 215 of the PATRIOT Act. He rejected the ACLU's concerns about what *could* be done with these data and their contention that other less-intrusive means could lead to the same information. No. 13 Civ. 3994 (S.D.N.Y. Dec. 27, 2013).

[55] Mueller & Stewart, *supra* note 9.

threat.[56] The Intelligence Community has sharpened its techniques since September 11, 2001 with this new reality in mind.

The complexity of the international system, incomplete and inconsistent information, and the "inherent limitations of the human mind" are perennial problems for intelligence professionals.[57] To overcome these realities, the Intelligence Community must apply a dizzying set of analytic techniques and mental discipline to review key assumptions about their operational tasks, validate the quality of the information collected and available to them, identify indicators of actualized threats, and continually strive to anticipate the thinking of those who seek to harm U.S. citizens or the security interests of the United States and our allies. This is no small task and it requires a mosaic of information, to include bulk metadata.

Judge Leon at least acknowledged his unfamiliarity with the complexities of any conversation about bulk metadata collection and analysis. By staying his order to discontinue the program, he concedes that the data may be of critical importance to national security: "[I]n light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending appeal."[58]

Examples of the efficacy of the program are provided below, yet the public should keep in mind the unsatisfying fact that intelligence analysis is a laborious process that requires reason and passion. The author concedes that none of these examples provides an irrefutable defense of the accessing of bulk metadata. The program does, however, provide a valuable link in the national security chain. Although frustrating to the intelligence professionals who devote a large portion of their professional lives to the protection of the security, and civil liberties, of all U.S. citizens the debate is welcome, yet certainly not new.

Critics and supporters alike must ask themselves whether they consider the evidence provided by intelligence professionals and those we have elected to oversee them or allow passion to cloud our judgment and poison our vision. Tom Nichols, professor of National

---

[56] The Privacy and Civil Liberties Board report highlights this inappropriate expectation in the following statement: "[W]e have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation." PRIVACY AND CIVIL LIBERTIES BOARD, *supra* note 50, at 146.

[57] *See generally* U.S. Government, A Tradecraft Primer: Structured Analytics Techniques for Improving Intelligence Analysis 1 (Mar. 2009).

[58] *Klayman*, CV 13-0851.

Security Affairs at the U.S. Naval War College, recently commented on this sort of rejection of expertise in his blog, The War Room: "A fair number of Americans now seem to reject the notion that one person is more likely to be right about something, due to education, experience, or other attributes of achievement, than any other."[59] Nichols' assessment is directly applicable to the critics of the bulk metadata collection program. No matter what evidence intelligence professionals proffer, no matter what fifteen Foreign Intelligence Surveillance Court judges have concluded on more than thirty occasions, no matter what elected officials charged with oversight of these activities say, it will be insufficient to those who are outraged in their ignorance that these programs ever existed. Despite the claim that the "benefits provided [by the bulk metadata program] have been minimal," the following examples illustrate the advantages of the program.

A. *Terror Groups*

It is likely that terrorist groups will change how they conceive, plan, and execute terrorist attacks as a result of the classified intelligence information now exposed to the public. Terrorist groups continuously adjust their methodologies for attacking their targets,[60] but the recent disclosures provide a roadmap for terror groups to avoid detection.

A similar example of how terrorist groups adjust their planning and communication techniques in response to the disclosure of classified information is found in the *9/11 Commission Report*. Referring to a 1998 *Washington Times* story disclosing that Osama Bin Laden communicated via a satellite phone, the Commission noted that al-Qaeda's senior leadership "had stopped using a particular means of communication almost immediately after a leak to *The Washington Times*. This made it much more difficult for the NSA to intercept his conversations."[61] Despite the controversy surrounding

---

[59] Tom Nichols, *The Death of Expertise*, THE WAR ROOM: TOM NICHOLS ON POLITICS AND FOREIGN POLICY (Dec. 11, 2013), http://tomnichols.net/blog/2013/12/11/the-death-of-expertise.

[60] According to the Director of National Intelligence, al-Qaeda in the Arabian Peninsula remains focused on attacks on US soil and "continues to adjust its tactics, techniques and procedures for targeting the West." *Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm.*, *supra* note 27, at 3.

[61] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 127 (2004) [hereinafter 9/11 COMMISSION REPORT].

this story, it makes logical sense that terror groups will not use technologies reportedly monitored by those who seek to disrupt their plans.

Similar changes in terror group practices can be anticipated with the Snowden disclosures. The details of how intelligence targets will alter their practices are speculative given the obscurity of terrorist methodologies, but a few points are clear.

If the reports are true and the NSA can exploit[62] the "worldwide use of nine U.S.-based Internet service providers, including Google, Yahoo, Skype, and YouTube," then it is reasonable to assume that terrorist groups using these technologies or services will discontinue use of these services. According to the *New York Post*, the Snowden disclosures resulted in jihadists posting Arabic news articles about [NSA's capabilities] . . . and recommended fellow jihadists to be very cautious, not to give their real phone number and other such information when registering for a website." [63] Similar posts recommending jihadists use "privacy-protecting email systems like TOR, also called The Onion Router, to hide their computer's IP address, and to use encrypted links to access jihadi forums"[64] provide direct evidence that the recent disclosures will change how terrorists plan and conduct their attacks.

Another example concerns alleged NSA access to Skype. Purchased by Microsoft in 2011, Skype claims to employ encryption to protect users from hackers and criminals.[65] Documents published by *The Guardian* suggest that the NSA may have had access to Skype servers.[66] Despite this suggested access, others claim that Skype calls made to other Skype customers were untraceable because of Skype's corporate location.

---

[62] DEP'T OF DEFENSE, DICTIONARY OF MILITARY AND ASSOCIATED TERMS JOINT PUBLICATION 1-02 92 (2010) ("Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes.").

[63] Post Staff Report, *Terrorists to Ditch Skype and YouTube After Leaks Reveal NSA Surveillance Tactics*, N. Y. POST (June 26, 2013), http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/.

[64] *Id.*

[65] *Does Skype use Encryption?* SKYPE.COM, https://support.skype.com/en/faq/FA31/does-skype-use-encryption?frompage=search&q=encryption&fromSearchFirstPage=false (last visited Feb. 28, 2014).

[66] *NSA Prism Program Slides*, THE GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.

> Skype is located in Luxembourg (outside of the United States), and . . . [encryption] keys used by Skype cannot be turned over to the FBI because Skype does not hold the keys themselves. The key is only known by the computers using the program to connect with each other, and Internet communication is inherently hard to trace because of how packets can be routed.[67]

As early as 2011, reports described how terrorist use of Skype was hindering law enforcement in India. According to the *Times of India*, "[t]errorist organizations targeting India have moved their communications significantly to Internet and other possible innovative means, denying Indian intelligence agencies any major breakthrough yet in their post-Mumbai blasts investigations." [68] Kashmiri terrorists are reportedly using smart phones and Skype according to a senior Indian Army officer. Terrorists, like the general population, migrate to technologies that enhance communications. The popularity and proliferation of Skype supports the hypothesis that international terror groups have used Skype.

Regardless of the validity of the reports of NSA access to Skype servers or the inability of access to Skype communications, the new attention to alleged Skype vulnerabilities will encourage illicit users to move to other technologies. By exposing real or imagined capabilities of the U.S. Intelligence Community, potential state and non-state targets of electronic surveillance are better equipped to avoid surveillance by avoiding specific technologies and technical services.

One such service is the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. SWIFT, a member-owned cooperative, enables the standardized exchange of proprietary financial data such as payments, securities, and bank commodity trades.[69] Financial transactions, such as those facilitated by SWIFT,

---

[67] Luke Brady, *Talk Like a Terrorist: Use Skype*, UNITED LIBERTY (Nov. 21, 2008), http://www.unitedliberty.org/articles/talk-like-a-terrorist-use-skype (However, *see* Nicole Perlroth, Jeff Larson and Scott Shane, *N.S.A. Able Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&pagewanted=all&_r=0).

[68] Josy Joseph, *Terrorists Move to Skype, Frustrate Eavesdroppers*, THE TIMES OF INDIA (July 19, 2011), http://articles.timesofindia.indiatimes.com/2011-07-19/india/29790655_1_satellite-phones-intelligence-agencies-thuraya.

[69] *See generally* SWIFT COMPANY, www.swift.com (specific information on FIN traffic *available at* http://www.swift.com/assets/swift_com/documents/about_swift/SIF_2013_09.pdf).

are a direct concern to counterterrorism officials. The 9/11 Commission noted, "[v]igorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us understand their network, search them out, and disrupt their operations."[70]

In support of this understanding, an intergovernmental policymaking group established to address money-laundering issues in 1989 expanded its mission to include "identifying sources and methods of terrorist financing and adopted nine special recommendations on terrorist financing to track terrorists' funds."[71] The Financial Action Task Force on Money Laundering, comprising thirty-six member countries, develops and promotes "policies to combat money laundering and terrorist financing."[72]

Because terror financing became a priority well before September 11, 2001, the European Union and the United States began to permit U.S. agencies "limited access to bank data transferred through the SWIFT network."[73] The agreement supported the U.S. Terrorist Finance Tracking Program established after the September 11 attacks.[74] Recent disclosures have focused attention on the data reportedly accessed by the NSA.

In response to this arrangement being made public, the European Union has threatened to "suspend or even terminate the crucial EU-U.S. Terrorist Finance Tracking Programme."[75] The national security impact of this disclosure is the potential loss of an apparently valued source of financial intelligence.[76] The importance of terrorist financing is self-evident. If, pursuant to an international agreement, the NSA had access to international money transfers, it is reasonable to believe

---

[70] 9/11 COMMISSION REPORT, *supra* note 61, at 382.

[71] JAMES K. JACKSON, CONG. RESEARCH SERV., RS21904, THE FINANCIAL ACTION TASK FORCE: AN OVERVIEW AT "SUMMARY" (2012) *available at* https://www.fas.org/sgp/crs/terror/RS21904.pdf.

[72] *Id.* at 1.

[73] Jerin Mathew, *Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift's Interbank Messaging System Breach*, INTERNATIONAL BUSINESS TIMES (Sept. 25, 2013), http://www.ibtimes.co.uk/edward-snowden-nsa-scandal-swift-tftp-eu-508882.

[74] *Id.*

[75] *Id.*

[76] KRISTIN ARCHICK, CONG. RESEARCH SERV., RS22030, U.S.-EU COOPERATION AGAINST TERRORISM (2013) *available at* http://www.fas.org/sgp/crs/row/RS22030.pdf.

that U.S. Intelligence Community was well positioned to interdict the planning and execution of violent actions against the United States or her allies. If financial transfer information becomes unavailable as a result of the illicit disclosures of collection of networks such as SWIFT, then U.S. understanding and ability to prevent terrorist actions is significantly degraded.

Snowden's disclosures have already changed terror group's practices making it more difficult for U.S. intelligence agencies to provide warnings about terror groups' plans and intentions. The loss of insight into these targets diminishes U.S. security, but also prevents the U.S. from sharing information with its allies and partners, diminishing U.S. global influence. The net effect of Snowden's disclosures is to increase terrorist consciousness of their own vulnerabilities. Their response has been immediate and may have a dangerous cumulative effect.[77]

II. FOREIGN RELATIONS

> However the Snowden episode turns out . . . what it mainly illustrates is that we are living in an age of American impotence. The Obama administration has decided it wants out from nettlesome foreign entanglements, and now finds itself surprised that it's running out of foreign influence.[78]

Beyond the national security impact of making terrorist intentions and plans harder to discover and the change in practices of terrorist and opposition groups, Snowden's release of classified information will diminish national security by degrading U.S. foreign relations. American security relies heavily on foreign partnerships that have increased in breadth and scope since September 11, 2001.

Foreign governments are likely to share less information and require more scrutiny of future interactions with U.S. intelligence and no country allegedly targeted for collection is pleased to see the public reports about it. Rising anti-Americanism will strain already tense relationships with countries such as Russia and China; European Union officials have expressed outrage over the Snowden

---

[77] *See generally* GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 121 (2010).

[78] Bret Stephens, *The Age of American Impotence*, WALL ST. J., June 25, 2013, *available at* http://online.wsj.com/news/articles/SB10001424127887324637504578565530512048940.

disclosures.[79] The reports have already distracted the U.S. and Russian delegations during the August 2013 G-20 Summit in Russia during which tensions about Snowden's extradition and asylum status were unresolved.[80]

In addition to diplomatic relationships, U.S. intelligence agencies have extensive relationships with foreign intelligence services. Not only will diplomatic interactions be more difficult, but the intelligence relationships will be challenged as well. U.S. intelligence has good relations with many foreign intelligence services despite what one may read in the press during periods of heightened intelligence interest.

The DNI has the authority to establish intelligence arrangements with foreign governments.[81] The Director of the CIA has a mandate to "conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations . . .. "[82] The Director of the Defense Intelligence Agency is also required to "conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments . . . ."[83] The Director of the NSA has a similar mandate: The Director of the NSA shall "conduct foreign cryptologic liaison relationships . . . . "[84]

Each of these mandated liaison relationships will likely suffer because of the recent disclosures. These relationships can sour if foreign public opinion becomes dissatisfied with U.S. activities that may occur in secret, but with the approval of other heads of state.

---

[79] David Jackson, *Obama, Merkel Agree to Talks on U.S. Spying,* USA TODAY (July 4, 2013, 12:46 PM), http://www.usatoday.com/story/theoval/2013/07/04/obama-merkel-snowden-surveillance-leaks/2488927/.

[80] *See generally* Stephanie Condon, *Obama "Reevaluating" Summit with Russia After Snowden Asylum,* CBSN (Aug. 1, 2013), http://www.cnbc.com/id/100989042 and *Putin, Obama to Meet at G-20 Despite Snowden Flap,* CNBC (Aug. 26, 2013), http://www.cbsnews.com/news/obama-reevaluating-summit-with-russia-after-snowden-asylum/.

[81] Exec. Order No. 12333, *supra* note 32, at § 1.3(b)(4)(A).

[82] *Id.* at § 1.7(a)(5).

[83] *Id.*

[84] *Id.* at § 1.7 (c)(8).

A. *Russia*

The disclosure of alleged intelligence collection may have shifted the balance of moral authority toward Moscow as global awareness of the reported NSA programs proliferated. Russian President Vladimir Putin has been emboldened by the Snowden revelations as illustrated by his actions concerning Syria since the first release of data by *The Guardian* on June 5, 2013.

Russia's goal in Syria before the release of the classified information was to avoid a "[w]estern-backed effort at coercive regime change."[85] Russia has been anxious about the popularity of Islamist groups in predominantly Sunni Muslim countries after the Arab Spring revolutions.[86] Russia attributes the growth of these groups to U.S. attempts to spread democracy throughout the Middle East.[87] Thus, President Putin's political motivations have traditionally been more about domestic stability than about expanding Russia's foreign influence.[88] There was much speculation about how the events in Syria would be addressed by the G-20 summit. Analysts reported that Putin was unlikely to discuss the topic.[89]

Despite this anxiety, Russia was relatively subdued on Syria until after the Snowden revelations. Emboldened by the growing global discontent with the U.S., Putin became more vocal on Syria and on U.S. foreign policy. His most dramatic maneuver was to publish an

---

[85] Samuel Charap & Jeremy Shapiro, *How the US Can Move Russia on Syria,* AL-MONITOR (July 22, 2013), http://www.al-monitor.com/pulse/originals/2013/07/syria-russia-geneva-engagement-peace-process-us-interests.html.

[86] Fiona Hill, *The Survivalist in the Kremlin*, PROJECT SYNDICATE (July 4, 2013), http://www.project-syndicate.org/commentary/putin-s-rigid-approach-to-protecting-russia-by-fiona-hill.

[87] *Id.*

[88] Fred Dews, *What Will Russia Do if the U.S. Strikes Syria*, BROOKINGS INSTITUTE (Aug. 28, 2013), http://www.brookings.edu/blogs/brookings-now/posts/2013/08/28-what-will-russia-do-if-us-strikes-syria (According to Brookings Institute Senior Fellow Cliff Gaddy, "[t]he whole point of their policy on Syria is that they are trying to protect themselves. What they are afraid of is instability. Not really caring that much about who is in power as long as the people in power in the country control the forces within their borders as best they see. I don't think that he has a plan [for Syria] but the overall plan is somehow to protect Russia from the bad things that are happening.").

[89] U.S.-Russia Reporter Roundtable Moderated by Tina Trenkner, Communications Coordinator of Foreign Policy, BROOKINGS INSTITUTE at 11 (Aug. 29, 2013), http://www.brookings.edu/~/media/research/files/interviews/2013/08/29%20us%20russia%20relations/us%20russia%20relations%20g20%20syria%20arms%20control.pdf.

opinion article in the *New York Times* on September 11, 2013. According to Fiona Hill, of the Brookings Institute:

> Russian President Vladimir Putin has done it again, grabbing American and international attention with his *New York Times* op-ed cautioning the United States against the use of force in Syria, and scolding America for considering itself exceptional. Putin's piece has been met with surprise and outrage in the U.S., but its basic message has resonated with groups opposed to a unilateral U.S. strike against regime of Syrian President Bashar al-Assad. Putin has put himself right where he wants to be, at the top of the headlines on Syria, and writing the script for where the United States will have to take the crisis next: Back to the United Nations.[90]

Other circumstances concerning Syria undoubtedly helped encourage Putin to be more vocal,[91] but Russia is viewed by many as having taken the diplomatic high ground against President Obama's threat of military force. It is not difficult to interpret Putin's emboldened message, since he was considering and then granted temporary asylum to Edward Snowden while the debate on Syria was taking shape.

B. *European Union.*

Traditionally, strong diplomatic and intelligence sharing relationships with members of the European Union have also been strained by revelations of programs allegedly collecting the personal

---

[90] Fiona Hill, *Lessons in Communication from Vladimir Putin*, MSNBC (Sept. 14, 2013), http://www.msnbc.com/msnbc/lessons-communication-vladimir-putin#discussions.

[91] "First came the British parliamentary vote blocking Prime Minister David Cameron's initiative to join any U.S. military assault. Then came U.S. President Barack Obama's decision to put the issue to a vote before a reluctant Congress. The French government announced that—unlike in Mali—it would not go it alone in Syria. And United Nations Secretary-General Ban Ki-moon stated that the chemical weapons inspection team he had dispatched to Syria would need time to complete its work before determining whether there was sufficient evidence for the UN to approve the use of force." Fiona Hill, *Putin Scores on Syria: How He Got the Upper Hand –And How He Will Use it*, BROOKINGS (Sept. 6, 2013), http://www.brookings.edu/research/opinions/2013/09/06-putin-scores-syria-hill.

communication of thirty-five heads of state.[92] These reports of U.S. surveillance in Europe are "eating away at the fabric of trust that is part of the alliance."[93] According to the Council on Foreign Relations Senior Fellow Charles A. Kupchan, there is a direct relationship between the political discomfort with alleged U.S. intelligence collection and European disappointment about the President's inability to better balance security and civil liberties.[94] Kupchan has noted that many Europeans feel that Obama "has failed to deliver on his pledge to clean up some of the excesses left behind by the George W. Bush administration."[95]

German Chancellor Angela Merkel originally defended the apparent intelligence cooperation disclosed by Snowden. She pointed out that Germany had "avoided terrorist attacks thanks to information from allies."[96] But, in the face of new disclosures, she is now discussing limits on privacy intrusions. Merkel has alluded repeatedly to "Cold War" tactics and has said spying on friends is unacceptable.[97] Her spokesman has said a mutually-beneficial transatlantic trade deal requires a level of "mutual trust."[98]

Chancellor Merkel has been criticized for her apparently feigned indignation about alleged cooperation with the U.S. Intelligence Community. "Germany has demanded explanations for Snowden's allegations of large-scale spying by the NSA, and by Britain via a programme codenamed 'Tempora,' on their allies including

---

[92] James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, THE GUARDIAN, Oct. 24, 2013, *available at* http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

[93] Bernard Gwertzman, *Interview of Charles A. Kupchan: U.S. Spying Casts Shadow Over Atlantic Alliance*, COUNCIL ON FOREIGN RELATIONS (Oct. 29, 2013), https://secure.www.cfr.org/europe/us-spying-casts-shadow-over-atlantic-alliance/p31745.

[94] *Id.*

[95] *Id.*

[96] *Merkel's Public Indignation a Scam: Snowden Says Germans and Other Western States in Bed with NSA*, SIGNS OF THE TIMES (July 7, 2013), http://www.sott.net/article/263704-Merkels-public-indignation-a-scam-Snowden-says-Germans-and-other-Western-states-in-bed-with-NSA.

[97] *Id.*

[98] *Id.*

Germany and other European Union states, as well as EU institutions and embassies."[99]

The Head of German domestic intelligence has said he knew nothing about the reported NSA surveillance.[100] Opposition parties believe otherwise. They claimed that, because German intelligence activities are coordinated within the Office of the Chancellor, high-level officials must have known about speculative NSA activities.[101] *Der Spiegel* has reported that the NSA monitored about twenty million German phone connections and ten million Internet sessions on an average day and sixty million phone connections on above average days.[102] Thus, unconfirmed U.S. intelligence activities are now an issue that will affect German political leadership and the diplomatic and intelligence relationships between Germany and the U.S.

The impact on European Union allies is already seen in the talks being held between European Union member states and the United States about American surveillance tactics that may have included spying on European allies.[103] President Obama assured Germany that the U.S. "takes seriously the concerns of our European allies and partners."[104]

The initiation of a dialogue between the United States and European Union Members about intelligence collection and appropriate oversight[105] will also complicate the transatlantic relationship. Restrictions or legislation that shifts standards of privacy and data protection will diminish American and European Union security.

C. *France*

Tensions in the European Union are not limited only to Germany. Although not as vocal, the French government has expressed concerns

---

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] Jackson, *supra* note 79.

[104] Laura Smith-Spark, *EU Envoys Meet Over Claims of U.S. Spying on European Allies,* CNN (July 4, 2013), http://www.cnn.com/2013/07/04/world/europe/europe-us-spying/.

[105] Jackson, *supra* note 79.

about U.S. intelligence activity because of the Snowden leaks. In response to allegations that the NSA had collected "more than [seventy] million phone calls in France over a [thirty]-day period," U.S. Ambassador to France, Charles Rivkin, was called to meet with French diplomats.[106] A news release from French President Francois Hollande's office said he expressed his "deep disapproval with regard to these practices" and that "such alleged activities would be unacceptable between allies and friends."[107]

French indignation aside, the disclosures suggest a greater level of French involvement in global electronic surveillance. According to *The Guardian*, the Snowden materials contain high praise for the United Kingdom's GCHQ's French partner, the General Directorate for External Security (DGSE). The French are reported to be a "highly motivated, technically competent partner, who have shown great willingness to engage on [Internet protocol] issues, and to work with GCHQ on a 'cooperate and share' basis."[108] French media, too, has reported that the DGSE is involved in the alleged collection. In early November, *La Jeune Politique* reported on the strained relations between Washington, D.C. and Paris. An article published by *Le Monde*, detailed "the nature of the NSA's probing into France and . . . reported that data on over 70.3 million phone calls and SMS messages had been recorded by the NSA within a [thirty]-day span."[109] These reports "threw diplomatic relations into question and prompted a visit by Secretary of State John Kerry."[110]

American officials also noted the compliance of foreign intelligence services in the collection programs. According to NSA Director Keith B. Alexander, some documents released by Snowden "didn't represent data collected by the NSA or any other U.S. agency and didn't include records from calls within those countries."[111] In

---

[106] Ed Payne & Khushbu Shah, *Report: U.S. Intercepts French Phone Calls on a 'Massive Scale'*, CNN (Oct. 21, 2013), http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying.

[107] *Id.*

[108] Julian Borger, *GCHQ and European Spy Agencies Worked Together on Mass Surveillance*, THE GUARDIAN, Nov. 1, 2013, *available at* http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

[109] Grace Jamieson, *French Intelligence DGSE Implicated in Snowden NSA Leaks* LA JEUNE POLITIQUE (Nov. 9, 2013), http://lajeunepolitique.com/2013/11/09/french-intelligence-dgse-implicated-in-snowden-nsa-leaks/.

[110] *Id.*

[111] Adam Entous & Siobhan Gorman, *Europeans Shared Spy Data With U.S.*, WALL ST. J., Oct. 29, 2013, *available at*

congressional testimony, Alexander noted that the data was "instead from a system that contained phone records collected by the U.S. and North Atlantic Treaty Organization (NATO) countries 'in defense of our countries and in support of military operations.'"[112] He said the conclusion that the U.S. collected the data is incorrect. He also stated, "it's false that it was collected on European citizens."[113]

The disclosures and resulting comments from the U.S. government put French leaders in a difficult political position. Despite their initial vocal protest of U.S. intelligence activities, now it appears as if the French intelligence services were not only in on the collection, but also provided the data to their American and British partners. According to U.S. Secretary of State John Kerry, "France is one of the U.S.'s closest allies" and that France and the U.S. "work together to protect the security of their citizens."[114] If these claims are accurate, then it is safe to assume the collaboration and sharing of intelligence goes beyond those activities illegally disclosed by Snowden.

Assuming that the French do provide intelligence assistance to and data sharing with NATO, GCHQ, and the NSA, the political pressures may be so strong as to curtail that assistance and sharing. If the media reports about French technical collection capability, the positive GCHQ assessment of French intelligence abilities, and General Alexander's statements about the reasons for intelligence relationships are all true, then any reduction in intelligence and data sharing will reduce the effectiveness of French, United Kingdom, European Union, NATO, and U.S. intelligence operations. If the current pressures result in less sharing or more restricted information exchanges between France and the U.S., then U.S. national security is impacted.

Some predict that the discomfort with the public disclosure of critical intelligence activities will result in the establishment of new norms of intelligence-gathering within the Atlantic Alliance. Rules such as "no snooping on officials above a certain level; or no significant intelligence gathering without informing the intelligence agency of the other side" are being considered.[115] There is current legislation in the European parliament that seeks to "tighten privacy

---

http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502.

[112] *Id.*

[113] *Id.*

[114] Payne & Shah, *supra* note 106.

[115] Gwertzman, *supra* note 93.

laws and make it more difficult for Europeans to share information with non-European companies like Google and Facebook."[116] This will make intelligence more difficult and more expensive to collect, also impacting U.S. national security.

D. *Latin America*

Snowden's illegal disclosures have impacted U.S. national security by weakening foreign relations not only with Russia and Western Europe, but also in Latin America. Threats to U.S. national security from Latin America remain significant. "Economic stagnation, high rates of violent crime and . . . ruling party efforts to manipulate democratic institutions to consolidate power, and slow recovery from natural disasters are challenging [security measures]."[117] Countries hostile to the U.S., such as Iran, have been expanding their influence in Latin America and the Caribbean.[118]

Threats from illicit narcotics trafficking emanate primarily from the Western Hemisphere. Mexico and Colombia are source countries for the majority of illegal drugs consumed in the U.S., according to the DNI. Illicit trafficking continues to undermine U.S. security. Some of the highest violent crime rates are found in Honduras, El Salvador and Guatemala. "In addition, weak and corrupt institutions in these countries foster permissive environments for gang and criminal activity, limit democratic freedom, encourage systemic corruption, and slow recovery."[119] National security threats are abundant in Latin America, and recent illegal disclosures of classified information will not help diplomatic or intelligence sharing relationships with permissive or corrupt governments.

The disclosures have impacted U.S. national security relationships with Latin America, particularly Brazil. Good intentions over the past three years to establish a trade deal and Brazilian membership in the

---

[116] *Id.*

[117] *Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm.*, *supra* note 27, at 26.

[118] *Id.* President Ahmadinejad traveled to the region twice in 2012. Tehran has cultivated ties to leaders of the Venezuelan-led Alliance for the Peoples of our Americas (ALBA) in Bolivia, Cuba, Ecuador, Nicaragua, and Venezuela, and maintains cordial relations with Cuba and Nicaragua. Relations with Tehran offer these governments a way to stake out independent positions on the international issue of Iran, while extracting financial aid and investment for economic and social projects.

[119] *Id.*

United Nations Security Council have been unsuccessful. Brazil's President Dilma Vana Rousseff has stated that each country has much to gain from deepening coordination with the United States. It is reasonable to assume, given the threats to stability and the illicit narcotics trafficking from Latin America, that the U.S. Intelligence Community has a partnership with Brazil. If true, then the disclosures by Snowden will complicate this cooperation. According to the *New York Times*, "[d]iplomatic ties have also been damaged, and among the results was the decision by Brazil's president, Dilma Rousseff, to postpone a state visit[120] to the United States in protest over revelations that the agency spied on her, her top aides and Brazil's largest company, the oil giant Petrobras."[121] Although an apology[122] may be enough to have salvage the trade deal, other issues continue to strain the relationship between Washington and Brasília.

According to the Council of Foreign Relations, the Snowden scandal, the White House "response to it and President Dilma Rousseff's decision to cancel the state visit has [sic] revealed the weakness of the U.S.-Brazil relationship."[123] Snowden's disclosures are now spawning an effort within Latin America to strengthen protections against alleged NSA collection. "According to the AP, Brazilian Foreign Minister Luiz Alberto Figueiredo said, '[w]e're going to talk with our partners, including developed and developing nations, to evaluate how they protect themselves and to see what joint measures could be taken in the face of this grave situation.'"[124]

Not only is U.S. national security affected by reactions in Brazil, but U.S. commercial interests as well. According to the *Los Angeles*

---

[120] Brian Winter, *Exclusive: Brazil's Rousseff Wants U.S. Apology for NSA Spying*, REUTERS (Sept. 4, 2013), http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904 (Rousseff was due to make a formal state visit to Washington . . . to meet U.S. President Barack Obama and discuss a possible $4 billion jet-fighter deal, cooperation on oil and biofuels technology, as well as other commercial agreements).

[121] Eric Schmitt & Michael Schmidt, *Qaeda Plot Leak Has Undermined U.S. Intelligence*, N.Y. TIMES, Sept. 29, 2013, *available at* http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=all&_r=0.

[122] Winter, *supra* note 120.

[123] Julia E. Sweig, *The 'Postponement' Requires Hard Truths*, COUNCIL ON FOREIGN RELATIONS (Sept. 25, 2013), http://www.cfr.org/brazil/dear-president-dilma/p31379.

[124] Peter Grier, *Are Edward Snowden NSA Leaks Messing up US Foreign Relations*, CHRISTIAN SCIENCE MONITOR (Sept. 3, 2013), http://www.csmonitor.com/USA/DC-Decoder/Decoder-Buzz/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

Times, President Rousseff is "promoting legislation that would require technology companies such as Google and Facebook to store data collected in Brazil on Brazilian soil and therefore submit it to Brazilian law."[125] In addition, Brazil is now planning to develop a secure e-mail system to improve the security of government communications against American spying. Ironically, "President Dilma Rousseff used the secure messaging channel on Twitter to make the announcement that she's going to order SERPRO—that country's federal data processing service—to implement a whole-of-government secure e-mail system."[126]

The reaction in Brazil over the illegal disclosures about alleged surveillance illustrates the diplomatic impact of the disclosure of classified information. The relationships with Latin American trade and diplomatic partners will continue to be tense because of the Snowden leaks. According to the *National Security Strategy*, the "strategic partnerships and unique relationships we maintain with Canada and Mexico are critical to U.S. national security and have a direct effect on the security of our homeland."[127] Thus, Snowden's actions will continue to degrade critical U.S. diplomatic and information sharing relationships.[128]

E. *Pakistan*

The U.S.' relationship with Pakistan has been "tragic and often tormented."[129] The country's internal instability, complex tribal dynamics, and political ideology have threatened U.S. security and international peace. Pakistan's rapidly growing population, "nuclear arsenal, and relationships with China and India will continue to force it onto the United States' geostrategic map in new and important ways over the coming decades."[130] With respect to diplomatic relations with

---

[125] Kathleen Hennessey & Vincent Bevins, *Brazil Postpones State Visit to U.S. Over Snowden Spying Leaks*, L.A. TIMES, Sept. 17, 2013, *available at* http://www.latimes.com/world/worldnow/la-fg-wn-ff-brazil-us-edward-snowden-spying-leaks-20130917,0,5186201.story#axzz2jmpqWim6.

[126] Richard Chirgwin, *Brazil Whacks PRISM With Secure Email Plan*, THE REGISTER (Oct. 14, 2013), http://www.theregister.co.uk/2013/10/14/brazil_waxes_lyrical_on_security/.

[127] NATIONAL SECURITY STRATEGY, *supra* note 25, at 42.

[128] Grier, *supra* note 124.

[129] Daniel Markey, *No Exit from Pakistan*, COUNCIL ON FOREIGN RELATIONS (Oct. 2013), http://www.cfr.org/pakistan/no-exit-pakistan/p31250.

[130] *Id.*

the United States, Islamabad is primarily concerned with Afghanistan and the consequences of the rapidly shrinking U.S. military presence.[131]

The Obama Administration claims that al-Qaeda remains centered in Pakistan and that this core "remains the most dangerous component of the larger network . . ."[132] Threats to U.S. national security will increase if the country's governance and security regress to historical levels, if the Taliban maintains control of sections of Afghanistan, and al-Qaeda is not neutralized. According to the *National Security Strategy*, "[t]o prevent future attacks on the United States, our allies, and partners, we must work with others to keep the pressure on [al-Qaeda] and increase the security and capacity of our partners in [Afghanistan and Pakistan]."[133]

Beyond the al-Qaeda threat, the DNI is concerned about the future economic issues in Pakistan. With a very limited tax base, poor tax collection system, and reliance on U.S. foreign aid, the country has no promise of economic growth. These economic circumstances can encourage corruption and the acceptance of terrorist groups who provide much needed currency.[134]

It is undeniably wise to collect intelligence in regions from which these types of national security threats can originate. According to *The Washington Post*, there are intelligence gaps concerning the security of Pakistan's nuclear program, chemical and biological weapons capabilities, and the "loyalties of counterterrorism sources recruited by the [CIA]."[135] These concerns are so pervasive that budget documents are reported to divide the world into two illicit weapons categories: Pakistan and everybody else.[136]

An illegally disclosed summary of the U.S. Intelligence Community's budget allegedly indicates a significant increase in

---

[131] *See generally Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm.*, *supra* note 27, at 18.

[132] NATIONAL SECURITY STRATEGY, *supra* note 25, at 20.

[133] *Id.*

[134] *Worldwide Threat Assessment: Hearing Before the House Permanent Select Comm.*, *supra* note 27, at 18.

[135] Greg Miller, Craig Whitlock & Barton Gellman, *Top-Secret U.S. Intelligence Files Show New Levels of Distrust of Pakistan*, WASH. POST (Sept. 2, 2012), http://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_print.html.

[136] *Id.*

intelligence activities against Pakistan. This increase may indicate a substantial level of distrust of Pakistan. "They also reveal a more expansive effort to gather intelligence on Pakistan than U.S. officials have disclosed."[137] Husain Haqqan, a former Pakistani ambassador to the United States, supports this belief: "If the Americans are expanding their surveillance capabilities, it can only mean one thing. The mistrust now exceeds the trust."[138]

The loss of trust can complicate cooperation with Pakistan intelligence services, restrict intelligence sharing between the two countries, and thus reduce the security of both the U.S. and Pakistan.

The Snowden disclosures are undermining an already tense relationship between the U.S. and Pakistan. The illegal disclosures will likely reduce intelligence sharing and military cooperation at a time when threats for both countries are still extremely grave. The disclosures have diminished U.S. national security by damaging the diplomatic and intelligence relationship with a key ally in a region from whence one of the greatest attacks against the U.S. originated.

The diplomatic and intelligence relationships established over the past sixty years have been critical to the security of the U.S. national security is proportionally linked to cooperation with other nations. The quantity and quality of intelligence sharing with foreign intelligence services can reduce the burden and expense on U.S intelligence agencies. Regardless of the veracity of the information illegally disclosed by Snowden, the tensions it is causing in foreign relations negatively impact the intelligence sharing and cooperation with partner nations. Less sharing and cooperation equals reduced national security for the United States.

Intelligence relationships with foreign security services support good partnerships between the United States and the partner nation. These relationships facilitate U.S. access to areas where the U.S. could not otherwise go. Partners can offer intelligence agility with an ability to collect information that may take longer in the U.S. They provide local insight to a particular target with expertise not resident in the U.S. Intelligence Community. And relationships with foreign intelligence services may provide cover for U.S. interests by masking American action under their domestic security or military organizations.[139] These advantages have been placed at risk by the recent disclosures of sensitive information.

---

[137] *Id.*

[138] *Id.*

[139] Eric Rosenbach & Aki J. Peritz, *Confrontation or Collaboration? Congress and the Intelligence Community*, HARVARD KENNEDY SCHOOL (July 2009) *available at*

III. COMMERCIAL

Diplomatic and intelligence cooperation between nations is vital to U.S. national security, but so too is the cooperation between the private and public sectors within the U.S. Policy and technology developments over the past sixty years have diminished the capacity of the U.S. government to be first to develop state-of-the-art technology. This has not always been the case. According to the Intelligence and National Security Alliance:

> Throughout the history of U.S. intelligence, there has been a necessary partnership between government, the private sector, and academia to enhance research, development, manufacturing, and fielding of systems that support the intelligence mission. A broad range of innovations including the earliest computers and dynamic spaceborne collection systems resulted from this partnership.
>
> Through careful attention and nurturing of these partnerships, impressive cutting-edge technologies were developed and utilized on projects including the U-2, SR-71, CORONA overhead collection systems and the CRAY supercomputers.[140]

Most major defense contractors claim to support intelligence programs throughout the Intelligence Community.[141] Because the U.S. national security apparatus apparently depends so heavily on the private sector, any damage to that relationship will have a corresponding negative impact on national security. It appears as if the illegal disclosures by Snowden are diminishing national security by causing a rift between high-tech firms and the NSA.

---

http://belfercenter.ksg.harvard.edu/publication/19153/intelligence_and_international_cooperation.html.

[140] INTELLIGENCE AND NATIONAL SECURITY ALLIANCE, CRITICAL ISSUES FOR INTELLIGENCE ACQUISITION REFORM: INDUSTRY'S ASSESSMENT OF THE INTELLIGENCE COMMUNITY ACQUISITION PROCESS 1 (Oct. 2008) *available at* http://www.insaonline.org/i/p/a/i/d/a/Index.aspx?hkey=d73d5c3e-80a5-492b-9fd5-2f7caab8b8da.

[141] *See generally* BOOZ ALLEN HAMILTON, http://www.boozallen.com (last visited Jan. 25, 2014); NORTHROP GRUMMAN, http://www.northropgrumman.com (last visited Jan. 25, 2014); LOCKHEED MARTIN, http://www.lockheedmartin.com (last visited Jan. 25, 2014); GENERAL DYNAMICS, http://www.gd-ais.com (last visited Jan. 25, 2014).

A letter sent last year by six leading technology companies illustrate this rift. On October 31, 2013 Facebook, Google, Apple, Yahoo, Microsoft and AOL urged the White House to "work with Congress in addressing . . . critical reforms that would provide much needed transparency and help rebuild the trust of Internet users around the world."[142] These companies evidently believe that current surveillance practices require re-examination: "Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs."[143]

This call for reform—perhaps motivated more by corporate interests than national security interests—may result in less access to information, less cooperation between the public and private sectors, and more bureaucratic demands on the Intelligence Community when accessing data that has little or no impact on the privacy of U.S. citizens. As noted by the first Assistant Secretary for Policy at the Department of Homeland Security and former General Counsel at the NSA Stewart Baker, "[i]n the long run, any effective method of ensuring privacy is going to have to focus on using technology in a smart way, not just trying to make government slow and stupid."[144] Companies such as Facebook, Google, Apple, Yahoo, Microsoft and AOL handle so much global data and continue to create new ways with which to connect, it is unwise to undermine any speculative partnership with these and similar private companies. Information sharing is already a challenging enough issue for the public and private sectors.

The same principles described by the *9/11 Commission Report* concerning information within the government, apply to information sharing between the government and the private sector:

> But the security concerns need to be weighed against the costs. Current security requirements nurture over-classification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks . . . but few

---

[142] Letter from Facebook, Google, Apple, Yahoo, Microsoft and AOL, to The Honorables Leahy, Lee, Conyers, and Sensebrenner (Oct. 31, 2013) *available at* http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf.

[143] *Id.*

[144] Baker's book has enlightened commentary on the privacy issue. STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 314 (2010).

> rewards for sharing information. There are no punishments for not sharing information. Agencies uphold a need-to-know culture of information protection rather than promoting a need-to-share culture of integration.[145]

The current version of the ideas described more than ten years ago could be that data available to corporations is overly protected and excessively compartmented within the private sector. Each company and government agency should incentivize sharing when national security is at risk. There should be liability for not providing information, rather than liability protections for sharing information with the U.S. government. Both public and private sectors must adopt a culture of integration.

The most recent and likely legislation promoting insufficient, but improved information sharing was S. 2105, The Cybersecurity Act of 2012.[146] This bill, like many other before it, failed to become law because of mutual mistrust between the government and private sector and a suspicion of mutual incompetence.[147] Enhanced information sharing, whether under S. 2105 or any other bill, would have contributed to national security. Because of the disclosures by Snowden, there is now no appetite in Washington to pursue any information exchange between the national security apparatus and corporate America. According to *The Washington Post*:

> The tone of industry reaction to the NSA revelations has grown more aggressive since the first stories appeared in *The Washington Post* and Britain's *Guardian* newspaper in June. Companies that initially were focused on defending their reputations gradually began criticizing the government and challenging it in court. Some companies also have worked to harden their networks against infiltration. A turning point came with *The Washington Post* revealed an NSA program that collects user information from Google and Yahoo as it moves among data centers overseas. To

---

[145] 9/11 COMMISSION REPORT, *supra* note 61, at 417.

[146] S. 1551, 113th Cong. (2013).

[147] *See generally*, Charles Abbott, Cyb*ersecurity Bill Dead after Second U.S. Senate Rebuff*, REUTERS (Nov. 14, 2012), http://www.reuters.com/article/2012/11/15/us-usa-cyber-legislation-idUSBRE8AE04720121115.

> some, this amounted to a degree of intrusiveness that, though speculated about by privacy activists, was beyond what many in the industry thought possible.[148]

Snowden's disclosure of classified information has not only chilled the relationship between Silicon Valley and the U.S. government, but also it has damaged the bottom line for American technology firms. According to *The World Post*, recent losses for Google, Cisco, and AT&T can be attributed to the alleged role of American technology companies in the Snowden scandal.[149] "Election officials in India canceled a deal with Google to improve voter registration. In China, sales of Cisco routers dropped [ten] percent in a recent quarter. European regulators threatened to block AT&T's purchase of the wireless provider Vodaphone."[150] With their bottom lines at risk, it is understandable that American technology companies would distance themselves from the U.S. government. Given the history of cooperation between American industry and American government, this distance is bad for national security, bad for American business and bad for the U.S. citizens because technological advancement will be slower and will take longer to penetrate various sectors of the economy.

The national security impact is clear: Less cooperation between the U.S. national security departments and agencies will result in less and more difficult access to data and less and more difficult access to technical innovation.

IV. PUBLIC CONFIDENCE

The American National Security Strategy "begins with a commitment to build a stronger foundation for American leadership, because what takes place within our borders will determine our strength and influence beyond them."[151] What is taking place within

---

[148] Craig Timberg & Ellen Nakashima, *Amid NSA Spying Revelations, Tech Leaders Call for New Restraints on Agency*, THE WASH. POST (Oct. 31, 2013), http://www.washingtonpost.com/world/national-security/amid-nsa-spying-revelations-tech-leaders-call-for-new-restraints-on-agency/2013/10/31/7f280aec-4258-11e3-a751-f032898f2dbc_print.html.

[149] Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions*, THE WORLD POST (Jan. 24, 2014), http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html.

[150] *Id.*

[151] NATIONAL SECURITY STRATEGY, *supra* note 25, at 2.

our borders in response to the disclosures of potentially classified information is reducing U.S. national security by undermining public confidence in the NSA, the Intelligence Community, and the federal government. The daily media indictments of one of the premier intelligence agencies in history is disrespectful to the thousands of American citizens who work at the NSA, and has presented the public with an inaccurate image of Intelligence Community oversight. The loss of public trust resulting from amateur media analysis and by Snowden's actions is already damaging national security by distracting national security professionals from their jobs. In our democracy, reductions in public support and agency credibility will inevitably result in fewer resources, reduced authority, and additional scrutiny. For students of national security history, this portends a pendulum swing back to less information sharing, less authority to collect intelligence vital to U.S. national security, and a reversion to less sharing of information within the U.S. government and with foreign allies.

According to a Pew Research poll conducted shortly after the first illegal disclosures by *The Guardian*, "for the first time since 9/11, Americans are now more worried about civil liberties abuses than terrorism."[152] According to Pew, fifty-six percent of Americans believe U.S. federal courts have inadequately limited counter-terrorism telephone and Internet data collection by the government.[153] "An even larger percentage [seventy percent] believes that the government uses this data for purposes other than investigating terrorism."[154] These data show the misunderstanding of the value of the alleged NSA programs, despite congressional testimony and declassified documents that demonstrate that these programs have stopped violent attacks against the United States and its allies. Regardless of the value of the disclosed activities, the political reaction has been swift.

President Obama announced in early August that reforms were coming for NSA surveillance. Section 215 of the USA Patriot Act and the role of the Foreign Intelligence Surveillance Court are now under

---

[152] Glenn Greenwald, *Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy*, THE GUARDIAN, July 26, 2013, *available at* http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew.

[153] *Id.*

[154] Pew Research Center for People and the Press, *Few See Adequate Limits on NSA Surveillance Program*, PEW RESEARCH (July 26, 2013) http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

review. "Obama wants to let a civil liberties representative weigh in on the court's deliberations to ensure that an adversarial voice is heard and will form a high-level group of outside experts to review the U.S. surveillance effort."[155] The President has also ordered the declassification of many documents surrounding the collection of data in the hope of restoring the public trust damaged by the recent disclosures.

Congress has also announced its own reforms. The Intelligence Oversight and Surveillance Reform Act,[156] introduced by Senators Ron Wyden, Mark Udall, Richard Blumenthal, and Rand Paul, will "prohibit bulk collection of Americans' records, shield Americans from warrantless searches of their communications and install a constitutional advocate to argue significant cases before the secret Foreign Intelligence Surveillance Court."[157] No action has been taken on the bill since its introduction on September 25, 2013.

Congress has also considered an amendment to the Defense Appropriations bill that would restrict the NSA's access to data.[158] It was the first legislative challenge to programs that the White House, the ODNI, the Department of Justice, and the NSA have claimed have stopped violent attacks against the U.S. The amendment was defeated by twelve votes in the House of Representatives sending a clear message to the Obama Administration that there is anxiety about the program. "Though the amendment barely failed, the vote signaled a clear message to the NSA: [W]e do not trust you."[159]

The Snowden disclosures may also have larger implications for other elements of the U.S. government. As a consequence of the

---

[155] Steve Holland & Jeff Mason, *Obama Says Reform Ahead for NSA Surveillance Program*, MILWAUKEE WISC. J. SENTINEL (Aug. 9, 2013), http://www.jsonline.com/news/usandworld/obama-begins-news-conference-addresses-nsa-b9972397z1-219024921.html.

[156] S. 1551, *supra* note 146.

[157] Press Release, Senator Ron Wyden: Surveillance Reform Package Ends Bulk Collection of Phone Records; Creates Constitutional Advocate for Secret Court (Sept. 25, 2013) *available at* http://www.wyden.senate.gov/news/press-releases/surveillance-reform-package-ends-bulk-collection-of-phone-records-creates-constitutional-advocate-for-secret-court.

[158] *See generally*, Justin Amash, *Amash NSA Amendment Fact Sheet*, U.S. Representative Justin Amash (July 24, 2013), *available at* http://amash.house.gov/speech/amash-nsa-amendment-fact-sheet.

[159] Alan Grayson, *Congressional Oversight of the NSA is a Joke. I Should Know, I'm in Congress*, THE GUARDIAN, Oct. 25, 2013, *available at* http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight.

disclosures, Congress and the executive branch considered placing a political appointee at the head of the NSA and separating the roles of Director, NSA and Commander, U.S. Cyber Command. Although the President rejected these options, it appears as if dramatic shifts in well-functioning structures would be considered because of the sensational media coverage and political pressure.

With the reduction in potential legal authority for the NSA, public sentiments against NSA surveillance that has contributed so much to national security, and the pressures that are a consistent feature of budget negotiations, can reductions to the NSA budget be far behind? With less money, less authority, and less credibility, the NSA will soon have fewer people, less data, and a weakened ability to contribute to national security. According to top agency counsels, reforms under consideration may reduce Americans privacy in an effort to enhance it.[160] Lawyers from the Intelligence Community are now arguing against certain reforms, in support of the status quo.[161]

Perhaps it was inevitable that the national security apparatus constructed since 9/11 would be dismantled when Americans no longer view the threat to the U.S. as starkly as they did on September 11, 2001. Amid seeming crises of political dysfunction, government shutdowns, and persistent unemployment, perhaps the public no longer sees al-Qaeda, Iran's nuclear program, Muslim extremism, and nuclear proliferation as providing the NSA a sufficient justification to access metadata.

As noted by lawyer, diplomat, writer, and philosopher Joseph de Maistre, "[e]very nation has the government it deserves."[162] If the citizens of the American republic demand a reduction in their own security as a result of actions taken in violation of laws their representatives established, then we will not only get the government we deserve, but also the level of security we have chosen.

V. CONCLUSION

Regardless of the legitimacy—or lack thereof—of Snowden's actions, the material he has revealed in violation of law, regulation, and oath has placed U.S. security at risk. The disclosures have resulted in significant damage to diplomatic relationships with countries that

---

[160] John Hudson, *Top Obama Lawyers: Reforming the NSA Could Hurt Americans' Privacy,* FOREIGN POLICY BLOG (Nov. 4, 2013), http://thecable.foreignpolicy.com.

[161] *Id.*

[162] JOHN BARTLETT, BARTLETT'S FAMILIAR QUOTATIONS 353 (Justin Kaplan ed., 17th ed. 2003).

share intelligence with the U.S., damage to domestic commercial relationships between the U.S. public and private sectors leading to less information sharing and innovation, and damage to the public confidence in the NSA leading to fewer resources and authority to protect the U.S. in the manner that it has done so since 9/11. The disclosures will also facilitate operational changes in the behavior of current adversaries' practices and attention to the protection of their information. It will become more difficult, more expensive, and more time consuming to collect and analyze information on terrorist groups, foreign governments, and foreign militaries.

Our Republic is resilient and will survive the exposure of the "plumbing" of the NSA's intelligence apparatus.[163] Surviving will be more dangerous, more expensive, and take more time than reforms would have required absent Snowden's illegal activities. Just as Snowden must do on his own, we must all ask ourselves if the transparency that he has forced onto the system is worth the diminishing of American security.

---

[163] *See generally* comments from Michael V. Hayden during the Washington Post Live's Cyber Summit. *Defending Our Data: Can Government and Industry Work Together?* WASH. POST (Oct. 3, 2013), http://www.washingtonpost.com/postlive/conferences/cybersecurity-2013/.