BRENNAN
CENTER
FOR JUSTICE

STRENGTHENING INTELLIGENCE OVERSIGHT

Foreword by Hon. Walter F. Mondale & Hon. Gary Hart

Edited by Michael German

Endorsed by Former Church Committee Staff Members

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving Constitutional protection in the fight against terrorism. Part think-tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect Constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on government transparency and accountability; domestic counterterrorism policies and their effects on privacy and First Amendment freedoms; detainee policy, including the detention, interrogation, and trial of terrorist suspects; and the need to safeguard our system of checks and balances.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE CHURCH COMMITTEE

Following a series of public revelations of far-reaching government abuse in the 1970s, the Senate established the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly referred to as the "Church Committee") to conduct the nation's first comprehensive investigation of intelligence activities. The bipartisan Church Committee uncovered systematic government abuses of intelligence authorities and recommended significant reforms and oversight mechanisms to curb future abuse, including oversight committees in both the House and the Senate. Forty years later, however, intelligence scandals are again eroding public confidence in our national security. Former Church Committee members and staff are now calling for a new comprehensive investigation into intelligence activities with the hope of establishing oversight mechanisms that address a changing technological and legal landscape.

ABOUT THE EDITOR

Michael German is a fellow with the Brennan Center for Justice's Liberty and National Security Program. His work focuses on law enforcement and intelligence oversight and reform. Prior to joining the Brennan Center, Mr. German served as policy counsel for the American Civil Liberties Union Washington Legislative Office and as a special agent with the Federal Bureau of Investigation, where he specialized in domestic terrorism and covert operations. His first book, "Thinking Like a Terrorist: Insights of a Former FBI Undercover Agent," was published in 2007. Mr. German graduated from Northwestern University School of Law, and graduated *cum laude* from Wake Forest University with a B.A. in Philosophy.

ACKNOWLEDGEMENTS

The Brennan Center gratefully acknowledges The Atlantic Philanthropies, C.S. Fund, Democracy Alliance Partners, Ford Foundation, and Open Society Foundations for their generous support of the Liberty & National Security Program.

This report reflects the intial efforts of the Brennan Center and its Liberty and National Security Program. The Church Committee staff members especially thank Michael German and Frederick A. O. Schwarz, Jr. for their drafting, Faiza Patel for her guidance, and Shannon Parker for her coordination. In addition, the Church Committee staff members thank Elizabeth Goitein, Seth Hoy, John Kowal, Jim Lyons, Desiree Ramos Reiner, and Michael Waldman for their invaluable input and assistance.

CHURCH COMMITTEE STAFF MEMBERS

Former Church Committee staff members involved in this report include:

David Aaron

Frederick Baron

Joseph Dennin

James Dick

John Elliff

Peter Fenn

Karl F. "Rick" Inderfurth

Loch Johnson

Elliot Maxwell

Paul Michel

William Miller

Christopher Pyle

Gordon Rhea

Eric Richard

Frederick A. O. "Fritz" Schwarz, Jr.

Patrick Shea

Athan Theoharis

Burton Wides

TABLE OF CONTENTS

FOREWORD

*By Hon. Walter F. Mondale and Hon. Gary Hart**

Forty years ago, Congress established a select investigative committee charged with conducting a thorough, bipartisan examination of our government's secret intelligence operations undertaken over the course of several presidential administrations. It represented the first time our nation — or any nation to our knowledge — opened its national security apparatus to such independent and public scrutiny. We are honored to have served on that Committee, under the skilled leadership of the late Sens. Frank Church and John Tower, and with the support of a talented and dedicated staff.

Our work was conducted with the recognition that effective intelligence capabilities are essential to ensuring our national security and developing sound foreign policies. But these operations, like all government activities, must comply with the law. We concluded that much of the error and abuse we found resulted from excessive secrecy that forfeited the strengths of our constitutional system: the value added by the input of informed overseers in Congress and the courts, and the public support earned through democratic accountability.

Today, intelligence activities are back in the news, too often for the wrong reasons. Many Americans are questioning whether the structural reforms developed as a result of the Church Committee investigation remain sufficient to ensure intelligence activities are properly tailored to meet their objectives without infringing on individual rights or betraying American values.

Eighteen Church Committee staff members have assembled once again to produce this insightful report calling for a comprehensive re-evaluation of our systems of intelligence oversight. Their effort could not be more critical or timely. The scope and complexity of our intelligence operations has grown exponentially, and recent revelations about mass surveillance programs and the abuse of detainees in U.S. custody confirm that existing controls are not as effective as they need to be.

This 40th anniversary of the formation of the Church Committee provides an opportunity to reassert our Founders' confidence that our national security can be most effectively maintained with robust systems of democratic accountability. We applaud the efforts of the Church Committee staff members for their continuing contribution to this critical national debate.

* *Mondale served as a U.S. Senator from Minnesota and Vice President of the United States. Hart served as a U.S. Senator from Colorado. Both were members of the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Operations, 1975-76.*

I. INTRODUCTION

In the early 1970s, a series of leaks and other disclosures of covert intelligence operations revealed illegal, inappropriate, and unethical activities involving the Federal Bureau of Investigation, the Central Intelligence Agency, the U.S. military, and even the White House, shocking many Americans. At the height of the Cold War, maintaining effective intelligence capabilities was essential to our nation's security. But these scandals eroded public confidence that our military, intelligence, and law enforcement agencies operated in a manner that respected the law, democratic accountability, and American values, which undermined their ability to accomplish their crucial missions. Congress was compelled to act.

In 1975, the U.S. Senate established the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly referred to as the "Church Committee") to conduct the nation's first comprehensive public examination of intelligence community activities since World War II. Led by Sens. Frank Church (D-Idaho) and John Tower (R-Texas), the Committee's bipartisan efforts exposed systematic executive branch abuses of authority that were enabled by excessive secrecy and a lack of effective internal governance or independent external controls. Based upon the Church Committee's recommendations, Congress and the executive branch established several significant reforms designed to establish constitutionally-based checks and balances over intelligence activities and curb future abuse.

More than 40 years later, however, new revelations about the nature and scope of U.S. intelligence activities undertaken since the terrorist attacks of September 11, 2001 — from mass surveillance to torture — have sparked outrage at home and abroad, and led to new calls for comprehensive reform.

Much has changed since 1975. Technological innovations and increasing globalization are creating new risks and vulnerabilities, even as they give the intelligence agencies and their private sector partners astonishing capabilities to monitor and catalogue essentially every detail of modern life. The intelligence enterprise, a $70 billion per year industry,[1] has grown significantly, with more than 5 million employees and contractors now holding security clearances. While counterterrorism remains a priority and the war in Afghanistan grinds on, global threats are only increasing and diversifying. The U.S. renewed its military engagement in Iraq and expanded it to Syria. Political unrest threatens Ukraine, Somalia, Sudan, Nigeria, Israel, Yemen, Libya, and Iraq, just to name a few, and the global economic recession has emerged as a significant national security issue. These diverse threats necessitate unprecedented levels of international coordination and cooperation on security matters, making the maintenance of trusted relationships among partner nations and adherence to international legal standards even more essential to our mutual safety.

Lawful, properly controlled intelligence activities are critical to our national security. But they require public support, which can only be achieved through sound governance, independent oversight, and public accountability. To this end, several former Church Committee staff members signed a letter last year requesting that Congress establish a new special investigative committee to conduct a thorough public re-examination of intelligence community authorities and practices, and their impact on privacy and civil liberties. While recent investigations by the Privacy and Civil Liberties Oversight Board and the President's Review Group on Intelligence and Communications Technologies are extraordinarily helpful and will undoubtedly inform this new committee's work, they focused on just a few intelligence collection programs.[2] Only a comprehensive examination of how the multitude of intelligence

programs, agencies, and authorities work in combination can measure the cumulative effect on privacy and civil liberties, ensure compliance with the law, and identify waste and redundancy that undermines performance.

Moreover, as important as the Privacy and Civil Liberties Oversight Board and President's Review Group investigations are, it is the constitutional responsibility of Congress, as a co-equal branch of government and the direct representatives of the people, to restore the public trust in U.S. intelligence programs. The Senate Intelligence Committee's five-year inquiry into the CIA's abusive detention and interrogation practices provides a striking example of the diligence Congress can apply in meticulously scrutinizing covert government activities, and preparing a report suitable for public release. But it also exposes its limits. The summarized report details how the CIA successfully frustrated oversight of its torture program for several years by refusing, delaying, or inappropriately limiting congressional briefings, and providing incomplete, inaccurate, and misleading information to its overseers. The resources necessary to conduct such an investigation of one program within one agency reveal the depth of the challenge Congress faces in fulfilling its intelligence oversight responsibilities.

Congress needs to demonstrate its ability to check executive branch overreach across the multiple programs and agencies, re-establish democratic controls over intelligence policies, and ensure public accountability of intelligence practices. As part of a comprehensive review of the intelligence enterprise, Congress must examine its own performance in overseeing all 17 intelligence community member agencies, including the Federal Bureau of Investigation, the Central Intelligence Agency, the Drug Enforcement Administration, intelligence components of the Departments of Defense (including the National Security Agency), State, Treasury, Energy, and particularly the more recently established Department of Homeland Security.[3] The purpose of such a review should be to evaluate whether current legal controls and congressional oversight structures and practices are effective in allocating intelligence resources properly and efficiently; to check agency abuses; and to adequately inform all members of Congress and the American public about the scope, necessity, and effectiveness of all authorized intelligence activities, to the greatest extent possible.

To their credit, both the House and Senate have periodically reviewed various aspects of their oversight operations to assess how to improve them. But their day-to-day duties of monitoring burgeoning, complex intelligence collection, counterintelligence, and covert action is extremely time consuming for committee members, even apart from their other congressional responsibilities. It would not be realistic for them to also undertake the kind of comprehensive and integrated review of the myriad intelligence oversight issues we raise below.

The Church Committee's work is perhaps best remembered for exposing significant wrongdoing by the intelligence agencies, often secretly authorized by presidents of both political parties, which undermined American freedoms and democratic values. But its lasting legacy was providing Congress with the factual foundation and legal framework for crafting appropriate organizational structures and constitutional controls to ensure that intelligence operations remain effective, lawful, and consistent with our national interests. Examining whether the controls and structures created four decades ago remain an effective bulwark against error and abuse is necessary and appropriate. And the growing mistrust of U.S. intelligence activities at home and abroad make it essential.

II. WHY A NEW COMPREHENSIVE EXAMINATION OF THE INTELLIGENCE ENTERPRISE IS NECESSARY

A. What Has Changed

1. Significant Growth of the Intelligence Community

As the Church Committee noted in its final report, the need to guard against the tendency of government to overreach in the name of national security intensifies in times of crisis. The terrorist attacks of September 11, 2001, by a loose network of non-state actors presented a different and in many ways more difficult operational challenge for an intelligence apparatus originally built to address Cold War threats. Congress responded by quickly passing the USA Patriot Act, significantly amending the complex array of legal authorities governing both domestic and foreign intelligence collection, and increasing funding for this rapidly growing enterprise.[4] The wars in Afghanistan and Iraq imposed considerable new demands, as the intelligence agencies had to quickly adapt and reorganize to understand and interdict a more nebulous and nimble enemy.

The intelligence agencies also swelled their ranks by incorporating state and local law enforcement and other government and non-government entities into federal intelligence operations, and engaging a multitude of private sector contractors to expand their labor force. Today there are more than 5 million security-cleared government employees and contractors working in the military-intelligence enterprise.[5] A 2010 report by *The Washington Post* identified more than 1,200 government entities and over 1,900 private companies working in some capacity on counterterrorism, homeland security, and intelligence.[6] The number of cleared individuals with access to the volumes of sensitive information poses a heightened risk of abuse and unauthorized disclosures. Moreover, this rapid growth challenges the capacity of existing oversight and accountability structures, particularly where private contractors and other non-government entities are involved.

It is critical for Congress and the American people to understand whether the intelligence community is using its new resources and authorities responsibly and effectively, and whether the structures set up to check abuse remain sufficient in light of current circumstances. Much has changed since the post-Church Committee reforms were put into effect. The expanded size and scope of today's intelligence enterprise alone is enough to justify a new comprehensive examination by Congress. But other developments make the need for such a review even more urgent.

2. Technological Advances

The Church Committee warned that continuing technological developments would increase the government's surveillance capabilities in ways that could challenge Congress's ability to anticipate problems and check abuse.[7] Breathtaking achievements in the U.S. information technology and computing industries have since revolutionized global communications, giving billions of people around the world instant access to information and services, spurring innovation and international commerce, and facilitating the free expression of ideas. Rather than embracing a free and secure Internet

as an unprecedented open source of foreign intelligence and a tool for empowering democracy around the world, the intelligence agencies capitalized on their technological superiority to satisfy short-term intelligence goals.

American companies' dominant roles in providing Internet services, software, and networking infrastructure gave them unprecedented access to vast amounts of domestic and international electronic communications and commercial transactions. Unfortunately, our intelligence agencies secretly initiated warrantless domestic surveillance programs under presidential orders, in defiance of Congress's expressed intent that the Foreign Intelligence Surveillance Act serve as the "exclusive means" for foreign intelligence collection in the United States. The intelligence agencies seem to have prioritized collecting all they could, rather than only what they needed. The long-term consequences of these decisions are only beginning to be realized and important questions remain unresolved. One is whether such massive data collection is a necessary or effective method of identifying and interdicting national security threats, or whether the influx of information actually diverts resources and obscures the most important data. Another is whether the intelligence oversight mechanisms established in the 1970s remain effective checks against overreach and abuse in an era of such rapid technological innovation.

Telecommunications are not the only field in which new technologies have fueled the expansion of privacy-intrusive surveillance, too often with little regulation or public debate. Surveillance cameras in public spaces and private venues have become ubiquitous, and new technologies, such as the "domain awareness" system the NYPD developed with Microsoft,[8] promise greater integration of video data from multiple sources. Continuing progress in facial recognition software is making it easier to identify and track individuals across these different surveillance systems. The FBI's Next Generation Identification program is combining millions of criminal and non-criminal photographs with other biometric identifiers such as fingerprints, iris scans, and DNA in the largest database of its kind.[9] As more businesses require pre-employment background checks, the number of non-criminals included in this FBI database will continue to grow.

In addition to helping the government identify who people are, technology is making it easier for both the government and private companies to know where they've been. License plate readers, EZ Passes, GPS, and cell phone tracking technologies are creating enduring electronic records detailing many Americans' daily travels. The FBI and DHS have both been using unmanned drones for surveillance, with little public notice or oversight, and local law enforcement agencies are increasingly seeking to use them too.

Intelligence agencies are pursuing "big data" analytic tools that will allow more thorough exploitation of the massive volumes of data they are collecting through these various surveillance platforms, compounding the privacy risks of any single surveillance activity. Permissive information sharing practices between and among the government agencies and private companies increase the risk of misuse and abuse of Americans' personal information. If nothing else, the Snowden leaks show the NSA's internal controls were insufficient to protect the data it collected.

These collection and analysis programs do not just pose privacy problems. Federal law enforcement agencies have also reportedly adopted a practice of "parallel construction" to mask the methods by which they collect information used in criminal prosecutions.[10] The purpose is allegedly to hide the true sources

from defendants and judges, so their legality cannot be challenged in court. If true, this practice would amount to a violation of defendants' due process rights and potentially involve a fraud upon the court, undermining the very laws these agencies are sworn to uphold.

The U.S. Supreme Court is beginning to recognize that rapid technological developments alter the applicability of longstanding Fourth Amendment doctrines. Recent cases found warrantless use of GPS tracking devices on vehicles traveling on public roadways and warrantless police searches of cellular phones incident to arrest unconstitutional. In both cases, Justice Samuel Alito appealed to Congress to provide legislative guidance for law enforcement and intelligence agencies operating in the digital environment, rather than relying entirely on the courts to balance the privacy impact of new and developing technologies against the government's law enforcement and national security interests.

The government's aggressive exploitation of technology to expand intelligence collection opportunities also appears to have created new security vulnerabilities. The Snowden leaks revealed that the NSA undermined encryption standards and worked with tech companies to build "back doors" in software and hardware so it could bypass Internet security mechanisms. It also secretly trafficked in hacker tools and methodologies that allowed security vulnerabilities it identified to go unaddressed, leaving the public at risk. Deliberately weakening the cybersecurity infrastructure puts all Internet users at greater threat of cyber attacks and data thefts from hackers, criminals, and hostile foreign agents.

Congressional oversight committees are responsible for understanding and evaluating how the intelligence agencies are currently exploiting existing technologies, anticipating how developing technologies might necessitate additional regulation and scrutiny, and ensuring they have the technical expertise to perform these functions.

3. Increasing Globalization

It is not just communications that are more globally connected and integrated today. Increased international trade, finance, and travel make today's world more interconnected and interdependent, rendering the longstanding distinctions between U.S. persons and foreigners in our surveillance laws more difficult to manage and less meaningful. Millions of Americans live and work abroad, and tens of millions of foreign tourists and immigrants come to the United States each year. Foreign multinational corporations increasingly hire and invest in the United States, and vice versa. Other Americans might never have traveled outside of their cities or states, but their email, banking, or medical insurance records might be stored on servers in India or Ireland due to information technology outsourcing.

On the one hand, globalization creates new opportunities to expand political and economic freedom around the world and enhance peace and understanding across cultures. But it also creates vulnerabilities, facilitating transnational criminal activities, weapons proliferation, and the spread of infectious disease. Establishing and maintaining cooperative strategic relations with foreign nations and honoring human rights and international legal norms has therefore become ever more important to preserving domestic security. As the International Covenant on Civil and Political Rights, which the U.S. ratified in 1992, affirms: "the inherent dignity and ... the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."[11]

Failure to properly restrain intelligence gathering activities abroad in compliance with international law and treaty agreements risks the potential loss of cooperation and access to important data sets. In 2006, *The New York Times* revealed the CIA and U.S. Treasury Department had been given secret access to bank transfers through the international financial system SWIFT (Society for Worldwide Interbank Financial Telecommunicatoin) in violation of European privacy laws.[12] These public revelations led to years of negotiations, finally resulting in a 2010 treaty agreement between the U.S. and the European Union to regulate financial data transfers through the Terrorist Financial Tracking Program.[13] When it was discovered in 2013 that NSA continued to intercept SWIFT data in violation of the treaty, the European Parliament voted to suspend the program, potentially denying the U.S. information necessary to curb terrorist financing.[14]

Intelligence activities perceived as violating international privacy rights also threaten long term U.S. economic interests, as foreign markets seek ways to avoid U.S. surveillance. The perceived cooperation of U.S. tech companies in NSA surveillance operations is expected to cost an estimated $35 billion in lost foreign investment in the U.S. cloud computing market by 2016.[15] The "balkanization" of the Internet by countries seeking to defeat U.S. spying by keeping data about their citizens within their own borders would further increase costs to U.S. tech companies operating in foreign markets, and sharply limit the economic efficiencies promised by the evolution to cloud-based services.[16] The democratizing benefits of a free and open Internet would also be lost.[17] Additionally, the loss of access to and communications with people residing in authoritarian countries would also harm our intelligence efforts.

The President's Review Group criticized the intelligence agencies for failing to conduct proper risk management evaluations prior to initiating covert programs. It argued that risks to privacy, civil liberties, Internet freedom, foreign relations, and international commerce had to be considered alongside risks to national security the program was designed to address.[18] It recommended a "Front-Page Rule," which would require an assessment of whether the American people would find the proposed intelligence activity necessary and proper if it appeared on the front page of the newspaper.[19] In addition, the Review Group proposed measuring how the targeted foreign government might react upon learning the same information, against the value of the intelligence obtained. German Chancellor Angela Merkel's anger over allegations the NSA tapped her personal cellphone likely inspired this advice, but the criticism could also apply to the NSA's aggressive expansion of its programs even after Americans expressed concerns over the warrantless wiretapping program. The recent arrests in Germany of two CIA spies, which led to the expulsion of the Berlin CIA station chief,[20] indicates the intelligence agencies have practical and legal problems from spying on allies.

Part of Congress's oversight responsibility includes assisting the intelligence agencies in conducting this type of pre-operational cost-benefit analysis. Members of Congress often have a much greater awareness of and appreciation for the breadth of U.S. interests involved in international relations, and the patience for taking a long-term approach that many working in the national security and intelligence professions do not. Not surprisingly, given the nature of their jobs, national security officials have a tendency to view potential threats as imminent and favor action over deliberation, which is what leads to a focus on resolving short-term problems without appropriately considering the long-term impact.

4. Demand for Reform at Home and Abroad

Many Americans and U.S. allies were shocked and angered to learn the extent of U.S. spying activities revealed by the Snowden leaks and have demanded reform. Reviews by the Privacy and Civil Liberties Oversight Board and the President's Review Board questioned both the legality and wisdom of the programs and recommended significant changes. President Obama responded to the criticism by issuing a presidential policy directive slightly narrowing some domestic and foreign intelligence collection programs and by calling for more lasting statutory reform. Several members of Congress have introduced legislation to end or limit some or all of the collection programs Snowden illuminated, but no statutory reforms have been enacted to date.

President Obama and Director of National Intelligence James R. Clapper, Jr. have both said they welcomed a public debate regarding the proper legal limits of government surveillance, but continuing secrecy obscures the scope of current spying operations. Legislation that would have limited NSA data collection passed unanimously through two committees in the House of Representatives but was severely weakened by House leadership in closed-door meetings with Obama administration officials before it was brought to the floor for a vote.[21] Continuing ambiguity surrounding the government's interpretation of key terms in the proposed legislation made it unclear whether the proposed reforms would impose sufficiently meaningful restraints, which weakened support. The bill ultimately failed.

The resistance to engaging in a frank public discussion about the government's view of its legal authorities, and to establishing clear limits to future collection, only breeds public cynicism that could undermine sincere reform efforts. What is clear is that the intelligence agencies have many programs that remain secret, including electronic surveillance operations based outside the U.S. that are not overseen by Congress or the FISA Court and would not be impacted by any of the proposed legislative reforms.

In contrast, the international community has begun to take action. In March 2014, the European Parliament voted to strengthen European privacy rights over data shared with companies outside the EU, and passed a resolution delaying a U.S. trade agreement over concerns about NSA spying.[22] In June 2014, the United Nations High Commissioner for Human Rights issued a report affirming that privacy in digital communications was a human right protected under international law. The report condemned a "transnational network of intelligence agencies [operating] through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes" as unlawful and a breach of human rights obligations.[23] The U.S. government's aggressive foreign intelligence surveillance practices jeopardize its role as a leader in promoting human rights and democracy in the international community.

5. Decades of Intelligence Oversight to Evaluate

Long before Snowden's leaks raised the issue to public prominence, Congress's performance in overseeing the intelligence community had come under withering scrutiny. The National Commission on Terrorist Attacks on the United States (the "9/11 Commission") described congressional oversight of intelligence and counterterrorism as "dysfunctional" and called for an overhaul, including

creating a joint intelligence committee to replace the separate House and Senate committees, and consolidating homeland security oversight to one committee.[24] As a potential alternative to the joint committee, the 9/11 Commission recommended combining intelligence authorization authority with appropriations in a single committee in each house.[25]

In 2005, these recommendations were seconded by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which also offered several "more modest suggestions."[26] In 2008, another Commission (on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism) concluded, "[t]he current structure of congressional oversight of national security is a relic of the Cold War [that] has not evolved in response to the changing nature of the threats that the United States faces in the 21st century."[27] In 2014, at the 10 year anniversary of the 9/11 Commission recommendations, the Bipartisan Policy Center lamented the continuing failure of Congress to embrace significant structural reforms, noting that the number of committees and subcommittees to which DHS reported had grown from 88 to 92 in the time since the 9/11 Commission report was issued.[28]

It is certainly possible that responsible members of Congress could conclude that these commissions' recommendations for structural reorganization of intelligence oversight are not the proper solutions. Indeed, since one of the original purposes of establishing the intelligence committees was to help keep the entire Congress fully and currently informed about intelligence matters, reducing the number of committees with intelligence oversight responsibilities could further compartmentalize information. Reducing the number of committees, and therefore the number of legislators the intelligence and homeland security officials are required to report to, might also add to the perception that the overseers are victims of regulatory capture, and end up serving more as agency "cheerleaders" rather than watchdogs.[29] Nonetheless, it is incumbent upon Congress to examine whether the current committee structure optimizes intelligence oversight or whether changes should be made.

6. Increasing Secrecy Undermines Checks and Balances

Even members of the intelligence committees have complained that excessive secrecy undermines their oversight efforts. *The New York Times's* exposure of the government's "warrantless wiretapping" program in 2005 revealed Congress had not been adequately informed about the NSA's post-9/11 collection activities. Despite a statutory requirement that the executive ensure that the intelligence committees are "fully and currently informed" about all intelligence activities, the Bush administration limited notifications regarding the NSA program to the "gang of four" — the chairs and ranking members of each intelligence committee — a procedure not authorized in the law.[30] One of those briefed, Sen. Jay Rockefeller (D-W. Va.), later complained the administration's secrecy demands "prevented members of Congress from conducting meaningful oversight of the legal and operational aspects of the program."[31] Another, Rep. Jane Harman (D-Calif.), went further, claiming the "gang of four" notifications a violation of "the specific requirements of the National Security Act of 1947." While the Act authorizes limited "gang of eight" notifications (adding House and Senate leadership to the four intelligence committee leaders), this provision applies only to "extraordinary circumstances" involving "covert actions," not intelligence collection programs.[32]

In fact, Harman argued that even the statutory "gang of eight" briefings render congressional oversight ineffective because members "cannot take notes, seek the advice of their counsel, or even discuss the issues raised with their committee colleagues."[33] While Rockefeller and Harman place the blame for the breakdown of effective congressional oversight on the executive's improperly limited notifications and secrecy demands, Congress in general and the gang of four (or eight) in particular could equally be criticized for going along with them. Congress has ample tools available, including the power of the purse, to ensure that it receives timely and accurate information necessary to perform its legislative and oversight functions.

The New York Times's exposure in 2005 of the NSA warrantless wiretapping also revealed that the Bush administration failed to seek FISA Court approval for the programs as required by the statute, though administration officials secretly notified two FISA Court judges about the programs at some point after implementation. These judges did not attempt to stop the programs, and in 2004 one judge even issued a secret opinion authorizing the government to collect metadata about Americans' domestic Internet usage in bulk under an expanded interpretation of FISA.[34] The 2005 leak led to a new series of secret accommodations with the FISA Court, which then authorized the bulk collection of U.S. telephony metadata. When the FISA Court finally balked at the programmatic interception of the content of international communications, Congress acquiesced to executive branch demands by passing the 2008 FISA Amendments Act.

Though the Patriot Act and FISA Amendments Act were debated in public, most Americans (and even some members of Congress) did not know the scale of collection taking place under these authorities. Sen. Ron Wyden (D-Ore.), an intelligence committee member, often warned that the government secretly interpreted FISA provisions in ways that significantly widened its powers.[35] But it was not until Snowden leaked thousands of classified documents describing the surveillance programs — and the FISA Court opinions that authorized them — that the public, Congress, and the courts were able to meaningfully participate in the debate. The 2013 Snowden disclosures showed that government officials had often mischaracterized both the scale and effectiveness of its activities to Congress, the FISA Court, and the public.

The documents also revealed that the government repeatedly failed to comply with the legal restrictions that Congress and the FISA Court imposed on its programs, which it blamed on misunderstandings regarding the complex technologies involved and the different rules governing the various programs. Though the opinions show the FISA Court struggled to rein in these programs, Judge Reggie Walton later acknowledged the court had no ability to conduct independent oversight of the intelligence agencies and relied entirely on self-regulation and reporting by the agencies.[36] Congress should ascertain whether the FISA Court has the staff and other resources needed to be independent and effective. Further, Congress should evaluate whether the FISA Court, with its limited capacity and lack of adversarial process to assist in factual development, is the proper venue to judge the constitutionality of secret government programs it cannot fully evaluate.

The Senate Intelligence Committee's CIA torture report revealed similar agency attempts to frustrate oversight by Congress and the courts.[37] According to the report, the CIA "actively avoided or impeded" congressional oversight by improperly delaying notification that it was using coercive interrogation

techniques; only briefing committee chairmen, vice chairmen, and their staff directors; refusing to answer questions for the record; and providing incomplete and inaccurate information about the program's implementation and management.[38] Because of the manner in which these limited briefings were conducted, neither the CIA nor the Committee retained records fully describing the matters discussed.[39] The CIA did not brief the full Committee on the program until September 2006, four years after it was implemented and only shortly before President Bush publicly acknowledged it.[40] According to Sen. Dianne Feinstein (D-Calif.), when the Senate Intelligence Committee investigation began its investigation in 2009, the CIA placed arduous constraints on committee staff's access to documents, searched their computers without warrants, and attempted to intimidate them with criminal referrals to the Justice Department.[41]

The CIA also fought in the courts to prevent public accountability over its interrogation program, arguing that even acknowledging that documents existed would "cause serious damage to the national security of the United States."[42] Meanwhile, the CIA was surreptitiously providing information about the still-classified program to journalists in an attempt to manipulate media coverage regarding the effectiveness of its interrogation practices.[43] A CIA attorney reviewing the CIA's media campaign said it "makes the [legal] declarations I made to the court a work of fiction."[44]

Congress is responsible for ensuring that all intelligence activities are effective, narrowly tailored to meet national security needs, and compliant with the law and American values. In a democracy based on the informed consent of the governed, the maximum amount of information that can be responsibly made available to the voters directly, or indirectly through their elected representatives, should be disclosed. Given the continuing public furor over the Snowden revelations and the CIA's torture program at home and abroad, it is crucial that Congress recognize that the current oversight structures are inadequate. It is time for Congress to conduct a thorough, public evaluation of its performance over the decades to determine whether more compelling structural reforms are required.

B. What Hasn't Changed

While the significant changes in the environment the intelligence agencies operate in makes a comprehensive review necessary, it is what has not changed that should guide the direction of the re-examination. The Church Committee's study of the history of intelligence activities in the United States confirmed three essential truths that we believe are still evident.

First, personal privacy is essential to liberty and the pursuit of happiness. "When Government infringes on [individual] rights instead of nurturing and protecting them, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated,"[45] the Church Committee wrote. In today's globalized environment, the potential chill on political and economic activity caused by arbitrary invasions of privacy threaten to harm important national interests in advancing democracy and economic freedom.

Second, the intelligence community needs to operate within the law and in a way that reflects American values. Accurate and timely intelligence is necessary to secure our nation and its people from a diversity of threats. But intelligence activities that undermine democratic processes and the rule of law threaten

national security over the long term. In the words of James Madison, the father of our Constitution, popular government can only exist with public information. In our democracy, there can be no secret law or secret interpretation of the law that empowers the government to invade the privacy or liberty of the people.

Third, Congress is responsible for establishing structures and systems to ensure our intelligence agencies are effective and operate within the law. Our Constitution gives Congress robust authority to regulate, investigate, and curtail improper or unauthorized executive branch intelligence activities. Oversight of intelligence has come a long way since the Church Committee issued its recommendations, and Congress is far more informed and involved in intelligence policy and practices. But the intelligence community has also grown in both size and reach, challenging an oversight structure designed decades ago to address far different threats. A public report reflecting the results of a rigorous and nonpartisan investigation of the effectiveness of the current systems of intelligence is necessary to restore public confidence.

III. USING THE CHURCH COMMITTEE AS A MODEL FOR A NEW EXAMINATION OF INTELLIGENCE ACTIVITIES

The success of the Church Committee holds many lessons for those that would attempt a similar undertaking today. It conducted a thorough public examination of secret intelligence operations that revealed unnecessary, flawed, and abusive activities. At the same time, it won public support for reform while still protecting properly classified information and retaining the trust of the intelligence community.

Certainly, many of the Committee's achievements can be attributed to the leadership of Sens. Frank Church and John Tower, who ran the investigation in a strictly bipartisan manner. Defining the scope of the investigation to include intelligence activities undertaken under the authority of presidents of both parties helped to alleviate any claims the Committee's criticisms were partisan.

Since the intelligence activities now under public scrutiny have spanned the terms of two presidents of different parties, conducting a rigorous examination unaffected by party politics should be similarly achievable.

The form a new investigative committee takes, whether a select committee, joint committee, or one of the standing committees currently assigned government oversight responsibilities, is ultimately less important than the issues on which it focuses. The Church Committee identified three main departures from our constitutional system of checks and balances that contributed to intelligence abuse. These included excessive executive power over intelligence matters, too much secrecy, and an inclination of some intelligence officials to avoid the rule of law.

Congress needs to evaluate whether its current intelligence oversight structures and practices effectively meet the challenge of these potential departures from our founding principles.

A. Checking Excessive Executive Power

A comprehensive re-evaluation of congressional oversight structures and methods should address the following concerns:

1. Historically, the executive branch tends to consolidate power during national security emergencies. Has Congress taken effective steps to ensure it continues to meet its constitutional obligations as a co-equal branch of government to oversee and check executive actions?

Under our constitutional system, government functions best when the three branches of government protect their own powers and aggressively check the powers of the others when challenged. The Church Committee found Congress often failed to exercise proper oversight of intelligence activities, which contributed to abuses of authority. At times the executive was to blame for intentionally withholding information from Congress. But Cold War fears also led to undue congressional deference to the

executive in matters of national security. While oversight of intelligence has vastly improved due to the reforms Congress implemented, the expansion and diversification of intelligence authorities and capabilities during this continuing post-9/11 national security crisis have tested whether these reforms remain effective. A comprehensive examination of intelligence, law enforcement, homeland security, and national defense activities could determine where gaps have developed and how Congress might more effectively execute its constitutional mandate.

2. The intelligence community has expanded significantly in both the size and scope of its activities. Have congressional resources kept pace to maintain effective oversight?

Congress needs to ensure it has sufficient well-trained staff and resources to evaluate the many reports it receives from the agencies, inspectors general, Congressional Research Service, Government Accountability Office, and outside interest groups, and still conduct daily oversight of a global intelligence enterprise. Congressional oversight committees must also keep the other members of Congress fully and currently informed. While this is an enormous task, Congress has recently taken some small but important steps to increase its capacity to audit and investigate intelligence agencies. Congress clarified the Government Accountability Office's authority to audit intelligence community agencies, overcoming strong resistance from the Obama administration and the agencies. The Government Accountability Office has been effective at evaluating the costs and effectiveness of government programs to ferret out waste, fraud, and abuse, and the intelligence agencies could clearly benefit from independent examination.

Congress also created a statutory intelligence community inspector general with broad access to employees and activities of all intelligence agencies and components, and the responsibility to coordinate activities with agency inspectors general and regularly report to Congress.[46] This office should provide the intelligence community with additional internal controls and Congress with a new source of information about intelligence activities.

Congress modified its procedures to better coordinate intelligence appropriators with the House and Senate Intelligence Committees. Each chamber took a different approach, so the investigation should examine which is more effective, and whether more radical changes would give Congress better control over funding for intelligence operations it finds problematic. The Senate Intelligence Committee also removed term limits for its members with the belief that this would allow senators on the Committee to gain deep experience that could improve oversight. Term limits were originally required to ensure senators rotated off the intelligence committee, so they could bring their knowledge of intelligence matters to their work on other committees, thereby improving the knowledge base of the entire body. Some fear the removal of term limits will make the committee more insular and leave the rest of the Senate less informed about intelligence.

3. The technological revolution has increased the power and reach of the intelligence agencies. Does Congress have sufficient access to cleared independent technologists that can evaluate the impact of new developments?

In 1997, the Senate Intelligence Committee established a volunteer Technical Advisory Group made up of government and non-government experts in many scientific fields to provide technical assistance and advice.[47] Although it is essential that the Committee receive expert advice, particularly regarding advances in science and technology, it is equally important that the Committee hear a diversity of opinions. There is very little public information regarding who comprises the Technical Advisory Group, how its members are selected and vetted for conflicts of interest, or how the Committee evaluates the advice they provide. The lack of transparency regarding the Technical Advisory Group raises questions about who influences intelligence policy decisions. Particularly as the public expresses concerns about the symbiotic relationship between the intelligence community and the U.S. tech industry in the wake of the Snowden leaks,[48] establishing a transparent process for selecting members to the Technical Advisory Group becomes critical. The intelligence committees should ensure they hire staff with technical expertise. They should provide them with appropriate clearances, so that the committee members have a trusted source to vet the arguments and evidence provided by outside experts.

4. The Church Committee recommended that Congress assert control over intelligence agencies by issuing legislative charters that circumscribe agency authorities, yet this was not fully realized. Would creating a legislative charter for the FBI and NSA, and a new charter for the CIA (after 68 years), give Congress more control over these agencies?

The Justice Department forestalled legislative efforts to establish a statutory charter for the FBI by issuing Attorney General Guidelines in 1976 to limit its investigative authorities. These guidelines were amended several times over the years, including four times under the Bush administration alone. The investigators should examine whether Congress could provide greater guidance and stability to the FBI and the other agencies by issuing statutory charters. The NSA, a Defense Department agency, has never had a legislative charter. Now that the NSA is gathering, analyzing, and processing an enormous amount of U.S. persons' data, the argument for congressional regulation of its activities is greater.

B. Challenging Excessive Secrecy

1. Secrecy is often necessary to successful intelligence programs, but excessive secrecy can be harmful to a democratic society. As the representatives of the people, members of Congress have an obligation to be our eyes and ears, giving us the information we need to evaluate government activities. Does Congress provide the American public and our allies enough information to accurately assess the national security threat environment and evaluate our national security policies?

An evaluation of congressional oversight should examine whether the intelligence and homeland security committees are able to get the information necessary to properly guide intelligence activities and inform the rest of Congress, and the public, so that sound policies can be enacted. Congress has recently modified some aspects of its oversight authority to strengthen its ability to obtain information about intelligence activities from the executive. After the controversy regarding the inadequacy of the "gang of four" notifications about the warrantless wiretapping program, Congress modified the "gang of eight" notification provision of the National Security Act of 1947 to require the executive submit written explanations to justify limiting disclosure, with notice to the full committee members within

180 days.[49] The investigators should examine whether these reforms have been sufficient and whether further measures are necessary.

Expanding the intelligence committees' access to information about intelligence activities is only the first step in challenging excessive secrecy, however. The intelligence committees are also responsible for ensuring that all members of Congress are properly informed about the nature and scope of government activities to the greatest extent possible, so that they may properly execute their legislative, appropriations, and oversight obligations. Moreover, intelligence, law enforcement, homeland security, and national defense policies can only remain effective if they retain the support of the American people and our allies. Congress must ensure the public has adequate access to information to evaluate the necessity and propriety of these critical programs to ensure that both our security and our liberties are protected.

Sen. Charles Grassley (R-Iowa) told *Politico* that the 10-year "mystery" over NSA spying contributed to the public skepticism about the program: "Our government, and maybe I'm at fault too, because we don't do enough oversight, but there's a lot more that could have been made public. If there had been more information out there, there would have been less suspicion and not all these questions being raised."[50] An informed public is the strength of a democracy, not a threat to it.

2. Excessive secrecy is also a direct threat to national security. What is Congress doing to reduce overclassification, which squanders intelligence resources, impedes information sharing, promotes leaks by eroding respect for the classification system, and denies the public access to information it can use to better evaluate national security policy?

The 9/11 Commission warned that the "systemic resistance to sharing information" is the largest impediment to sound intelligence analysis, but our "[c]urrent security requirements nurture over-classification and excessive compartmentalization of information."[51] Congress has done next to nothing to address over-classification, even as the amount of classified information produced has skyrocketed since 9/11.[52]

3. Excessive secrecy is impeding the courts from acting as a bulwark against government excess, to the detriment of individual rights and public confidence in our legal system. How can Congress strengthen the courts' ability to hear and resolve constitutional challenges to intelligence practices?

The Bush and Obama administrations have used the state secrets evidentiary privilege not just to protect discrete pieces of properly classified information from disclosure in civil cases, but as an immunity doctrine, demanding the dismissal of lawsuits alleging torture, extraordinary rendition, and even FBI spying on Americans in Southern California.[53] In cases challenging the constitutionality of the FISA Amendments Act, the Justice Department sought dismissal based on the argument that because the government's surveillance took place in secret the plaintiffs could not prove they had been spied on.[54] Congress should examine how it can empower the courts so judges can properly protect classified evidence while allowing lawsuits to proceed using unclassified information, particularly constitutional challenges to intelligence activities.

C. Enforcing and Strengthening the Rule of Law

1. In a Democracy, There Can Be No Secret Law

Judge James Robertson, who served on the FISA Court from 2002 to 2005, told the Privacy and Civil Liberties Oversight Board that the FISA Amendments Act fundamentally changed the nature of the FISA Court. He said: "[W]hat the FISA process does is not adjudication, it is approval … [This] process works just fine when it deals with individual applications for surveillance warrants … [but the 2008 amendment] turned the FISA Court into something like an administrative agency which makes and approves rules for others to follow."[55] Worse, the FISA Court makes these rules, which impact the privacy and civil liberties of many Americans, in complete secrecy. The Obama administration claimed that FISA Court decisions could not be made public because the interpretations of the law were so closely bound to the specific facts of the secret investigations.[56] Once Snowden leaked several of the opinions to the press, it became apparent this was not true. Rather, it was the scope of the government's interpretation of its authorities that the administration and the FISA Court wanted to hide. Indeed, the administration subsequently declassified and released several other partially-redacted opinions, making clear the FISA Court's legal analysis could be released without harm. Congress should examine how it can modify the FISA process to make it more transparent and accountable.

But FISA is only one source of secret law. Congress should examine a multitude of sources, including Office of Legal Counsel opinions, unpublished regulations and presidential policy directives, redacted opinions in Article III courts, and secret international agreements, to ensure that the public knows what the law is and retains the right to challenge it.

2. Intelligence Officials Must be Held Accountable for False Statements to Congress and the Courts

The desire to keep the government's interpretation of its surveillance authorities secret from the public led several intelligence agency officials to make false statements to Congress, the FISA Court, and even the Supreme Court. A notable example was Director of National Intelligence James Clapper's response to Sen. Ron Wyden's question about whether the NSA has any programs that collect information about millions or tens of millions of Americans. Clapper's response, "no, not wittingly," was proven false by the Snowden leaks just weeks later.[57] FISA Court opinions from 2009 and 2011 revealed that intelligence officials repeatedly misled the court about the scope and operations of its programs.[58] In arguing that a constitutional challenge to the FISA Amendments Act should be dismissed on standing grounds, the solicitor general falsely stated (perhaps unwittingly) that other potential plaintiffs would have standing because Justice Department policy was to notify defendants if the government intercepted their communications under the statute. In fact, the Justice Department policy at that time prevented such notifications.[59] The truth was not revealed, even to the solicitor general apparently, until well after the Supreme Court dismissed the lawsuit for lack of standing. None of these officials faced any consequences from these false statements.

Nothing will undermine public confidence in government more than the perception that government officials can make false or misleading statements with impunity. If the intelligence agencies' secrecy demands require the creation of secret systems of oversight, government officials appearing before these bodies are obligated to provide full and truthful answers to any and all questions asked of them. Congress must make clear that the law applies equally to everyone.

IV. CONGRESS NEEDS TO DEVELOP METRICS TO EVALUATE THE EFFECTIVENESS OF NATIONAL SECURITY POLICIES AND PROGRAMS

The Privacy and Civil Liberties Board's report on the government's intelligence activities under the FISA Amendments Act included a recommendation that the government "should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs."[60] It would be improper for any government agency to operate major programs without evaluating their effectiveness, much less agencies with such important security missions. Congress must fill the void and, in consultation with the agencies, develop metrics to measure the performance of all intelligence, law enforcement, and homeland security programs. In conducting such an evaluation it is important to recognize, as the President's Review Group suggested, that all risks must be considered and addressed.

A. Impact on Individual Rights

As the Church Committee reported, most intelligence activities take place in secret, and the victim of abusive government activity may never know the source of his misfortune.[61] The scope of today's mass surveillance programs threaten everyone's privacy rights by their mere existence, and potentially chill free speech and association, particularly over the Internet. The President's Review Group highlighted these concerns, identifying privacy as a "central aspect of liberty" that must be protected.[62] Legislators with responsibility over intelligence, law enforcement, and homeland security programs owe a special obligation to ensure these activities do not infringe on individual rights.

B. Impact on Other Interests

Other important interests to protect include our relations with foreign nations. Treating allies with respect is essential, of course, but the rule of law should be our guide even when dealing with adversaries. American values should not just be something we talk about. Our actions in the international arena will set an example for other nations, so we must ensure that our actions match our words.

Congress is also responsible to ensure the taxpayers' money is spent wisely, so the financial costs of the programs must be weighed against their effectiveness. Waste, fraud, and abuse in these programs does real harm to our security, not just the bottom line. And spending government resources on security measures means other priorities cannot be addressed. There are also other ancillary economic consequences of intelligence activities, which U.S. tech companies are currently experiencing as a result of the global response to NSA surveillance activities.[63]

Government officials working in the national security field have a natural tendency to overestimate near-term threats and favor quick and decisive action to address them. As policymakers responsible for a broad range of national interests, Congress must be more deliberative and compel these agencies to consider the long-term impacts of their activities.

C. Cost-Benefit Analysis

Finally, these costs must be measured against the benefits, which are often much harder to evaluate. If an agency overestimates a potential threat, then employs expensive and intrusive means to deter it, does the fact that the threat did not materialize mean the methods were effective? After more than a dozen years of war, pervasive surveillance, infringements on liberty, as well as trillions of dollars spent and thousands of soldiers lost, can we tell if Americans are any safer or more prosperous? Congress must develop its own ability to independently evaluate the threats we face and the proper means to address them to ensure all the interests of the American people are being served, including the right to be free from unwarranted government interference.

V. CONCLUSION

A comprehensive evaluation of U.S. intelligence activities and the effectiveness of congressional oversight is necessary to ensure compliance with law and American values. This is not a partisan matter. Members of both parties have expressed deep concerns about recent revelations and joined to propose legislative controls. Nor is it a matter of inevitable legislative-executive conflict. Over the long term, the executive branch has a great interest in having Congress, and, to the extent possible, the public, understand what intelligence is all about — and how it may affect Americans' private lives as well as our national security.

The Church Committee was formed by a newly elected Congress at a moment when the public demanded answers. Four decades later, 2015 offers a similar opportunity for Congress to engage seriously with the intelligence challenges of the 21st century.

ENDNOTES

1 The total intelligence budget is a combination of the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). In fiscal year 2014 the NIP was $50.5 billion, and the MIP $17.4 billion, for a total intelligence budget of $67.9 billion. This figure represents a decrease from the record high $80.1 billion budgeted in 2010. Steven Aftergood, *Intelligence Budget Data*, Fed'n of Am. Scientists (last visited Jan. 13, 2015), http://fas.org/irp/budget/index.html#4.

2 The President's Review Grp. on Intelligence and Commc'ns Tech., Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (2013) [hereinafter PRG Report], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; Privacy and Civil Liberties Oversight Bd., 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 (2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf; Privacy and Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014) [hereinafter PCLOB 702 Report], *available at* http://www.pclob.gov/library/702-Report.pdf.

3 *Mission*, Intelligence Community, http://www.intelligence.gov/mission/member-agencies.html (last visited Jan. 13, 2015) (describing the Intelligence Community and each of the 17 organizations which jointly comprise it).

4 *U.S. Security Spending Since 9/11,* Nat'l Priorities Project (May 26, 2011), https://www.nationalpriorities.org/analysis/2011/us-security-spending-since-911/.

5 The most recent report from the Office of the Director of National Intelligence reports 5,150,379 people were eligible for access to classified information in 2013. Office of the Dir. of Nat'l Intelligence, 2013 Report on Security Clearance Determinations 4 (2014), *available at* http://www.dni.gov/files/documents/2013%20Report%20on%20Security%20Clearance%20Determinations.pdf.

6 Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, Wash. Post Top Secret Am. (July 19, 2010, 4:50 PM), http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/.

7 U.S. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee"), Intelligence Activities and the Rights of Americans, S. Rep. No. 94-755, bk. II at 289 (1976) [hereinafter Church Committee Report].

8 Colleen Long, *NYPD, Microsoft Create Crime-Fighting 'Domain Awareness' Tech System*, Huff. Post (Feb. 20, 2013), http://www.huffingtonpost.com/2013/02/20/nypd-microsoft-domain-awareness-crime-fighting-tech_n_2727506.html.

9 Jennifer Lynch, *FBI to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, ArsTechnica (Apr. 14, 2014, 12:35 PM), http://arstechnica.com/tech-policy/2014/04/fbi-to-have-52-million-photos-in-its-ngi-face-recognition-database-by-next-year/.

10 John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

11 International Covenant on Civil and Political Rights, Preamble, Dec. 19, 1966, 999 U.N.T.S. 171.

12 Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. Times (June 23, 2006), http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all&_r=0.

13 Terrorist Finance Tracking Programme, Eur. Comm. on Migration and Home Aff. (last visited Jan. 13, 2015), http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp/index_en.htm (describing the history and main features of the E.U.-U.S. Terrorist Finance Tracking Programme agreement).

14 Press Release, European Parliament, MEPs Call for Suspension of EU-US Bank Data Deal in Response to NSA Snooping (Oct. 23, 2013), *available at* http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22725/html/MEPs-call-for-suspension-of-EU-US-bank-data-deal-in-response-to-NSA-snooping.

15 Daniel Castro, The Info. Tech. & Innovation Found., How Much Will PRISM Cost the U.S. Cloud Computing Industry? (2013), *available at* http://www2.itif.org/2013-cloud-computing-costs.pdf.

16 *See, e.g.,* Ian Brown, *Will NSA Revelations Lead to the Balkanisation of the Internet?*, Guardian (Nov. 1, 2013, 02:05 PM), http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet; Michael Hickens, *Post-Snowden 'Balkanization' of the Internet Should Worry CIOs*, Wall St. J. (Apr. 14, 2014, 5:23 PM), http://blogs.wsj.com/cio/2014/04/14/post-snowden-balkanization-of-the-internet-should-worry-cios/.

17 Sascha Meinrath, *We Can't Let the Internet Become Balkanized*, Slate (Oct. 14, 2013, 9:15 AM), http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html.

18 PRG Report, *supra* note 2, at 15-18.

19 *Id.* at 170.

20 Alison Smale, Mark Mazzetti & David E. Sanger, *Germany Demands Top U.S. Intelligence Officer Be Expelled*, N.Y. Times (July 10, 2014), http://www.nytimes.com/2014/07/11/world/europe/germany-expels-top-us-intelligence-officer.html?_r=2.

21 *See* Statement, New America Found. Open Technology Inst., OTI Withdraws Support for USA Freedom Act After House Leaders and Obama Administration Water Down its Surveillance Reforms (May 20, 2014), *available at* http://newamerica.net/node/110983.

22 Glyn Moody, *US-EU Relations After Two Important Votes in European Parliament: It's (More) Complicated*, TechDirt (Mar. 14, 2014, 5:33 PM), https://www.techdirt.com/articles/20140314/09113926578/us-eu-relations-after-two-important-votes-european-parliament-its-more-complicated.shtml.

23 Office of the U.N. High Comm'r for Human Rights, U.N. Human Rights Council, *The Right to Privacy in the Digital Age*, ¶ 30, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

24 Nat'l Comm'n on Terrorist Attacks upon the U.S. ("9/11 Commission"), The 9/11 Commission Report 420-421 (2004), *available at* http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

25 *Id.* at 420.

26 Comm'n on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction, Report to the President of the U.S., at 337 (2005), *available at* http://fas.org/irp/offdocs/wmd_report.pdf.

27 Comm'n on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, World at Risk 87 (2008).

28 Thomas Kean et al., Bipartisan Policy Ctr, Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of *The 9/11 Commission Report* 21 (2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf.

29 Brendan Sasso & Bob Cusack, *Patriot Act Author: Feinstein's Bill 'A Joke'*, The Hill (Dec. 10, 2013, 6:00 AM), http://thehill.com/homenews/house/192561-feinsteins-nsa-bill-is-a-joke-says-rep-james-sensenbrenner (quoting an interview with Rep. James Sensenbrenner).

30 50 U.S.C. § 3093(b)(1) (2015) (requiring the full congressional intelligence committees be kept "fully and currently informed") (formerly 50 U.S.C. § 413b); *see* Marshall Curtis Erwin, Cong. Research Serv., R406898, "Gang of Four" Congressional Intelligence Notifications (2013), *available at* http://fas.org/sgp/crs/intel/R40698.pdf.

31 Press Release, Sen. John D. (Jay) Rockefeller, Dec. 19, 2005 (commenting on the Terrorist Surveillance Program).

32 Letter from Rep. Jane Harman, Ranking Member H. Permanent Select Comm. on Intelligence, to President George W. Bush (Jan. 4, 2006), *available at* http://www.dailykos.com/story/2007/11/23/413783/-What-s-the-Matter-with-Jane-Harman.

33 *Id.*

34 *See* Alan Butler & Amie Stepanovich, *Square Peg, Round Hole — How the FISC Has Misapplied FISA to Allow for Bulk Metadata Collection*, Just Security (Dec. 2, 2013, 9:11 AM), http://justsecurity.org/3858/butler-stepanovich-square-peg-round-hole-fisc-fisa/.

35 *See* Jonathan Weisman, *Sounding the Alarm, but with a Muted Bell*, N.Y. Times (June 6, 2013), http://www.nytimes.com/2013/06/07/us/politics/senators-wyden-and-udall-warned-about-surveillance.html.

36 Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, Wash. Post (Aug. 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

37 U.S. S. Select Comm. on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program 5-6, 437-456 (2014) [hereinafter Senate Torture Report], *available at* http://www.intelligence.senate.gov/study2014/executive-summary.pdf.

38 *Id.* at 5-6, 437-454.

39 *d.* at 438-439.

40 *Id.* at 446.

41 Press Release, Statement on Intel Committee's CIA Detention, Interrogation Report (Mar. 11, 2014), *available at* http://www.feinstein.senate.gov/public/index.cfm/2014/3/feinstein-statement-on-intelligence-committee-s-cia-detention-interrogation-report (transcribing Sen. Dianne Feinstein's statement on the Senate floor regarding the Intelligence Committee's study on the CIA Detention and Interrogation Program).

42 *See* Jameel Jaffer, *The Torture Report and the "Glomar Fig Leaf"*, Just Security (Dec. 10, 2014, 4:14 PM), http://justsecurity.org/18242/glomar-fig-leaf/.

43 Senate Torture Report, *supra* note 37, at 401-408.

44 Senate Torture Report, *supra* note 37, at 405.

45 Church Committee Report, *supra* note 7, at bk. II p. 290.

46 Intelligence Authorization Act of Fiscal Year 2010, Pub. L. No. 111-259, § 405, 124 Stat. 2709 (codified as amended at 50 U.S.C. § 403); *see Who We Are*, Office of the Dir. of Nat'l Intelligence, http://www.dni.gov/index.php/about/organization/office-of-the-intelligence-community-inspector-general-who-we-are (last visited Jan. 22, 2015).

47 S. Rep. No. 107-51, at 38 (2000), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-107srpt51/html/CRPT-107srpt51.htm.

48 *E.g.*, Shane Harris, *Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State*, Salon (Nov. 16, 2014, 6:58 AM), http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/.

49 Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, Subtit. D, § 331(c), 124 Stat. 2654 (codified as amended at 50 U.S.C. § 3093 (2015), formerly 50 U.S.C. § 413b).

50 Darren Samuelsohn, *Hill Draws Criticism over NSA Oversight*, The Hill (Mar. 2, 2014, 10:14 PM), http://www.politico.com/story/2014/03/hill-draws-criticism-over-nsa-oversight-104151.html#ixzz38RhFFXMy.

51 The 9/11 Commission Report, *supra* note 24, at 417.

52 Over-classification is a complex topic with myriad causes. The amount of classified material produced each year is tracked by the National Archives' Information Security Oversight Office. From 2000 to 2004 the number of original classification decisions increased from 220,926 to 351,150. Since 2004, the number of original classification decisions has dropped sharply, to only 58,794 in 2013. While this dramatic decrease would seem to bode well for overall classification, the scope of derivative classification — classification decisions based on the original classifications — have risen sharply over the same period: from more than 15 million decisions in 2004 to over 80 million decisions in 2013 (which was down from a record 95 million in 2012). Part of this increase can be explained by a 2009 ISOO order that agencies count classified information that exists in electronic form, but the ratio of original to derivative classification decisions actually began increasing in 2006. *See* Info. Sec. Oversight Office, Nat'l Archives and Records Admin., 2013 Report to the President (2014), *available at* http://www.archives.gov/isoo/reports/2013-annual-report.pdf; David Perera, *ISOO: Original Classification Down, Derivative Classification Up*, FierceGovernmentIT (May 30, 2012), http://www.fiercegovernmentit.com/story/isoo-original-classification-down-derivative-classification/2012-05-30.

53 *See* Fazaga v. FBI, 885 F. Supp.2d 978 (C.D. Cal. 2012); *see generally* David Rudenstine, *The Courts and National Security: The Ordeal of the State Secrets Privilege*, 44 U. Balt. L. Rev. 37 (2015).

54 *See* Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013); Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F. 3d 644 (6th Cir. 2007).

55 Privacy and Civil Liberties Oversight Bd., Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act 35-36 (July 9, 2013), *available at* http://www.pclob.gov/library/20130709-Workshop_Transcript.pdf.

56 *E.g.,* Steven Aftergood, *Move to Declassify FISA Court Rulings Yields No Results*, Fed'n of Am. Scientists Secrecy News (May 29, 2012), http://fas.org/blogs/secrecy/2012/05/fisa_null/ (quoting Dean Boyd of the Department of Justice National Security Division noting the rarity of cases in which "a FISA Court produced substantial legal opinions that could be severed from the sensitive facts of the underlying applications.").

57 *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 66 (2013) (testimony of James R. Clapper, Att'y Gen.). *See also* Letter from Rep. F. James Sensenbrenner, Jr., Rep. Darrell Issa, Rep. Trent Franks, Rep. Ted Poe, Rep. Trey Gowdy, Rep. Raul Labrador & Rep. Blake Farenthold to Eric H. Holder, Jr., Att'y Gen. (Dec. 19, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/final_clapper_letter.pdf (discussing Hon. Clapper's comment and Sen. Dianne Feinstein and Sen. Ron Wyden's responses of surprise and comment that the statement was "obviously misleading, false"); Glenn Greenwald & Spencer Ackerman, *NSA Collected U.S. Email Records in Bulk for More than Two Years under Obama,* Guardian (June 27, 2013, 11:20 AM), http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

58 *In re* Production of Tangible Things from [REDACTED], No. 08-13, at 12 (FISA Ct. Mar. 2, 2009) (Walton, J.), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf; [REDACTED], 2011 WL 10945618, at n. 14 (FISA Ct. Oct. 3, 2011) (Bates, J.).

59 Letter from Sen. Mark Udall, Sen. Ron Wyden & Sen. Martin Heinrich to Hon. Donald Verrilli, Jr., Solicitor Gen. (Nov. 21, 2013), *available at* http://www.wyden.senate.gov/news/press-releases/udall-wyden-heinrich-urge-solicitor-general-to-set-record-straight-on-misrepresentations-to-us-supreme-court-in-clapper-v-amnesty.

60 PCLOB 702 Report, *supra* note 2, at 148.

61 For example, the victims of COINTELPRO were unaware that the FBI was behind the attacks against them. Church Committee Report, *supra* note 7, at bk. 2, p. 2-3.

62 PRG Report, *supra* note 2, at 47.

63 *See supra* notes 15-16 and accompanying text.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute info on our work, publications, events, and more.

Voting Newsletter | Latest developments, state updates, new research, and media roundup.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Money in Politics | Latest state and national developments and original analysis.

Redistricting Round-Up | Analysis of current legal battles and legislative efforts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Citizens United Five Years Later
Daniel I. Weiner

Election Spending 2014: Outside Spending in Senate Races Since Citizens United
Ian Vandewalker

15 Executive Actions
Michael Waldman and Inimai Chettiar

Federal Prosecution for the 21st Century
Lauren-Brooke Eisen, Nicole Fortier, and Inimai Chettiar

How to Fix the Voting System
Wendy Weiser, Jonathan Brater, Diana Kasdan, and Lawrence Norden

The Impact of Judicial Vacancies on Federal Trial Courts
Alicia Bannon

Democracy & Justice: Collected Writings, Vol. VII
Brennan Center for Justice

For more information, please visit www.brennancenter.org

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646-292-8310
www.brennancenter.org